Europejskie rozporządzenie o ochronie danych osobowych (RODO z ang. General Data Protection Regulation – GDPR) to to unijne rozporządzenie które wprowadza całkowicie nowe podejście do ochronnych danych osobowych. Nowe przepisy wprowadzają szereg obowiązków, nowe rodzaje odpowiedzialności jak również wysokie sankcje finansowe.

Proponujemy następujące etapy wrażania rozporządzenia RODO:
• warsztaty dla zespołu wprowadzającego zmiany,
• audyt wstępny,
• analizę ryzyka w procesach przetwarzania danych osobowych,
• dostosowanie procesów biznesowych,
• dostosowanie systemu informatycznego,
• dostosowanie dokumentacji (procedur, klauzul i umów),
• szkolenie pracowników i współpracowników,
• audyt końcowy.
Kluczowe obszary przy wdrażaniu RODO:
1) Analiza ryzyka
• określenie zasad wdrożenia zabezpieczeń zgodnych z RODO,
• zdefiniowanie procesów zachodzących u klienta,
• zidentyfikowanie zagrożeń, podatności, prawdopodobieństwa i skutków.
• zdefiniowania obecnych zabezpieczeń,
• opracowanie zasad postępowania z ryzykiem.

Dostosowanie środków technicznych i IT
• dostosowanie środków technicznych i IT do oszacowanego ryzyka,
• ocena przystosowania zastosowanych zabezpieczeń,
• stworzenie procedury m.in.: szyfrowania danych osobowych i pseudonimizacji, zapewnienia ciągłości działania, regularnego testowania zastosowanych środków.

Dostosowanie środków organizacyjnych
• dostosowanie środków organizacyjnych do oszacowanego ryzyka,
• ocena obecnych zabezpieczeń,

• wprowadzenie wśród pracowników procedur postępowania z danymi (zasady czystego biurka, czystego ekranu, polityki kluczy, itd.).

Usuwanie danych
• analiza danych podlegających niszczeniu i terminów w jakich to jest dokonywane,
• analiza metod usuwania danych i ich skuteczności,
• stworzenie procedur niszczenia danych z nośników papierowych oraz danych z nośników elektronicznych.

Wdrożenie zasady przejrzystości
• zweryfikowanie klauzul informacyjnych i zgód pod kątem sformułowania ich jasnym i przejrzystym językiem,
• przegląd dotychczasowych dokumentów, komunikatów, pism, regulaminów kierowanych do osób, których dane dotyczą pod kątem stosowania zady przejrzystości,
• przyjęcie procedur, iż wszystkie komunikaty kierowane do osób, których dane dotyczą są sformułowane jasnym i prostym językiem.

Stworzenie dokumentacji ochrony danych osobowych
• przegląd dotychczas obowiązujących wzorów dokumentacji
• dostosowanie funkcjonujących polityk do nowych przepisów przy uwzględnieniu oszacowanego ryzyka,
• stworzenie nowych procedur dostosowanych do wymogów RODO.

Rejestr czynności przetwarzania
• analiza czy organizacja ma obowiązek stworzyć przedmiotowy rejestr,
• weryfikacja procesów związanych z przetwarzaniem danych osobowych,
• stworzenie szablonu rejestru czynności przetwarzania w kontekście zidentyfikowanych procesów.

Weryfikacja podstaw przetwarzania
• przegląd procesów związanych z przetwarzaniem danych osobowych i ustalenie

podstaw prawnych uprawniających do przetwarzania danych osobowych,
• weryfikacja podstaw do przetwarzania danych wrażliwych,
• przegląd treści zgód na podstawie, których dochodzi do przetwarzania danych osobowych
• dostosowanie formularzy zgód na przetwarzanie danych osobowych.

Inspektor ochrony danych
• analiza czy organizacja ma obowiązek powołać inspektora ochrony danych osobowych,
• wskazanie jakie kwalifikacji powinien mieć IOD, ustalenie jego kompetencji i wskazanie zadań,
• stworzenie funkcji IOD tak aby mogła pełnić rolę tzw. punktu kontaktowego (m.in. powołanie, zapewnienie organowi nadzorczemu oraz osobom, których dane dotyczą bezpośredniego kontaktu z nim).

Wdrożenie mechanizmu ochrony domyślnej i w fazie projektowania
• stworzenie procedury przejrzystości co do funkcji i przetwarzania danych osobowych (umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń) oraz minimalizacji przetwarzania danych osobowych,
• stworzenie procedur by podczas opracowywania i projektowania produktów, usług, aplikacji wzięto pod uwagę prawo do ochrony danych osobowych i zapewnić administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych.

Certyfikacja
• analiza potrzeby poddania się przez organizację certyfikacji,
• weryfikacja gotowości organizacji do poddania się certyfikacji.

Zgłaszanie naruszeń
• stworzenie procedury postępowania w razie wystąpienia incydentu ochrony danych osobowych,
• stworzenie szablonu rejestru naruszeń ochrony danych osobowych.

Współadministrowanie

• zidentyfikowanie spółek wchodzących w skład grupy kapitałowej,
• analiza przepływu danych pomiędzy spółkami i identyfikacja współadministratorów,
• stworzenie szablonu i zawarcie wspólnych uzgodnień pomiędzy spółkami współadministrującymi danymi.

Umożliwienie realizacji praw podmiotu danych
• dostosowanie systemów informatycznych tak aby mogły na żądanie osoby, której dane dotyczą m.in.: usuwać całkowicie jej dane osobowe, przenosić do innego usługodawcy jej dane osobowe, wygenerować plik z wszystkimi jej danymi osobowymi itd.,
• stworzenie procedury udzielania odpowiedzi na zapytania osoby, której dane dotyczą w terminie miesiąca zgodnie z zasadą przejrzystości.

Dostosowanie procesu profilowania
• analiza procesów przetwarzania danych osobowych pod kątem zautomatyzowanego przetwarzania danych osobowych w tym profilowania,
• ustalenie podstaw do przetwarzania danych osobowych w sposób zautomatyzowany,
• stworzenie klauzul zgód na dokonywanie profilowania rodzącego skutki prawne po stronie osoby, której dane dotyczą.

Spełnienie nowego obowiązku informacyjnego
• analiza jak dotychczas wyglądało spełnianie obowiązku informacyjnego i jakimi kanałami było dokonywane,
• stworzenie nowych formularzy zawierających informacje jakie muszą zostać zakomunikowane osobie, której dane mają być przetwarzane.

Ocena skutków dla ochrony danych
• analiza czy organizacja jest zobligowana do dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych,

• dokonanie oceny skutków planowanych operacji przetwarzania danych dla ochrony danych osobowych.

Zmiana współpracy z procesorem
• analiza dotychczasowego wzoru umowy powierzenia przetwarzania danych osobowych zawieranego z procesorem,
• stworzenie wykazu procesorów,
• dostosowanie nowego wzoru umowy powierzenia do wymogów RODO.

Dostosowanie zasad transferu danych poza EOG
• analiza czy administrator danych osobowych przekazuje dane osobowe poza Europejski Obszar Gospodarczy,
• ustalenie podstaw do przekazywania danych do państwa trzeciego,
• dostosowanie procesu przekazywania danych do państw trzecich do wymogów RODO.