Rozporządzenie UE
o ochronie danych
osobowych (RODO):

Czy jesteś na nie przygotowany?

EY
Building a better working world

Co powinieneś wiedzieć o nowym rozporządzeniu UE o ochronie danych osobowych?

Ochrona danych osobowych weszła w okres bezprecedensowych zmian. Jest to spowodowane przez:

- Nowe rozporządzenie UE o ochronie danych osobowych (RODO) – największą reformę ochrony danych osobowych od 21 lat
- Nagłaśnianą przez media wzrastającą liczbę poważnych naruszeń danych osobowych, co doprowadziło konsumentów i regulatorów do zajęcia się problemem zarządzania danymi osobowymi
- Upadek rozwiązania „Bezpiecznej Przystani" (ang. *Safe Harbor*) i zastąpienie go nową podstawą transferów danych do USA – „Tarczą Prywatności" (ang. *Privacy Shield*)

Po czterech latach trudnych negocjacji, 25 maja 2016 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych osobowych z *vacatio legis* do 25 maja 2018 r. Ten okres przejściowy daje czas na analizy wpływu reformy na poszczególne instytucje i branże. Wiele instytucji już teraz rozpoczęło przygotowania zdając sobie sprawę z tego, iż skala zmian jest duża, a wdrożenie wymaganych rozwiązań – bardzo wymagające.

Rozporządzenie w sposób rewolucyjny zmienia zasady ochrony danych osobowych. Podtrzymuje kluczowe zasady określone w dyrektywie 95/46/WE, którą zastąpi, przynosi przełomowe zmiany, nowe rozwiązania i wzmocnienie dotychczasowych wymagań. Wprowadza wiele nowych uprawnień osób fizycznych i obowiązków administratorów danych. Określa obowiązki każdej instytucji, która aktywnie korzysta lub choćby przechowuje dane osobowe, niezależnie od branży i niezależnie od tego, czy jest prywatna czy publiczna.

Celem Rozporządzenia jest aktualizacja i wzmocnienie rozwiązań zapewniających ochronę danych ze względu na wpływ technologii przetwarzania danych. Nakłada ono nowe obowiązki m.in. na instytucje finansowe, sklepy internetowe, podmioty świadczące usługi online, operatorów portali społecznościowych, czy podmioty dokonujące globalnych transferów danych w ramach korporacji.

Reforma wprowadza dotkliwe kary pieniężne, które będą nakładane na administratorów danych, mogące wynieść nawet 20 mln EUR lub 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego. Co więcej – stosuje się wyższą z tych kwot.

Główne zmiany wprowadzone przez RODO

Sankcje

Kary grzywny za naruszenie RODO są dotkliwe. Regulator będzie mógł nałożyć grzywnę w wysokości do:

- 4% całkowitego rocznego światowego obrotu lub
- 20.000.000 EUR

4% Kary grzywny w wysokości do 4% całkowitego rocznego światowego obrotu

lub **20 mln EUR**

Ochrona danych osobowych niezależnie od miejsca ich przetwarzania

Rozporządzenie dotyczy wszystkich administratorów danych osobowych i podmiotów przetwarzających te dane, mających siedzibę w UE, a także spoza UE, jeżeli oferują usługi lub produkty w państwach członkowskich.

Inspektor Ochrony Danych (IOD)

IOD (następca Administratora Bezpieczeństwa Informacji) musi być powołany, jeżeli działalność w organizacji wiąże się z systematycznym monitoringiem osób, których dane dotyczą (w tym pracowników) na dużą skalę, a więc np. z wyciąganiem wniosków z obserwacji ich zachowania w sieci, lub z przetwarzaniem na dużą skalę danych wrażliwych, np. o stanie zdrowia.

Program ochrony danych

Organizacje muszą wykazać, że zapewniły:

- Ustanowienie systemu monitorowania, przeglądu i oceny procedur przetwarzania danych osobowych
- Minimalizowanie przetwarzania i przechowywania danych osobowych, np. przez pseudonimizację
- Wdrożenie środków ochronnych przy przetwarzaniu danych
- Dokumentowanie zasad, procedur i czynności przetwarzania danych osobowych, które muszą być możliwe do udostępnienia organom nadzorczym na ich wniosek

Ocena wpływu na prywatność

Organizacje muszą dokonać oceny ryzyka i wpływu zamierzonego przetwarzania na prywatność podmiotów danych.

Zgoda

- Zgoda konsumenta na przetwarzanie danych osobowych musi być dobrowolna i świadoma oraz wskazywać cel przetwarzania danych
- Klienci muszą być poinformowani o przysługującym im prawie do wycofania swojej zgody, a jej wycofanie musi być równie łatwe jak jej wyrażenie
- Klauzule służące do odbierania zgody muszą być formułowane czytelnym językiem
- Zgoda musi być „wyraźna" szczególnie w przypadku wrażliwych danych osobowych lub transgranicznego przepływu danych
- Pozyskanie zgody musi być poprzedzone jasną informacją o podstawach prawnych, celu i innych aspektach przetwarzania ich danych

Obowiązkowa notyfikacja naruszeń

- Organizacje muszą zgłaszać organowi nadzorczemu naruszenia danych osobowych do 72 godzin od ich stwierdzenia, chyba że jest mało prawdopodobne, by naruszenie stanowiło zagrożenie dla osób fizycznych
- W razie znacznego ryzyka dla osób fizycznych, osoby te również będą musiały być poinformowane o incydencie
- Wymaga to również zobowiązania processorów do raportowania incydentów organizacji

72h Zgłaszanie organowi nadzorczemu naruszenia danych osobowych

Nowe uprawnienia osób, których dotyczą przetwarzane dane

- **Prawo do bycia zapomnianym** – prawo wystąpienia w określonych okolicznościach do administratorów danych osobowych o usunięcie bez zbędnej zwłoki wszelkich danych osobowych, w tym w Internecie
- **Prawo do przenoszenia danych** – jeżeli osoby fizyczne przekazały dane osobowe usługodawcy mogą następnie żądać, by ten przeniósł te dane do innego usługodawcy w popularnym formacie elektronicznym, o ile jest to technicznie wykonalne
- **Prawo do sprzeciwu wobec profilowania** - tworzenia statystycznej charakterystyki osoby i podejmowania decyzji na tej podstawie w automatycznym procesie

Ochrona prywatności w fazie projektowania i domyślna ochrona danych

- Organizacje powinny uwzględniać ochronę danych przy rozwijaniu procesów biznesowych i nowych systemów już na etapie projektowania usług, systemów i aplikacji
- Ustawienia prywatności domyślnie są ustawione na wysokim poziomie, bez konieczności ingerencji użytkownika

Współadministratorzy i podmioty przetwarzające dane na zlecenie

- Odpowiedzialność za ochronę danych osobowych będzie mogła być podzielona między kilku różnych współadministratorów danych. Obowiązek ochrony danych obejmuje również podmioty przetwarzające dane na zlecenie

Transfery danych do państw trzecich

Rozporządzenie określa wyjątki od zakazu transferu danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony i porządkuje te wyjątki przypisując je do sytuacji, w których ich zastosowanie jest optymalne.

Czy przedsiębiorcy są gotowi na rozporządzenie UE o ochronie danych osobowych?

Organizacje mają czas na przygotowanie się do RODO podczas okresu przejściowego, po upływie którego krajowe przepisy wydane zgodnie ze starą dyrektywą o ochronie danych osobowych zostaną zastąpione nowym Rozporządzeniem. Z uwagi na to, że reforma wprowadzana jest rozporządzeniem UE, wejdzie ona w życie w Polsce i w każdym państwie UE automatycznie, RODO będzie stosowane bezpośrednio bez odrębnej implementacji.

Teraz jest czas, aby podjąć działania i zadać sobie następujące pytania:

Ochrona danych osobowych niezależnie od miejsca ich przetwarzania

Czy jesteś administratorem danych lub przetwarzasz je na zlecenie w UE? Czy przetwarzasz dane osobowe poza UE, ale są to dane obywateli UE?

Inspektor Ochrony Danych

Czy Twoja główna działalność obejmuje systematyczny monitoring osób, których dane dotyczą (w tym pracowników), a więc np. czy wyciągasz wnioski z obserwacji ich zachowania w sieci? Czy głównym przedmiotem Twojej działalności jest przetwarzanie danych na dużą skalę lub przetwarzanie na dużą skalę danych wrażliwych, np. o stanie zdrowia oraz danych o przestępstwach i wyrokach skazujących za nie?

Program ochrony danych

Czy przeprowadziłeś udokumentowaną analizę obecnego stanu ochrony danych w Twojej organizacji i zmian koniecznych do spełnienia wymagań RODO? Czy posiadasz udokumentowany program ochrony danych osobowych, który spełnia te wymagania?

Obowiązkowa notyfikacja naruszeń

Czy byłbyś w stanie powiadomić GIODO o naruszeniu danych osobowych w ciągu 72 godzin?

Ochrona prywatności w fazie projektowania i domyślna ochrona danych

Czy uwzględniasz ochronę danych osobowych i prywatności przy rozwijaniu Twoich procesów biznesowych i nowych systemów już na etapie projektowania usług, systemów i aplikacji?

Nowe uprawnienia osób, których dotyczą przetwarzane dane

Czy będziesz w stanie realizować nowe uprawnienia podmiotów danych: „do bycia zapomnianym", do ograniczenia przetwarzania, do przenoszenia danych i do sprzeciwu wobec profilowania?

Zgoda i powiadomienie

Czy Twoje klauzule służące do odbierania zgody są formułowane czytelnym językiem? Czy osoby, których dane zbierasz, zostały jasno poinformowane o podstawach prawnych, celu i innych aspektach przetwarzania ich danych?

Przekazywanie danych osobowych poza UE

Czy przekazujesz dane osobowe poza UE i EOG, np. korzystając ze wspólnych systemów informatycznych w ramach grupy kapitałowej?

Jak możesz się przygotować do wejścia w życie rozporządzenia UE o ochronie danych osobowych?

Przygotowanie się do wdrożenia RODO wymaga od organizacji analizy i pełnego zrozumienia ich obecnej zgodności z wymaganiami prawnymi. Ważnym pierwszym krokiem będzie uzyskanie jasności co do kluczowych aspektów przetwarzania przez nie danych osobowych, w tym:

Jakie dane osobowe są przetwarzane?

Na jakich podstawach prawnych?

Gdzie wewnątrz danej organizacji ten proces się odbywa?

Gdzie i dokąd dane są przekazywane (w tym z/do osób trzecich i transgranicznie)?

Jak zabezpieczone jest przetwarzanie danych osobowych podczas całego procesu?

Jak długo mają być przechowywane?

Podmioty rynku finansowego powinny przeanalizować zastosowanie nowych wymogów RODO dla różnych obszarów ryzyka. Ze świadomością swoich luk w zgodności z regulacjami, organizacje będą w stanie ocenić ryzyka związane z ich danymi osobowymi oraz opracować plany naprawcze zawierające priorytety, mające na celu dostosowanie ich zarządzania danymi osobowymi do nowej perspektywy regulacyjnej RODO.

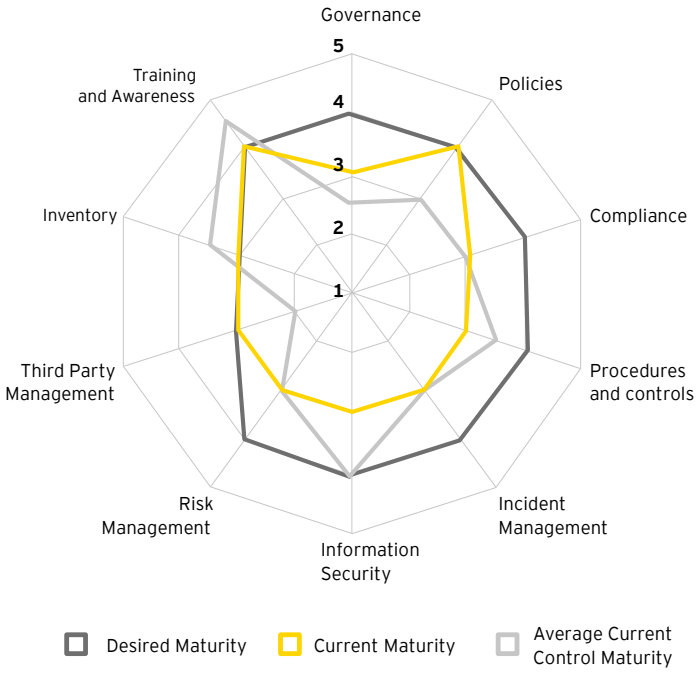
Jak możemy Ci pomóc w przygotowaniu się na RODO?

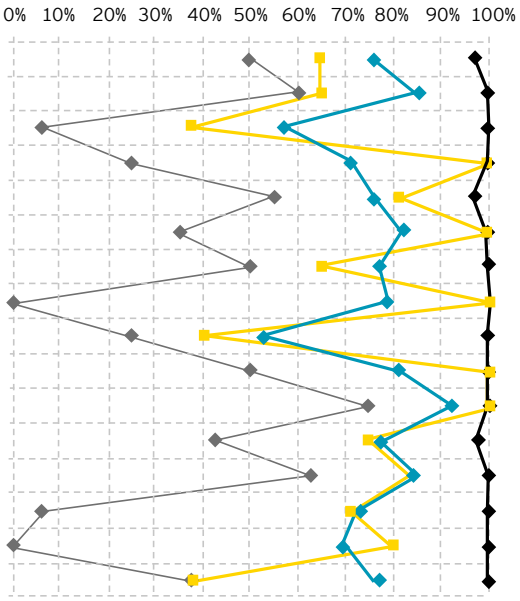
Rozwiązanie	Opis działań	Świadczona usługa	Ramy czasowe
Przyspieszona ocena ochrony danych osobowych	Wstępna ocena dojrzałości systemów ochrony danych osobowych	▶ Ukierunkowana ocena mierząca gotowość na nowe wymagania RODO	**1-3** dni
Kompleksowa ocena ochrony danych osobowych	Szczegółowa ocena dojrzałości systemów ochrony danych osobowych Ocena ryzyka	▶ Ocena ryzyka i dojrzałości systemów pod kątem RODO uwzględniająca ramy działalności biznesowej organizacji ▶ Rekomendacje i plan działań naprawczych ▶ Ocena ryzyka specyficznych produktów i procesów	**2-4** tygodnie w zależności od rozmiaru i złożoności organizacji
Ocena wpływu na prywatność	Dostosowana indywidualnie ocena oddziaływania na prywatność	▶ Ocena Twoich obecnych lub projektowanych systemów wskazująca na kluczowe ryzyka w ochronie danych	**1-2** tygodnie w zależności od rozmiaru i złożoności procesu lub systemu
Międzynarodowa strategia transferu danych	Standardowe Klauzule Umowne Wiążące Reguły Korporacyjne Inne narzędzia takie jak kodeksy postępowania lub zasady bezpiecznego transferu danych między UE a USA	▶ Identyfikacja przepływów danych ▶ Stworzenie odpowiednich narzędzi do transferu danych, w tym rozwój i wdrożenie: ▶ Standardowych Klauzul Umownych (dla administratorów danych i przetwarzających dane) ▶ Wiążących Reguł Korporacyjnych ▶ Polityk i procedur (takich jak: program audytu, wewnętrzne zarządzanie zgodnością, etc.) ▶ Zarządzania prywatnością ▶ Kodeksów postępowania ▶ Zasad transferu UE – USA	**1-24** miesięcy w zależności od rozmiaru podmiotu i rodzaju narzędzi, które będą musiały być wdrożone
Program zapewnienia zgodności z RODO	Odzwierciedlenie obowiązujących wymagań prawnych Rozwiązania w zakresie kontroli zgodności Dokumentowanie procesu przetwarzania danych osobowych Przygotowanie i wdrożenie procedur i polityk	▶ Zaprojektowanie i wdrożenie programów poprawy ochrony danych osobowych, w tym opracowanie i wdrożenie: ▶ Struktury ochrony danych osobowych ▶ Zarządzania prywatnością i struktury organizacyjnej ▶ Polityk i procedur ▶ Szkoleń i działań zwiększających świadomość ▶ Zarządzania incydentami ▶ Zarządzania relacjami z osobami trzecimi ▶ Zarządzania ryzykiem ▶ Kontroli i postępowań ▶ Kontroli bezpieczeństwa informacji ▶ Programu zgodności wiążących reguł korporacyjnych ▶ Bieżącej kontroli zgodności	**3-24** miesiące w zależności od stanu rozwoju i rozmiaru organizacji
Dodatkowe doradztwo i wsparcie prawne	Analiza prawna i sporządzenie dokumentów prawnych	▶ Analiza prawna zgodności z przepisami o ochronie danych osobowych ▶ Ocena wszelkich niezgodności oraz zaproponowanie działań naprawczych ▶ Sporządzenie umów dla administratorów danych i przetwarzających dane ▶ Szkolenie administratora bezpieczeństwa informacji/ inspektora ochrony danych	Ustalane na podstawie analizy każdego przypadku, w zależności od zakresu usługi

Przykładowe produkty

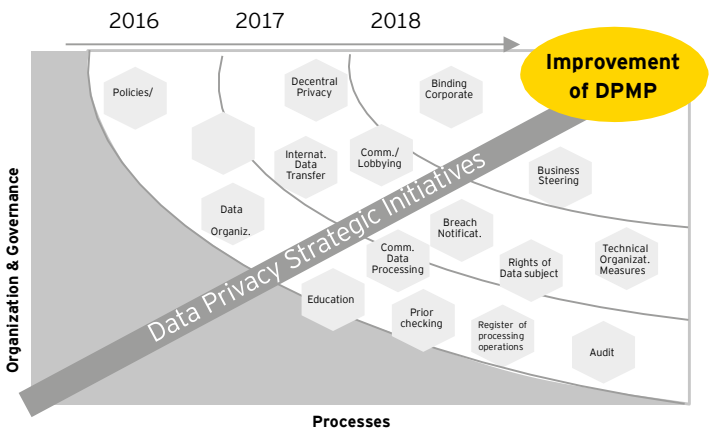
Pracujemy z przedsiębiorcami nad zwiększeniem rozumienia przez nich stopnia rozwoju swoich procesów i swojej zgodności z regulacjami.

Poniżej przedstawiamy kilka przykładów produktów, które stworzyliśmy dotychczas w zakresie projektów dotyczących ochrony danych osobowych:

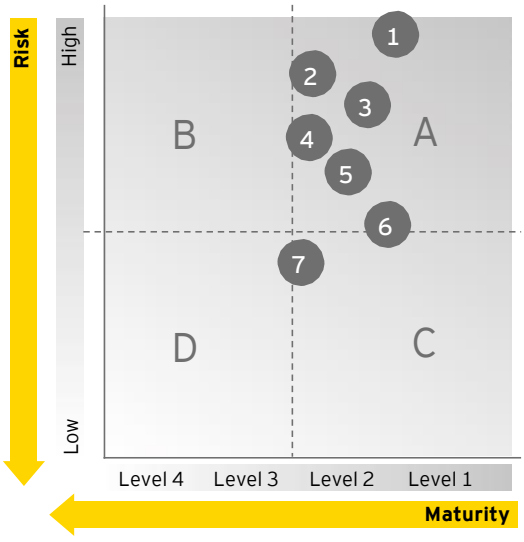




Strategy to improve data privacy management system



EY's risks map



Organizacje będą stawiać czoła wielu wyzwaniom przygotowując się do wejścia w życie RODO w przeciągu następnych dwóch lat. Dlatego ważne jest zrozumienie przez nie swojej obecnej pozycji oraz kroków niezbędnych do stopniowego osiągnięcia zgodności z RODO.

Jeżeli chcieliby Państwo omówić jakąkolwiek kwestię poruszoną w niniejszej broszurze to prosimy o skontaktowanie się z jedną z osób wymienionych na odwrocie.

EY | Assurance | Tax | Transactions | Advisory

O firmie EY

EY jest światowym liderem rynku usług profesjonalnych obejmujących usługi audytorskie, doradztwo podatkowe, doradztwo biznesowe i doradztwo transakcyjne. Nasza wiedza oraz świadczone przez nas najwyższej jakości usługi przyczyniają się do budowy zaufania na rynkach kapitałowych i w gospodarkach całego świata. W szeregach EY rozwijają się utalentowani liderzy zarządzający zgranymi zespołami, których celem jest spełnianie obietnic składanych przez markę EY. W ten sposób przyczyniamy się do budowy sprawniej funkcjonującego świata. Robimy to dla naszych klientów, społeczności, w których żyjemy i dla nas samych.

Nazwa EY odnosi się do firm członkowskich Ernst & Young Global Limited, z których każda stanowi osobny podmiot prawny. Ernst & Young Global Limited, brytyjska spółka z odpowiedzialnością ograniczoną do wysokości gwarancji (company limited by guarantee) nie świadczy usług na rzecz klientów. Aby uzyskać więcej informacji, wejdź na www.ey.com/pl

EY, Rondo ONZ 1, 00-124 Warszawa

SCORE: 00036-162

ey.com/pl

Kontakt

Kazimierz Klonecki
Partner

Tel. +48 505 105 080
Kazimierz.Klonecki@pl.ey.com

Michał Balicki
Adwokat

Tel. +48 519 033 737
Michal.Balicki@pl.ey.com

Krzysztof Dzioba
Radca prawny

Tel. +48 512 449 437
Krzysztof.Dzioba@pl.ey.com

Jakub Walarus
Menedżer

Tel. +48 519 511 402
Jakub.Walarus@pl.ey.com