10 największych błędów przy zapewnianiu zgodności z RODO

PAPIEROWE WDROŻENIE RODO

ZFODO

Prowadzone dotychczas przez organizacje działania, mające na celu dostosowanie do wymogów RODO, bywały chaotyczne. Często były wynikową informacji przeczytanych gdzieś w sieci przez osoby oddelegowane do zajęcia się tym „niewdzięcznym" zadaniem. Czasem, mimo dobrych chęci, niedookreślone przepisy RODO sprowadziły wdrażających rozporządzenie na manowce. Poniżej przedstawiamy zestawienie największych, najczęściej powtarzających się, rozbieżności między stanem pożądanym a faktycznym, które zostały zidentyfikowane przez członków ZFODO.

Idea RODO — 01

PRZYCZYNA BŁĘDU

Brak prawidłowego zrozumienia idei RODO.

BŁĄD

"Papierowe" wdrożenie – formalne przyjęcie w organizacji procedur, których nikt nie stosuje, a czasem nawet nie zna.

KONSEKWENCJE BŁĘDU

Faktyczny brak realizacji obowiązków administratora wynikających z RODO, skutkujące utratą danych, ich modyfikacji czy utraty dostępu do nich.

Analiza ryzyka dla zasobów — 02

PRZYCZYNA BŁĘDU

- Brak odpowiedniej świadomości na temat bezpieczeństwa informacji.
- Przeprowadzenie analizy ryzyka dla zasobów przez niewykwalifikowany personel, z małym doświadczeniem w obszarze bezpieczeństwa informacji.

BŁĄD

- Brak przeprowadzonej analizy ryzyka dla zasobów.
- Błędnie przeprowadzona analiza ryzyka dla zasobów.

KONSEKWENCJE BŁĘDU

- Brak zidentyfikowania zagrożenia wynikającego z wykorzystania danego zasobu do przetwarzania danych osobowych, a w konsekwencji możliwość utraty danych, ich modyfikacji czy utraty dostępu do nich.
- Niepoprawne zidentyfikowanie zagrożenia względem danego zasobu, a w konsekwencji złe dostosowanie zabezpieczenia, które nie będzie spełniało swojej roli, lub brak jakiegokolwiek zabezpieczenia.

Obszar IT — 03

PRZYCZYNA BŁĘDU

- Niedostosowanie obszaru IT
- Brak zdefiniowanej polityki retencji danych albo opracowanie jej wyłącznie na papierze – brak implementacji zasad retencji danych do systemów teleinformatycznych

BŁĄD

- Brak zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów oraz usług przetwarzania
- Niedostosowanie infrastruktury pod kątem możliwości realizacji praw osób, których dane dotyczą
- Przetwarzanie danych z naruszeniem zasady ograniczenia przechowywania

KONSEKWENCJE BŁĘDU

- Utrata, nieuprawniona modyfikacja lub nieuprawniony dostęp do danych
- Brak możliwości zrealizowania praw osób, których dane dotyczą
- Możliwe sankcje ze strony organu nadzorczego

Ocena skutków dla ochrony danych (DPIA) — 04

PRZYCZYNA BŁĘDU

- Błędna ocena co do braku przesłanek do przeprowadzenia oceny skutków dla ochrony danych (DPIA)
- Posłużenie się nieprawidłową metodyką sporządzenia DPIA

BŁĄD

- Brak przeprowadzenia oceny skutków dla ochrony danych (DPIA)
- Błędne przeprowadzenie DPIA

KONSEKWENCJE BŁĘDU

- Brak możliwości spełnienia przez administratora ciążącego na nim obowiązku – narażenie się na konsekwencje ze strony organu nadzorczego
- Niepodjęcie działań mających zminimalizować wystąpienie negatywnych skutków w postaci naruszenia praw lub wolności osób fizycznych na skutek ich niezidentyfikowania
- Błędna ocena skutków dla praw i wolności może powodować niepodjęcie działań mających na celu zmniejszenia ryzyka ich powstawania, a ostatecznie przyczynić się do strat finansowych, wizerunkowych itp. po stronie osoby fizycznej

Uregulowanie stosunku powierzenia — 05

PRZYCZYNA BŁĘDU

- Niezidentyfikowanie stosunku powierzenia istniejącego między podmiotami
- Brak weryfikacji podmiotu przetwarzającego przed powierzeniem danych

BŁĄD

- Brak uregulowania stosunku powierzenia lub powierzenie danych podmiotowi niedającemu wystarczających gwarancji bezpiecznego i zgodnego z RODO przetwarzania danych

KONSEKWENCJE BŁĘDU

- Niespełnienie przez administratora ciążącego na nim obowiązku zawarcia umowy powierzenia lub zawarcie umowy niespełniającej wszystkich wymogów RODO – narażenie się na konsekwencje ze strony organu nadzorczego
- Negatywne skutki związane z nieprawidłowym przetwarzaniem danych przez podmiot przetwarzający – możliwy jest przykładowo wyciek danych i w związku z tym strata finansowa i wizerunkowa po stronie administratora

Administrator czy jednak procesor? — 06

PRZYCZYNA BŁĘDU

- Identyfikowanie powierzonych przez inny podmiot danych jako „własnych"

BŁĄD

- Podejmowanie w stosunku do niewoich danych decyzji i działań jak administrator danych

KONSEKWENCJE BŁĘDU

- Możliwe sankcje ze strony organu nadzorczego spowodowane „przekroczeniem uprawnień" w stosunku do danych powierzonych przez inny podmiot

Obowiązek informacyjny — 07

PRZYCZYNA BŁĘDU

- Brak wdrożonej procedury przejrzystości, obejmującej spełnienie obowiązku informacyjnego

BŁĄD

- Brak spełnienia obowiązku informacyjnego przy zbieraniu danych od osoby fizycznej

KONSEKWENCJE BŁĘDU

- Brak realizacji obowiązku administratora wynikającego z RODO, skutkujące możliwością nałożenia sankcji ze strony organu nadzorczego

Koordynator wdrożenia — 08

PRZYCZYNA BŁĘDU

- Brak koordynatora wdrożenia po stronie organizacji lub też brak odpowiedniej „siły nacisku" z jego strony (brak faktycznej możliwości wyegzekwowania realizacji zadań związanych z wdrożeniem)

BŁĄD

- Brak lub znaczne spowolnienie realizacji zadań związanych z wdrożeniem

KONSEKWENCJE BŁĘDU

- Naruszenie obowiązków administratora (lub podmiotu przetwarzającego) związane np. z brakiem wdrożenia formalnie przyjętych procedur, a w konsekwencji możliwe sankcje ze strony organu nadzorczego

Świadomość pracowników — 09

PRZYCZYNA BŁĘDU

- Brak skutecznego uświadamiania pracowników o potrzebie i korzyściach związanych ze stosowaniem przepisów RODO
- Brak odpowiedniej świadomości na temat bezpieczeństwa informacji wśród pracowników każdego szczebla, spowodowany brakiem odpowiednich szkoleń, dostosowanych do grupy odbiorców

BŁĄD

- Lekceważące podejście pracowników do stosowania procedur i zasad bezpieczeństwa
- Brak w pracownikach poczucia odpowiedzialności za bezpieczeństwo przetwarzania danych

KONSEKWENCJE BŁĘDU

- Naruszenie obowiązków administratora (lub podmiotu przetwarzającego) związane z faktycznym brakiem stosowania formalnie przyjętych procedur, a w konsekwencji możliwe sankcje ze strony organu nadzorczego

Całościowe spojrzenie na wdrożenie — 10

PRZYCZYNA BŁĘDU

- Brak całościowego, systematycznego spojrzenia na ochronę danych w ramach organizacji lub w grupie przedsiębiorstw powiązanych
- Brak zrozumienia konieczności stałej, codziennej pracy nad utrzymaniem zgodności z rozporządzeniem (m.in. przeprowadzanie audytów, monitorowanie ryzyk)

BŁĄD

- Wybiórcze, wyrywkowe podejście do ochrony danych i obowiązków wskazanych w RODO, gaszenie pożaru, zamiast zapobiegania

KONSEKWENCJE BŁĘDU

- Chaos spowodowany brakiem koordynacji we wdrożeniu w ramach całej organizacji, poszczególne działania w ramach procesów podejmowane są w oderwaniu od innych procesów, co ostatecznie powoduje stratę czasu i zniechęcenie organizacji do regulacji RODO

Wskazane wyżej obszary to „grzechy główne", jednak są też inne aspekty wdrożenia nowych przepisów, które okazały się problematyczne. Dla przykładu, rola inspektora ochrony danych najczęściej jest niedoceniana, a jego pozycja w strukturze organizacji – niska. Często też IOD jest „z łapanki", nie posiada odpowiednich kwalifikacji oraz ma niewielki wpływ na decyzje podejmowane przez najwyższe kierownictwo, jego głos jest traktowany wyłącznie jako doradczy.

Innym, często nieuświadamianym sobie przez administratorów błędem, jest przekazywanie danych do państw trzecich czy organizacji międzynarodowych bez zastosowania jakichkolwiek przewidzianych w RODO zabezpieczeń. Najczęściej ma to miejsce w kontekście korzystania z dostarczanych przez podmioty zewnętrzne rozwiązań chmurowych, gdzie dane są faktycznie przechowywane poza EOG.

Kolejny wycinkiem wdrażania RODO, gdzie idee rozporządzenia nie zostały przez administratorów właściwie odczytane, jest informowanie organu nadzorczego o naruszeniach. Dochodzi albo do niepotrzebnego informowania o naruszeniach albo do nieinformowania o nich wcale, wówczas kiedy jest to konieczne. Trzeba jednak podkreślić, że problem tkwi wówczas w nieprawidłowej ocenie, czy dane naruszenie może powodować ryzyko naruszenia praw i wolności osób fizycznych, i jak wysokie jest to ryzyko.

Wreszcie, wielu administratorów z uwagi na brak w przepisach wyraźnego wymogu przyjęcia i wdrożenia odpowiednich polityk całkowicie tego zaniechuje, podczas gdy dla wykazania spełnienia wymogów z RODO stosowanie polityk jest niezbędne.

ZFODO

KONTAKT DLA MEDIÓW
e-mail: kontakt@zfodo.org.pl
tel.: 22 740 99 00