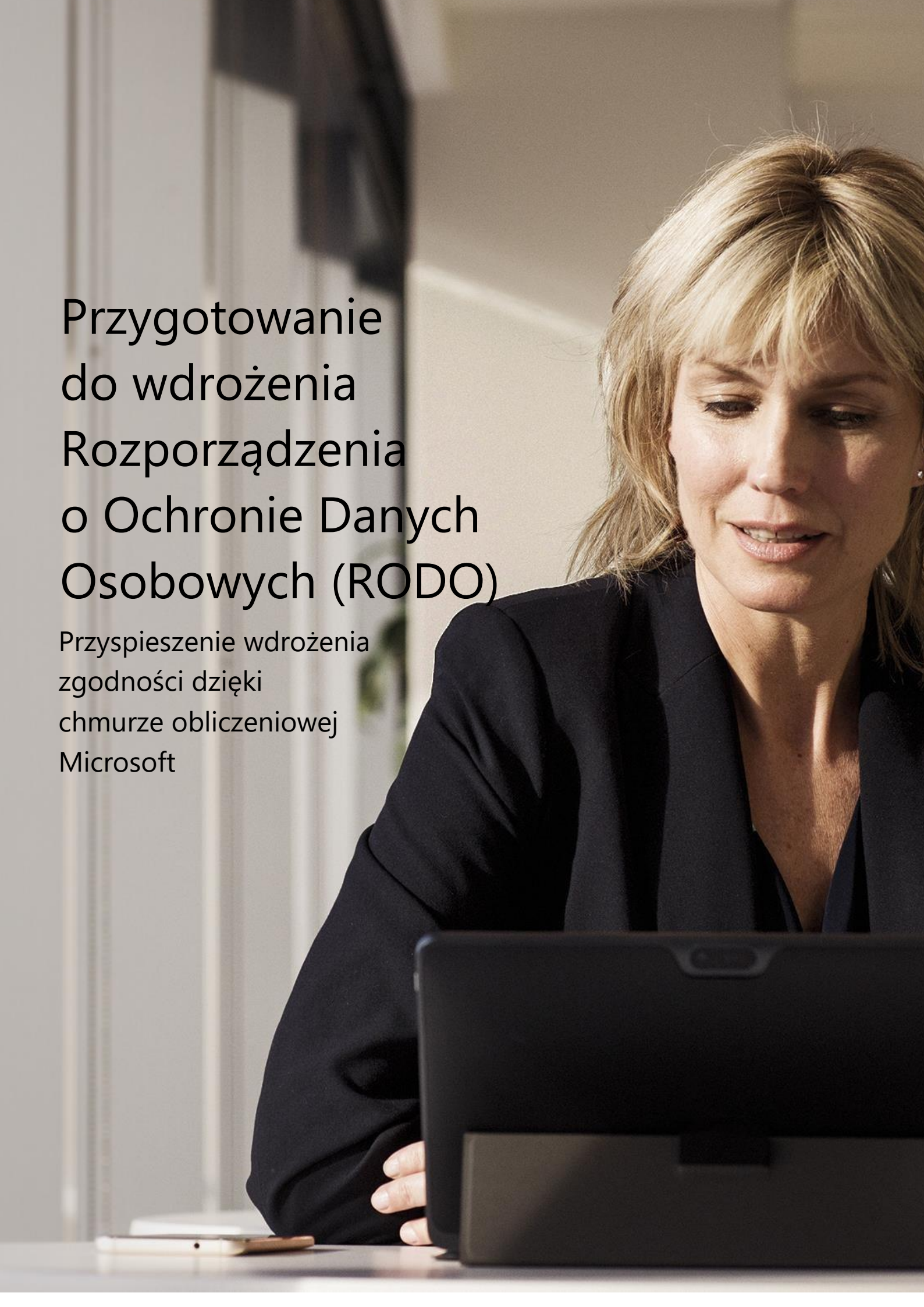

Przygotowanie do wdrożenia Rozporządzenia o Ochronie Danych Osobowych (RODO)

Przyspieszenie wdrożenia zgodności dzięki chmurze obliczeniowej Microsoft

Spis treści

Zastrzeżenia

Poniższy dokument jest komentarzem na temat Ogólnego Rozporządzenia o Ochronie Danych (RODO, GDPR), przedstawieniem w jaki sposób Microsoft interpretuje to prawo w dniu publikacji niniejszego dokumentu (maj 2017). Po dokładnej analizie Rozporządzenia Microsoft uważa, że prawidłowo odczytuje intencje i znaczenie tych przepisów prawa. Jednak wdrożenie RODO dla każdego procesu i każdej organizacji jest bardzo konkretne, a nie wszystkie aspekty i sposoby interpretacji artykułów są łatwe do rozstrzygnięcia.

W efekcie niniejszy dokument jest udostępniany wyłącznie w celach informacyjnych i nie powinien być traktowany jako porada prawna ani określenie sposobu, w jaki RODO może mieć zastosowanie do Państwa organizacji. Zachęcamy do współpracy z prawnie przygotowanymi specjalistami w celu określenia, jaki sposób wdrożenia jest najlepszy dla Państwa organizacji i w jaki sposób uzyskać zgodność z przepisami prawa.

MICROSOFT NIE UDZIELA W TYM DOKUMENCJIE ŻADNYCH GWARANCJI WYNIKAJĄCYCH Z ZAPISÓW PRAWA, BEZPOŚREDNICH LUB DOMNIEMANYCH. Dokument ten powinien być odczytywany dosłownie (ang. as is). Informacje i opinie dotyczące przepisów zawarte w tym dokumencie, adresy URL i inne odnośniki do witryn internetowych mogą ulec zmianie bez uprzedzenia. Niektóre linki mogą prowadzić do informacji w języku angielskim.

Ten dokument nie daje żadnych praw do jakiejkolwiek własności intelektualnej związanej z produktami Microsoft. Dokument może być kopiowany i wykorzystywany jako materiał przykładowy.

Data publikacji maj 2017
Wersja 1.1

Wprowadzenie

Z dniem 25 maja 2018 roku zacznie obowiązywać europejskie prawo o ochronie danych osobowych, które wprowadzi nowe globalne wymagania w zakresie prawa do ochrony danych osobowych, bezpieczeństwa i zapewnienia zgodności z obowiązującymi przepisami.

Ogólne Rozporządzenie o Ochronie Danych (General Data Protection Regulation), powszechnie nazywane RODO (ang. GDPR) , dotyczy głównie ochrony prawa do ochrony danych osobowych. RODO wprowadza restrykcyjne globalne wymagania w zakresie ochrony danych osobowych, regulujące sposób zarządzania i ochrony danych osobowych, przy jednoczesnym uszanowaniu wyborów dokonywanych przez poszczególne osoby – bez względu na to, gdzie dane są przesyłane, przetwarzane czy przechowywane.

Microsoft wraz ze swoimi klientami rozpoczął proces zmierzający do zrealizowania celów w zakresie ochrony danych osobowych wyznaczonych przez RODO. Microsoft uważa prawo do ochrony danych osobowych za fundamentalne i wierzy, że RODO stanowi ważny krok na drodze w kierunku wyjaśnienia, czym są i jak należy wdrażać prawa do ochrony danych osobowych osób fizycznych. Rozumiemy również, że wdrożenie RODO będzie wymagało wprowadzenia znacznych zmian przez organizacje działające na całym świecie.

Droga do RODO może wydawać się dużym wyzwaniem, a naszym zadaniem jest zapewnienie pomocy w jej pokonaniu.

Zaangażowanie Microsoft w proces wdrożenia RODO

Zaufanie to podstawowy element naszej misji, mającej na celu zapewnienie każdej osobie i każdej organizacji działającej na naszej planecie możliwości osiągania coraz wyższych celów. Nasze podejście do budowy zaufania jest oparte na ściśle określonych zasadach obejmujących pełne zaangażowanie w zapewnienie ochrony danych osobowych, bezpieczeństwa, zgodności z obowiązującymi przepisami i transparencji. Stosujemy te zasady przygotowując się do wdrożenia RODO.

Proces wdrożenia RODO postrzegamy jako wspólny obowiązek. Dlatego zobowiązujemy się do zapewnienia zgodności naszych usług chmurowych z RODO z chwilą wejścia regulacji w życie z dniem 25 maja 2018 roku.

Zobowiązujemy się również do dzielenia się naszymi doświadczeniami w zakresie zapewnienia zgodności ze złożonymi regulacjami, aby umożliwić Państwa organizacji znalezienie najlepszej drogi do spełnienia wymagań w zakresie ochrony danych osobowych wprowadzanych na mocy RODO. Dysponując najbardziej kompleksową ofertą rozwiązań w zakresie zapewnienia zgodności z obowiązującymi przepisami i bezpieczeństwa spośród wszystkich dostawców usług chmurowych oraz szerokim ekosystemem partnerów, jesteśmy przygotowani do zapewnienia wsparcia w realizacji Państwa programów w zakresie ochrony danych osobowych i bezpieczeństwa, zarówno teraz, jak i w przyszłości.

W ramach naszego zobowiązania do podjęcia z Państwem partnerskiej współpracy na drodze do wdrożenia RODO opracowaliśmy niniejszy dokument, który ma służyć Państwu jako pomoc w przygotowaniach. Dokument zawiera wprowadzenie do RODO, opis naszych działań w zakresie przygotowań do RODO oraz przykłady działań jakie Państwo mogą podjąć już dzisiaj we współpracy z Microsoft, aby rozpocząć swoją własny proces do zapewnienia zgodności z RODO.

Udostępnimy Państwu dalsze informacje wskazujące, w jaki sposób możemy służyć Państwu pomocą w zapewnieniu zgodności z tym ważnym, nowym prawem oraz jak w trakcie tego procesu, wspierać rozwój systemów ochrony danych osobowych osób fizycznych. Proszę odwiedzić poświęconą RODO w Centrum Zaufania Microsoft, aby zapoznać się z dodatkowymi materiałami oraz uzyskać dalsze informacje na temat pomocy jaką Microsoft może Państwu zaoferować celem spełnienia określonych wymagań RODO.

Zrozumieć RODO – wprowadzenie

Zanim przejdziemy do opisu konkretnych przykładów pokazujących, jak Microsoft może pomóc Państwu przygotować się do RODO, pragniemy odpowiedzieć na niektóre spośród najbardziej fundamentalnych i krytycznych pytań dotyczących rozporządzenia i co to może dla Państwa oznaczać. Dokładniejszy opis znajduje się tutaj.

Czym jest RODO?

RODO to nowa regulacja w zakresie ochrony danych osobowych obowiązująca w całej Unii Europejskiej. Zapewnia poszczególnym osobom większą kontrolę nad ich danymi osobowymi, przejrzystość w zakresie wykorzystywania danych osobowych i wymaga wprowadzenia mechanizmów bezpieczeństwa i kontroli mających na celu zapewnienie ochrony danych osobowych.

Czy RODO dotyczy mojej organizacji?

RODO ma szersze zastosowanie niż mogłoby się wydawać na pierwszy rzut oka. Prawo nakłada nowe zasady na firmy, agencje administracji państwowej, organizacje non-profit oraz inne organizacje oferujące produkty i usługi mieszkańcom Unii Europejskiej (UE) lub gromadzące i analizujące dane dotyczące rezydentów UE – przy czym przepisy te mają zastosowanie niezależnie od miejsca prowadzenia przez nie działalność: dotyczy to firm prowadzących działalność na terenie Unii Europejskiej, firm, które oferują usługi na jej terenie lub monitorują zachowanie obywateli Unii.

W odróżnieniu od przepisów prawa w zakresie ochrony danych osobowych obowiązujących w innych systemach prawnych, RODO dotyczy wszystkich organizacji, bez względu na ich wielkość i branżę, w której prowadzą działalność. UE jest często postrzegana na całym świecie jako wzór do naśladowania w zakresie ochrony danych osobowych, stąd oczekujemy również, że koncepcje zastosowane w RODO zostaną z czasem wprowadzone w innych częściach świata.

Kiedy RODO zacznie obowiązywać?

Przepisy RODO zaczynają obowiązywać z dniem 25 maja 2018 roku. Rozporządzenie zastąpi dotychczasową Dyrektywę o Ochronie Danych Osobowych (Dyrektywa 95/46/EC), obowiązującą od 1995 roku. W rzeczywistości RODO stało się prawem w UE w kwietniu 2016 roku, ale ze względu na znaczące zmiany jakie niektóre organizacje będą musiały wprowadzić w swojej działalności celem zapewnienia zgodności, zastosowano 2-letni okres przejściowy.

Jakie kluczowe pojęcia znajdują się w RODO?

RODO opiera się na sześciu zasadach:

- Wymóg zapewnienia przejrzystości przetwarzania i wykorzystywania danych osobowych.
- Ograniczenie przetwarzania danych osobowych do określonych, zgodnych z prawem celów.
- Ograniczenie gromadzenia i przechowywania danych osobowych do celów zgodnych z przeznaczeniem.
- Umożliwienie osobom fizycznym poprawiania lub wnioskowania o usunięcie ich danych osobowych.
- Ograniczenie czasu przechowywania danych osobowych do okresu, w którym jest to niezbędne do celu zgodnego z przeznaczeniem.
- Zapewnienie ochrony danych osobowych przy zastosowaniu odpowiednich praktyk w zakresie bezpieczeństwa.

Jakie są przykłady wymagań RODO dotyczących tych zasad?

- Zgodnie z RODO osoby fizyczne mają prawo wiedzieć, czy dana organizacja przetwarza ich dane osobowe oraz poznać cele tego przetwarzania. Osoba fizyczna ma prawo do wnioskowania o usunięcie lub sprostowanie swoich danych, wnioskowania o zaprzestanie ich przetwarzania, wyrażenia sprzeciwu wobec prowadzenia wobec niej bezpośrednich działań marketingowych oraz cofnięcia zgody na określone sposoby wykorzystywania swoich danych osobowych. Prawo do przenoszenia danych zapewnia osobom fizycznym prawo do przeniesienia ich danych w inne miejsca oraz do otrzymania pomocy w tym zakresie.
- RODO nakłada na organizacje wymóg ochrony danych osobowych w zależności od poziomu ich wrażliwości. W przypadku naruszenia ochrony danych osobowych podmioty przetwarzające dane są generalnie zobowiązane powiadomić stosowne organy nadzorcze w ciągu 72 godzin. Ponadto, jeżeli naruszenie danych osobowych może powodować duże ryzyko naruszenia praw i wolności osób fizycznych, wówczas organizacje będą również musiały, bez zbędnej zwłoki, powiadomić o tym fakcie osoby, których dane zostały naruszone.
- Musi istnieć podstawa prawna przetwarzania danych osobowych. Każda zgoda na przetwarzanie danych osobowych musi zostać „udzielona z własnej woli, w konkretnym celu, w sposób świadomy i jednoznaczny." RODO przewiduje szczególne wymagania w zakresie zapewnienia ochrony dzieci.
- Organizacje są zobowiązane dokonywać oceny skutków dla ochrony danych celem przewidywania skutków realizacji projektów z punktu widzenia zapewnienia ochrony danych osobowych i jeżeli zajdzie taka potrzeba, zastosowania środków zaradczych. Musi być prowadzona ewidencja działań w zakresie przetwarzania danych, udzielonych zgód na przetwarzanie danych oraz zapewnienia zgodności z RODO.

- Zapewnienie zgodności z RODO nie jest działaniem jednorazowym tylko stale realizowanym procesem. Brak zgodności z RODO może doprowadzić do nałożenia znaczących kar. Aby zapewnić zgodność z RODO zachęca się organizacje do wprowadzania kultury ochrony danych osobowych celem ochrony interesów osób fizycznych w zakresie ochrony ich danych osobowych.

Aby uzyskać bardziej szczegółowe informacje na temat RODO oraz lepiej zrozumieć takie terminy jak pseudonimizacja, przetwarzanie, administratorzy, przetwarzający, osoby, których dane dotyczą i dane osobowe, należy zajrzeć na stronę Microsoft.com/GDPR. Jesteśmy gotowi pomóc Państwu spełnić wymagania RODO oraz wspierać proces zapewnienia ochrony danych osobowych osób fizycznych.

Partnerstwo z Microsoft w procesie wdrażania RODO

Zapewnienie zgodności z RODO to wyzwanie dla całej firmy, które wymaga poświęcenia czasu, narzędzi, procesów i wiedzy oraz może wymagać wprowadzenia znaczących zmian w dotychczas stosowanych praktykach w zakresie ochrony i zarządzania danymi osobowymi. Droga do zapewnienia zgodności z RODO będzie łatwiejsza, jeżeli będą Państwo działali w ramach dobrze zaprojektowanego modelu usług chmurowych oraz wdrożą Państwo skuteczny program zarządzania danymi. Mogą Państwo liczyć na pomoc Microsoft i naszych partnerów w drodze do skutecznego zapewnienia zgodności z RODO.

Microsoft ma za sobą długą historię świadczenia usług chmurowych, którym można zaufać. Nasze podejście do zapewnienia ochrony danych osobowych, bezpieczeństwa, zgodności z obowiązującymi przepisami i przejrzystości jest oparte na ściśle określonych zasadach ma na celu budowę Państwa zaufania do technologii. Dysponujemy najszerszą na rynku ofertą rozwiązań mających na celu zapewnienie zgodności z obowiązującymi przepisami i pierwsi przyjęliśmy kluczowe standardy, takie jak standard dotyczący ochrony danych osobowych w chmurze ISO/IEC 27018. Nasi klienci i partnerzy wykorzystują nasze doświadczenie w zakresie zapewnienia ochrony danych osobowych, bezpieczeństwa, zgodności z obowiązującymi przepisami i na przejrzystych zasadach.

Oto co możemy Państwu zaoferować w ramach przygotowań do zapewnienia zgodności z RODO:

- **Technologia, która spełnia Państwa potrzeby**. Mogą Państwo skorzystać z naszej szerokiej oferty usług chmurowych przeznaczonych dla przedsiębiorstw celem wywiązania się z wynikających z RODO obowiązków w takich obszarach jak usuwanie, poprawianie, przenoszenie, zapewnienie dostępu do oraz zgłaszanie sprzeciwu wobec przetwarzania danych osobowych. Ponadto, mogą Państwo liczyć na nasz globalny ekosystem partnerów w zakresie wsparcia eksperckiego przy wdrażaniu technologii Microsoft.

- **Zobowiązania umowne**. Zapewniamy Państwu wsparcie wywiązując się ze zobowiązań wynikających z zawartych umów dotyczących naszych usług chmurowych, w tym realizując w wymaganych terminach obsługę serwisową rozwiązań w zakresie bezpieczeństwa oraz zapewniając stosowne powiadomienia zgodnie z nowymi wymaganiami RODO. Od września 2017 roku nasze umowy licencyjne dla klientów dotyczące usług chmurowych Microsoft zawierają zobowiązania do zapewnienia zgodności z RODO z chwilą wejścia Rozporządzenia w życie.

- **Dzielenie się naszym doświadczeniem**. Będziemy dzielić się z Państwem doświadczeniami z naszych działań do zapewnienia zgodności z RODO, aby szukając najlepszej drogi dla swojej organizacji mogli Państwo wykorzystać to, czego my się już nauczyliśmy.

Początek pracy nad zapewnieniem zgodności z RODO

Podejście do RODO z wykorzystaniem platformy informatycznej

Systemy wykorzystywane przez Państwa do tworzenia, przechowywania, analizowania i zarządzania danymi obejmują szeroką gamę środowisk informatycznych – urządzenia osobiste, serwery lokalne (*on-premises*), usługi chmurowe, czy nawet Internet Rzeczy. Oznacza to, że większość Państwa rozwiązań informatycznych może podlegać wymaganiom RODO.

Państwa działania mające na celu spełnienie wymagań RODO najlepiej rozpocząć od holistycznej analizy wymagań w kontekście wszystkich Państwa obowiązków regulacyjnych i prawnych w zakresie ochrony danych osobowych. Na przykład, wiele spośród mechanizmów zabezpieczających mających na celu zapobieganie, wykrywanie i reagowanie na luki w systemach zabezpieczeń i naruszenia ochrony danych osobowych wymaganych na mocy RODO jest podobnych do mechanizmów zabezpieczających wymaganych w świetle innych standardów ochrony danych osobowych, takich jak standard dotyczący ochrony danych osobowych w chmurze ISO/IEC 27018.

Zamiast śledzenia mechanizmów zabezpieczających wymaganych przez poszczególne standardy lub regulacje osobno, najlepsza praktyka polega na zidentyfikowaniu całego zbioru mechanizmów i funkcji zabezpieczających zapewniających spełnienie tych wymagań. Dlatego, zamiast dokonywania oceny poszczególnych technologii i rozwiązań pod kątem spełnienia wymagań tak kompleksowej regulacji jak RODO, lepszym podejściem może być oparcie się na platformie – obejmującej Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure i Dynamics 365 – celem łatwiejszego zapewnienia zgodności nie tylko z RODO, ale również spełnienia innych ważnych dla Państwa wymagań.

Zalecamy rozpoczęcie drogi do zapewnienia zgodności z RODO od czterech kluczowych kroków:

- **Inwentaryzacja danych –** identyfikacja, jakie dane osobowe Państwo posiadają i gdzie są one przechowywane.
- **Zarządzanie –** określenie, w jaki sposób dane osobowe są wykorzystywane i udostępniane.
- **Ochrona –** wprowadzenie mechanizmów zabezpieczających mających na celu zapobieganie, wykrywanie i reagowanie na luki w systemach zabezpieczeń i naruszenia ochrony danych osobowych.
- **Raportowanie –** podejmowanie działań w odpowiedzi na wnioski o udostępnienie danych, raportowanie naruszeń ochrony danych osobowych oraz prowadzenie niezbędnej dokumentacji.

Dla każdego z tych kroków podaliśmy przykładowe narzędzia, zasoby i funkcje oferowane przez poszczególne rozwiązania Microsoft, które można wykorzystać celem spełnienia wymagań wynikających z danego kroku. Niniejszy dokument nie stanowi kompleksowej instrukcji wskazującej szczegółowo „jak należy to zrobić", więc podajemy link pozwalający uzyskać bardziej szczegółowe informacje: Microsoft.com/GDPR.

Biorąc pod uwagę zakres potencjalnych zadań z rozpoczęciem przygotowań nie należy czekać do momentu wejścia w życie RODO. Powinni Państwo już teraz dokonać przeglądu stosowanych praktyk w zakresie ochrony i zarządzania danymi osobowymi.

W następnych rozdziałach przedstawiono poszczególne elementy każdego komponentu RODO i opisano, w jaki sposób można korzystać z produktów i usług oferowanych dzisiaj przez Microsoft, aby rozpocząć działania

Działania, które można podjąć już dzisiaj

Inwentaryzacja danych: identyfikacja posiadanych i miejsca ich przechowywania

Pierwszym krokiem w kierunku zapewnienia zgodności z RODO jest dokonanie oceny, czy RODO dotyczy Państwa organizacji oraz, jeżeli tak jest, w jakim zakresie. Ta analiza rozpoczyna się od zrozumienia, jakie dane Państwo posiadają i gdzie są one przechowywane.

Czy RODO dotyczy moich danych?

RODO reguluje gromadzenie, przechowywanie, wykorzystywanie i udostępnianie „danych osobowych". Definicja danych osobowych według RODO jest bardzo szeroka i obejmuje *wszelkie* dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Jeżeli Państwa organizacja posiada takie dane – w bazach danych na temat klientów, w formularzach służących do zbierania opinii wypełnianych przez Państwa klientów, w treści wiadomości przesyłanych pocztą elektroniczną, na zdjęciach, na nagraniach dokonanych za pomocą telewizji przemysłowej, w ewidencji programów lojalnościowych, bazach danych działu kadr, lub gdziekolwiek indziej – lub pragnie je gromadzić, oraz jeżeli dane należą lub dotyczą rezydentów UE, wówczas muszą Państwo zapewnić zgodność z RODO. Należy zauważyć, że dane osobowe nie muszą być przechowywane na terenie UE, aby podlegać wymaganiom RODO – RODO dotyczy danych gromadzonych, przetwarzanych lub przechowywanych poza UE, o ile dane te są powiązane z rezydentami UE.

Inwentaryzacja danych

Aby zrozumieć, czy RODO rzeczywiście *dotyczy* Państwa organizacji oraz, jeżeli tak jest, jakie obowiązki nakłada, ważne jest przeprowadzenie inwentaryzacji danych Państwa organizacji. To pomoże Państwu zrozumieć, jakie dane są osobowe oraz zidentyfikować systemy, w których te dane są gromadzone i przechowywane, zrozumieć, dlaczego zostały zgromadzone, w jaki sposób są przetwarzane i udostępniane oraz jak długo są zachowywane.
Poniżej podano konkretne przykłady, jak nasze rozwiązania chmurowe i lokalne (*on-premises*) mogą Państwu pomóc zrealizować pierwszy krok na drodze do zapewnienia zgodności z RODO.

Azure

Azure jako otwarta i elastyczna platform chmurowa, obejmuje usługę ułatwiającą inwentaryzację i identyfikowanie źródeł danych. Microsoft Azure Data Catalog to w pełni zarządzana usługa chmurowa pełniąca rolę systemu rejestracji i systemu inwentaryzacji źródeł danych w Państwa organizacji. Innymi słowy, zadaniem Azure Data Catalog jest pomoc Państwu w odkrywaniu, rozumieniu i użytkowaniu źródeł danych celem lepszego wykorzystania możliwości zapewnianych przez posiadane dane. Po zarejestrowaniu źródła danych w Azure Data Catalog, jego metadane są indeksowane przez tę usługę, aby ułatwić Państwu przeszukiwanie celem odkrycia danych, których Państwo potrzebują.

Dynamics 365

Dynamics 365 zapewnia szereg funkcji w zakresie wyświetlania (podglądu, wizualizacji) i kontroli (audytu) danych, z których można korzystać za pomocą kokpitów menedżerskich do raportowania i analityki systemu Dynamics 365 celem identyfikowania danych osobowych:

- Dynamics 365 obejmuje Report Wizard, z którego można korzystać celem łatwego tworzenia raportów bez konieczności korzystania z zapytań XML, czy SQL.
- Dashboards in Dynamics 365 zapewnia podgląd danych biznesowych – informacji na podstawie których można podejmować określone działania i które są dostępne do podglądu w skali całej organizacji.
- Microsoft Power BI to samoobsługowa platforma business intelligence (BI), z której można korzystać celem inwentaryzowania, analizowania i wizualizacji danych oraz ich udostępniania lub współpracowania na ich podstawie z kolegami.

Pakiet Enterprise Mobility + Security (EMS)

Pakiet Enterprise Mobility + Security obejmuje technologie w zakresie bezpieczeństwa oparte na tożsamości, ułatwiające odkrywanie, kontrolowanie i ochronę danych osobowych przechowywanych przez Państwa organizację, jak również ujawnianie potencjalnych słabych punktów i wykrywanie przypadków naruszeń danych osobowych.

Microsoft Cloud App Security to kompleksowa usługa zapewniająca bardziej szczegółowy podgląd, kompleksową kontrolę i lepszą ochronę danych w Państwa aplikacjach chmurowych. Można obejrzeć podgląd informacji o tym, które aplikacje chmurowe są wykorzystywane w Państwa sieci — identyfikujących ponad 13 000 aplikacji używanych przez wszystkie urządzenia – oraz uzyskać oceny ryzyka i bieżące dane analityczne.

Microsoft Azure Information Protection pomaga w identyfikacji, które Państwa dane są wrażliwe i gdzie są przechowywane. Można albo wprowadzać zapytania dotyczące danych oznaczonych określonym poziomem wrażliwości lub w sposób inteligentny identyfikować dane wrażliwe w momencie tworzenia pliku lub wiadomości poczty elektronicznej. Po zidentyfikowaniu można automatycznie klasyfikować i etykietować dane—zgodnie z pożądaną polityką firmy.

Office 365

Dostępnych jest szereg rozwiązań Office 365 ułatwiających identyfikowanie lub zarządzanie dostępem do danych osobowych:

- Data Loss Prevention (DLP) w ramach Office i Office 365 umożliwia identyfikację ponad 80 powszechnie używanych typów danych wrażliwych w tym danych finansowych, medycznych i informacji umożliwiających jednoznaczną identyfikację określonych osób.
- Content search w ramach Office 365 Security & Compliance Center umożliwia przeszukiwanie skrzynek pocztowych, publicznych folderów, Office 365 Groups, Microsoft Teams, stron SharePoint Online, lokalizacji One Drive for Business oraz konwersacji Skype for Business.
- Funkcja przeszukiwania Office 365 eDiscovery może być wykorzystywana do wyszukiwania tekstów i metadanych w treści we wszystkich Państwa aktywach Office 365 – SharePoint Online, OneDrive for Business, Skype for Business Online oraz Exchange Online.

- Office 365 Advanced eDiscovery, rozwiązanie oparte na technologii sztucznej inteligencji, ułatwia szybkie identyfikowanie dokumentów dotyczących określonego tematu (na przykład, prowadzonego śledztwa w sprawie zachowania zgodności z przepisami), przy zapewnieniu większej dokładności niż tradycyjne wyszukiwania na podstawie kluczowych słów, czy ręczne przeglądanie dużych ilości dokumentów. Advanced eDiscovery może znacząco obniżyć koszt i nakład prac potrzebnych do zidentyfikowania stosownych powiązań pomiędzy dokumentami, a danymi przy wykorzystania sztucznej inteligencji do uczenia systemu inteligentnego przeszukiwania dużych zbiorów danych oraz szybkiego wskazywania tych danych, które są istotne – co pozwala zmniejszyć ilość danych przed rozpoczęciem ich szczegółowego przeglądu.
- Advanced Data Governance wykorzystuje inteligencję i generowane za pomocą maszyn wnioski ułatwiające wyszukiwanie, klasyfikowanie, wprowadzanie procedur oraz podejmowanie działań mających na celu zarządzanie cyklem istnienia danych, które są najważniejsze dla Państwa organizacji.

SharePoint

Aplikację SharePoint Search Service oraz jej funkcję wyszukiwania można wykorzystywać do śledzenia danych osobowych. Do identyfikowania i wyszukiwania treści wrażliwych, SharePoint Server 2016 zapewnia taką samą funkcjonalność w zakresie zapobiegania utracie danych, co pakiet Office 365.

SQL Server i Azure SQL Database

Język SQL może być wykorzystywany do kierowania zapytań do baz danych oraz indywidualizowania narzędzi lub usług, które ułatwią realizację tej funkcji. Wyszukiwanie jest w pełni realizowane za pomocą zapytań, chociaż pełne rejestrowanie podejmowanych działań powinno być wykonywane na poziomie aplikacji. Narzędzie do tworzenia skryptów Script task pozwala na napisanie kodu służącego do realizacji zadań spełniających indywidualne wymagania użytkowników, takich jak złożone zapytania kierowane do zbiorów danych, które nie są dostępne w ramach wbudowanych zadań i transformacji zapewnianych przez SQL Server Integration Services. Narzędzie Script task umożliwia również połączenie funkcji w ramach jednego skryptu zamiast korzystania z wielu zadań i transformacji. Ten pakiet produktów obejmuje również zapewniającą bogate możliwości funkcjonalność business intelligence, pozwalającą użytkownikom końcowym na uzyskanie dostępu do wniosków wyciąganych na podstawie gromadzonych danych.

Windows i Windows Server

Do wyszukiwania danych w środowisku Windows można wykorzystywać narzędzie Windows Search umożliwiające śledzenie i lokalizowanie danych osobowych na maszynie lokalnej i wszelkich połączonych urządzeniach do których można uzyskać dostęp na podstawie posiadanych odpowiednich uprawnień. Aby rozszerzyć funkcjonalność narzędzia Windows Search o możliwość lokalizowania docelowych danych, należy skonfigurować opcje indeksacji (Indexing Options) na panelu sterowania (Control Panel) celem zindywidualizowania funkcjonalności narzędzia Windows Search (na przykład, indeksując zawartość plików).

Zarządzanie: określenie, w jaki sposób dane osobowe są wykorzystywane i udostępniane

RODO zapewnia osobom, których dane dotyczą większą kontrolę nad tym, w jaki sposób ich dane osobowe są rejestrowane i wykorzystywane. Osoba, której dane dotyczą może na przykład zwrócić się do Państwa organizacji o udostępnienie danych, które jej dotyczą, przesłania jej danych do innych usług, poprawienia błędów jej danych lub wyłączenia określonych danych z dalszego przetwarzania w określonych przypadkach. W niektórych przypadkach na wnioski te odpowiedzi muszą być udzielane w ustalonym terminie.

Zarządzanie danymi

Aby wypełnić swoje obowiązki wobec osób, których dane dotyczą muszą Państwo najpierw zrozumieć, jakie rodzaje danych osobowych są przetwarzane przez Państwa organizację, w jaki sposób i w jakim celu. Opisana wcześniej inwentaryzacja danych stanowi pierwszy krok do osiągnięcia takiego zrozumienia. Po zakończeniu inwentaryzacji ważnym zadaniem jest stworzenie i wdrożenie planu zarządzania danymi. Plan zarządzania danymi może ułatwić Państwu zdefiniowanie procedur, ról i obowiązków związanych z zapewnieniem dostępu, zarządzaniem i wykorzystaniem danych osobowych oraz pomóc Państwu w zapewnieniu zgodności stosowanych przez Państwa praktyk w zakresie przetwarzania danych z RODO. Na przykład, plan zarządzania danymi może dać Państwa organizacji pewność, że w sposób skuteczny spełniają Państwo wysuwane przez osoby, których dane dotyczą żądania usunięcia lub przesłania ich danych.

Usługi w chmurze firmy Microsoft

Aby zapewnić wsparcie Państwa strategii zarządzania danymi Microsoft rozwija usługi chmurowe stosując metodologię Microsoft Privacy-by-Design (ochrona danych na etapie projektowania) i Privacy-by-Default (domyślna ochrona danych). Kiedy powierzają Państwo swoje dane systemom Azure, Office 365, czy Dynamics 365, w dalszym ciągu pozostają Państwo ich jedynym właścicielem: zachowując prawa, tytuł i udziały w danych przechowywanych przy wykorzystaniu poszczególnych usług.

Oferowane przez Microsoft usługi chmurowe zapewniają mocne mechanizmy ułatwiające Państwu ochronę danych Państwa klientów przed nieodpowiednim dostępem lub wykorzystaniem przez osoby nieupoważnione, zgodnie ze szczegółowym opisem podanym w Microsoft Trust Center. Mechanizmy te obejmują ograniczenie dostępu personelu i podwykonawców Microsoft do danych oraz staranne zdefiniowanie wymagań w zakresie reagowania na wnioski organów administracji państwowej dotyczących udostępnienia danych klientów. Jednakże, mogą Państwo uzyskać dostęp do swoich własnych danych klientów w dowolnej chwili i w dowolnym celu.

Ponadto, przekierowujemy wnioski organów administracji państwowej dotyczące Państwa danych bezpośrednio do Państwa, o ile nie jest to prawnie zabronione i w przeszłości odwoływaliśmy się do sądu sprzeciwiając się podejmowanym przez organy administracji państwowej próbom zakazania ujawniania takich wniosków.

Aby zapewnić właściwe zarządzanie oferowanymi przez Microsoft usługami chmurowymi oraz udzielić naszym klientom zapewnień w tym zakresie, usługi chmurowe są audytowane przynajmniej raz w roku pod kątem zgodności z szeregiem globalnych standardów w zakresie ochrony danych osobowych, w tym HIPAA i HITECH, CSA Star Registry oraz szeregiem standardów ISO. Raporty te są dostępne na: https://servicetrust.microsoft.com/Documents/ComplianceReports.

Poza powyższymi zobowiązaniami zapewniamy Państwu niezbędną kontrolę nad sposobem zarządzania danymi oraz nad tym, kto ma dostęp do jakich danych w ramach Państwa organizacji.

Azure

Azure Active Directory to rozwiązanie w zakresie zarządzania tożsamością i dostępem w chmurze. Zarządza tożsamościami i kontroluje dostęp do platformy Azure, systemów lokalnych i innych zasobów chmurowych, danych oraz aplikacji. Za pomocą narzędzia Azure Active Directory Privileged Identity Management można przyznawać uprawnionym użytkownikom tymczasowe, prawa administracyjne Just-In-Time (JIT) do zarządzania zasobami na platformie Azure.

Azure Role-Based Access Control (RBAC) ułatwia zarządzanie dostępem do Państwa zasobów na platformie Azure. Umożliwia Państwu przyznawanie praw dostępu w zależności od roli przypisanej danemu użytkownikowi, ułatwiając przyznawanie wyłącznie niezbędnych uprawnień, potrzebnych poszczególnym użytkownikom do wykonywania ich zadań. Istnieje możliwość dostosowania narzędzia RBAC do indywidualnych wymagań wynikających z modelu biznesowego Państwa organizacji oraz stopnia tolerancji ryzyka.

Office 365

Rozwiązania Office 365 zapewniają szereg funkcji ułatwiających zarządzanie Państwa danymi osobowymi:

- Funkcje w zakresie zarządzania danymi dostępne w ramach Office 365 Security & Compliance Center ułatwiają archiwizację i zachowanie treści w skrzynkach pocztowych systemu Exchange Online, na stronach SharePoint Online i w lokalizacjach OneDrive for Business oraz importowanie danych do Office 365.
- Funkcja Retention systemu Office 365 ułatwia zarządzanie cyklem istnienia poczty elektronicznej i dokumentów poprzez zachowywanie potrzebnych Państwu treści oraz usuwanie stosownych treści, kiedy nie są już potrzebne.
- Advanced Data Governance wykorzystuje mechanizmy sztucznej inteligencji i wnioskowanie maszynowe ułatwiające wyszukiwanie, klasyfikowanie, wprowadzanie procedur oraz podejmowanie działań mających na celu zarządzanie cyklem istnienia danych, które są najważniejsze dla Państwa organizacji.
- Procedury w zakresie zarządzania informacją dostępne w ramach SharePoint Online umożliwiają kontrolowanie, jak długo poszczególne treści mają być zachowywane, sprawdzanie (audyt) co poszczególne osoby robią z treścią oraz przypisywanie dokumentom kodów kreskowych lub etykiet.
- Funkcja dziennika (journaling) w systemie Exchange Online ułatwia spełnienie wymagań w zakresie zachowania zgodności z przepisami prawa, regulacjami i zasadami organizacyjnymi poprzez rejestrowanie przychodzącej i wychodzącej komunikacji realizowanej za pomocą poczty elektronicznej.

Klasyfikacja danych

Klasyfikacja danych stanowi ważną część każdego planu zarządzania danymi. Przyjęcie systemu klasyfikacji obejmującego całą organizację może okazać się szczególnie przydatne w przypadku odpowiadania na wnioski osób, których dane dotyczą, ponieważ umożliwia Państwu łatwiejszą identyfikację i przetwarzanie wniosków dotyczących danych osobowych.
Oferujemy wskazówki i narzędzia ułatwiające Państwu poradzenie sobie ze złożonością procesu klasyfikacji danych.

Azure

Opracowanie Data Classification zawiera określone wskazówki dotyczące klasyfikacji danych na platformie Azure i szczegółowy opis zasad, na których oparte są techniki, proces, terminologia i wdrożenie klasyfikacji danych. Dokumentacja zawiera bogaty zbiór innych informacji i linków.

Dynamics 365

Przewodnik planowania w zakresie bezpieczeństwa i zapewnienia zgodności z obowiązującymi przepisami w systemie Dynamics 365 (online) zawiera wyczerpujące wskazówki pozwalające na zrozumienie kluczowych aspektów dotyczących zapewnienia zgodności z obowiązującymi przepisami i bezpieczeństwa przy planowaniu wdrożenia systemu Dynamics 365 (online) w środowiskach obejmujących usługi integracji katalogów przedsiębiorstwa (enterprise directory integration), takie jak synchronizacja katalogów (directory synchronization) oraz pojedyncze logowanie (single sign-on). Zawiera także informacje na temat procedur w zakresie ochrony i poufności danych osobowych, klasyfikacji danych oraz skutków dla ochrony danych.

Enterprise Mobility + Security (EMS)

Azure Information Protection ułatwia klasyfikowanie i etykietowanie danych z chwilą ich stworzenia lub modyfikacji. Następnie dane wrażliwe mogą zostać poddane działaniom ochronnym (szyfrowanie plus uwierzytelnianie plus prawa do wykorzystywania) lub oznakowane wizualnie. Etykiety klasyfikacyjne i działania ochronne mają charakter trwały, poruszają się wraz z danymi i dzięki temu dane przez cały czas mogą być zidentyfikowane i chronione – bez względu na to, gdzie są przechowywane, czy komu są udostępniane.

Office i Office 365

- Data Loss Prevention (DLP) w ramach Office i Office 365 umożliwia identyfikację ponad 80 powszechnie używanych typów danych wrażliwych w tym danych finansowych, medycznych i informacji umożliwiających identyfikację osób. Ponadto, DLP pozwala organizacjom na konfigurowanie działań, które należy podjąć po zidentyfikowaniu danych, celem zapewnienia ochrony informacji wrażliwych oraz zapobieżenia ich przypadkowemu ujawnieniu.
- Advanced Data Governance wykorzystuje inteligencję i generowane za pomocą maszyn wnioski ułatwiające wyszukiwanie, klasyfikowanie, wprowadzanie procedur oraz podejmowanie działań mających na celu zarządzanie cyklem istnienia danych, które są najważniejsze dla Państwa organizacji. Klasyfikuje dane na podstawie automatycznej analizy i zalecanej polityki, następnie podejmuje działania mające na celu zachowanie danych lub usunięcie tego, co jest konieczne.

Dane zachowane w danej lokalizacji, jak również zewnętrzne źródła danych można wprowadzić na platformę Office 365 oraz sklasyfikować według typu wiadomości. Klasyfikacja według typu wiadomości pozwala na przeszukiwanie, porządkowanie i eksportowanie poszczególnych źródeł danych, co ułatwia proces realizacji przeglądów e-discovery.

Windows i Windows Server

Microsoft Data Classification Toolkit dla Windows Server 2012 R2 zapewnia przykładowe wyszukiwane zwroty i reguły, które mogą Państwo wykorzystywać w celu ułatwienia realizacji działań związanych z zapewnieniem zgodności z obowiązującymi przepisami i prowadzonych przez informatyków z Państwa organizacji, audytorów, księgowych, prawników i innych specjalistów w zakresie zapewnienia zgodności z obowiązującymi przepisami.

Ochrona: wprowadzenie mechanizmów zabezpieczających, mających na celu zapobieganie, wykrywanie i reagowanie na luki w systemach zabezpieczeń i naruszenia ochrony danych osobowych

Organizacje sącoraz bardziej świadome znaczenia bezpieczeństwa informacji - ale RODO podnosi poprzeczkę. Wymaga od organizacji podejmowania odpowiednich działań technicznych i organizacyjnych w celu zapewnienia ochrony danych osobowych przed utratą, nieuprawnionym dostępem lub ujawnieniem.

Ochrona danych osobowych

Bezpieczeństwo danych to złożone zagadnienie. Wymaga zidentyfikowania rozważenia wielu rodzajów zagrożeń - poczynając od fizycznego włamania lub pracownika-oszusta po przypadkową utratę lub hakerów. Tworzenie planów zarządzania ryzykiem oraz podejmowanie kroków mających na celu obniżenie ryzyka, takich jak zabezpieczenie za pomocą hasła, rejestry rewizyjne (audit logs) i szyfrowanie, mogą ułatwić zapewnienie zgodności z obowiązującymi przepisami.

Oferowana przez Microsoft chmura została zaprojektowana tak, aby pomóc Państwu zrozumieć zagrożenia i bronić się przed nimi, a przy tym pod wieloma względami jest bardziej bezpieczna niż lokalne środowiska przetwarzania danych. Na przykład, nasze centra przetwarzania danych są certyfikowane zgodnie z międzynarodowymi standardami w zakresie bezpieczeństwa; są objęte fizycznym nadzorem (monitoringiem) przez 24 godziny na dobę oraz zapewniają ścisłą kontrolę dostępu. Sposób, w jaki zabezpieczamy naszą infrastrukturę chmurową, stanowi tylko część kompleksowego rozwiązania w zakresie bezpieczeństwa, a każdy z naszych produktów, zarówno chmurowych, jak i lokalnych, jest wyposażony w mechanizmy zabezpieczające mające za zadanie ochronę Państwa danych.

Azure

Następujące usługi i narzędzia Azure pomogą ochronić Państwa dane osobowe w środowisku chmurowym:

- Azure Security Center zapewnia podgląd i kontrolę nad bezpieczeństwem Państwa zasobów Azure. Stale monitoruje zasoby i zapewnia przydatne rekomendacje dotyczące bezpieczeństwa. Umożliwia zdefiniowanie procedur dotyczących Państwa subskrypcji Azure i grup zasobów z uwzględnieniem wymagań firmy w zakresie bezpieczeństwa, rodzajów wykorzystywanych aplikacji oraz wrażliwości Państwa danych. Wykorzystuje rekomendacje w zakresie bezpieczeństwa wynikające z procedur w celu procesie wdrażania niezbędnych zabezpieczeń — na przykład: uruchomienia oprogramowania do wykrywania i usuwania oprogramowania złośliwego (antimalware) lub szyfrowania dysków dla Państwa zasobów. Security Center pomaga także szybko uruchamiać usługi i urządzenia zabezpieczające oferowane przez Microsoft i partnerów celem wzmocnienia ochrony Państwa środowiska chmurowego.

- Szyfrowanie danych w Azure zabezpiecza dane w spoczynku i podczas przesyłania. Przykładowo, mogą Państwo automatycznie zaszyfrować swoje dane w momencie ich zapisywania w Azure Storage, korzystając z narzędzia Storage Service Encryption. Ponadto, mogą Państwo korzystać z narzędzia Azure Disk Encryption celem szyfrowania systemów operacyjnych i dysków danych wykorzystywanych przez maszyny wirtualne Windows i Linux. Dane są zabezpieczone podczas przesyłania pomiędzy aplikacją a platformą Azure tak, aby zawsze były dobrze zabezpieczone.
- Azure Key Vault umożliwia zabezpieczenie kluczy kryptograficznych, certyfikatów i haseł, które pomagają chronić Państwa dane. Narzędzie Key Vault wykorzystuje sprzętowe moduły zabezpieczające (hardware security modules – HSM) i zostało zaprojektowane w taki sposób, aby zachowali Państwo kontrolę nad swoimi kluczami i co za tym idzie nad swoimi danymi, w tym, aby uniemożliwić Microsoft zobaczenie lub pobranie Państwa kluczy. Mogą Państwo monitorować i kontrolować użycie swoich zapisanych kluczy korzystając z funkcji rejestrowania platformy Azure i importując swoje rejestry do Azure HDInsight lub do swojego systemu SIEM (security information and event management) w celu przeprowadzenia dodatkowej analizy i wykrycia zagrożeń.
- Microsoft Antimalware for Azure Cloud Services and Virtual Machines to bezpłatna, działająca w czasie rzeczywistym funkcja zabezpieczająca, która pomaga identyfikować i usuwać wirusy, programy szpiegujące (spyware) i inne oprogramowanie złośliwe mające na celu kradzież danych, za pomocą konfigurowalnych alarmów informujących o podejmowanych przez znane złośliwe lub niepożądane oprogramowanie próbach zainstalowania się lub uruchomienia w Państwa systemach na platformie Azure.

Dynamics 365

Można wykorzystywać strategie bezpieczeństwa systemu Dynamics 365 dla zapewnienia spójności i ochrony danych w ramach organizacji Dynamics 365. Można połączyć jednostki biznesowe, zabezpieczenia na poziomie ról, zabezpieczenia na poziomie rekordów i zabezpieczenia na poziomie pól, w celuzdefiniowania ogólnych zasad dostępu do informacji posiadanych przez użytkowników Dynamics 365.

- Zabezpieczenia na poziomie ról w Dynamics 365 pozwalają na grupowanie zbioru uprawnień ograniczających zadania, które może wykonać dany użytkownik. Jest to ważna funkcjonalność, w szczególności, gdy poszczególne osoby zmieniają role pełnione w ramach organizacji.
- Zabezpieczenia na poziomie rekordów w Dynamics 365 pozwalają na ograniczenie dostępu do określonych rekordów.
- Zabezpieczenia na poziomie pól w Dynamics 365 pozwalają na ograniczenie dostępu do określonych istotnych pól, takich jak pola zawierające informacje umożliwiające identyfikację osób.

Enterprise Mobility + Security (EMS)

W większości przypadków naruszeń danych osobowych, napastnicy uzyskują dostęp do sieci korporacyjnej za pomocą słabych, domyślnych lub skradzionych danych uwierzytelniających użytkownika. Nasze podejście do bezpieczeństwa rozpoczyna się od ochrony tożsamości przy wejściu do systemu poprzez zastosowanie dostępu warunkowego z uwzględnieniem ryzyka.

- Azure Active Directory (Azure AD) w ramach Enterprise Mobility + Security pomaga zapewnić ochronę Państwa organizacji na poziomie dostępu poprzez zarządzanie i ochronę tożsamości – w tym tożsamości uprzywilejowanych i nieuprzywilejowanych. Azure AD zapewnia jedną zabezpieczoną, wspólną tożsamość umożliwiającą uzyskanie dostępu do tysięcy aplikacji. Azure AD Premium zapewnia mechanizm Multi-Factor Authentication (MFA), czyli kontrolę dostępu w zależności od stanu urządzenia, lokalizacji użytkownika, tożsamości i ryzyka zalogowania oraz holistycznych raportów na temat bezpieczeństwa, audytów i alarmów. Azure AD Privileged Identity Management (PIM) pomaga wykrywać, ograniczać i monitorować uprzywilejowane tożsamości oraz ich dostęp do zasobów za pomocą kreatora zabezpieczeń (security wizard), przeglądów i alarmów. To umożliwia realizację takich scenariuszy jak ograniczony czasowo dostęp "just in time" i "just enough administration".

Enterprise Mobility + Security zapewnia szczegółowy podgląd aktywności użytkownika, urządzenia i danych w systemach lokalnych i w chmurze oraz pomaga chronić Państwa dane za pomocą silnych mechanizmów zabezpieczających..

- Azure Information Protection pomaga rozszerzyć kontrolę nad Państwa danymi na cały okres istnienia danych - od stworzenia i zapisania w systemach lokalnych i w usługach chmurowych, poprzez ich udostępnianie wewnątrz lub na zewnątrz firmy, monitorowanie dystrybucji plików, aż po reagowanie na nieoczekiwane działania.
- Cloud App Security zapewnia szczegółowy podgląd i silne mechanizmy zabezpieczające wykorzystywane przez Państwa pracowników oprogramowanie na zasadzie usługi (software as a service – SaaS) i aplikacje chmurowe, co pozwala uzyskać pełny kontekst i rozpocząć szczegółowe kontrolowanie danych na poziomie poszczególnych użytkowników.
- Microsoft Intune zapewnia funkcjonalność w zakresie zarządzania urządzeniami mobilnymi, aplikacjami mobilnymi i komputerami PC z poziomu chmury. Za pomocą Intune, mogą Państwo zapewnić swoim pracownikom dostęp do aplikacji, danych i zasobów firmy praktycznie z dowolnego miejsca za pomocą prawie każdego urządzenia, przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa informacji firmy.

Office i Office 365

Platforma Office 365 zapewnia bezpieczeństwo na każdym poziomie, poczynając od rozwoju aplikacji, poprzez fizyczne centra przetwarzania danych, aż po użytkowników końcowych. Aplikacje platformy Office 365 zapewniają zarówno wbudowane mechanizmy bezpieczeństwa, co upraszcza proces zabezpieczenia danych, jak i elastyczność pozwalającą konfigurować, zarządzać i zintegrować zabezpieczenia w sposób, który spełnia wyjątkowe potrzeby Państwa firmy. Mechanizmy w zakresie zapewnienia zgodności z obowiązującymi przepisami platformy Office 365 obejmują ponad 1 000 elementów zabezpieczających, które umożliwiają nam zachowanie na bieżąco zgodności Office 365 ze zmieniającymi się standardami obowiązującymi na rynku, w tym ponad 50 certyfikatami lub poświadczeniami zgodności.

Wiele mechanizmów zabezpieczających jest dostępnych automatycznie (domyślnie). Na przykład, zarówno SharePoint, jak i OneDrive for Business wykorzystują szyfrowanie danych podczas przesyłania i w spoczynku. Ponadto, mogą Państwo konfigurować i stosować certyfikaty cyfrowe celem maskowania danych osobowych oraz korzystać z mechanizmów zabezpieczających Office Access w celu przyznawania i ograniczania dostępu do danych osobowych. Office 365 oferuje inne mechanizmy pomagające zabezpieczyć dane i identyfikować, kiedy ma miejsce naruszenie danych osobowych:

- Secure Score zapewnia dostęp do informacji na temat stanu Państwa bezpieczeństwa oraz wskazuje dostępne zabezpieczenia pozwalające na obniżenie ryzyka przy jednoczesnym zachowaniu równowagi pomiędzy poziomem wydajności systemów, a poziomem ich bezpieczeństwa.
- Advanced Threat Protection (ATP) dla Exchange Online pomaga zapewnić ochronę poczty elektronicznej przed atakami ze strony złośliwego oprogramowania w czasie rzeczywistym. Pozwala tworzyć procedury, które pomagają zapobiegać uzyskiwaniu przez użytkowników dostępu do przesyłanych pocztą elektroniczną złośliwych załączników lub witryn internetowych. ATP dla Exchange Online obejmuje zabezpieczenie przed nieznanym oprogramowaniem i wirusami, ochronę w chwili kliknięcia (time-of-click) przed złośliwymi URL-ami oraz bogatą funkcjonalność w zakresie raportowania i śledzenia URL.
- Information Rights Management (IRM) pomaga Państwu i Państwa użytkownikom zapobiegać drukowaniu, przesyłaniu, zapisywaniu, edytowaniu lub kopiowaniu wrażliwych informacji przez osoby nieupoważnione. Korzystając z IRM w SharePoint Online można ograniczyć działania, jakie użytkownicy mogą podejmować w stosunku do plików, które zostały załadowane z list lub bibliotek, takie jak drukowanie kopii plików lub kopiowanie z nich tekstu. Korzystając z IRM w Exchange Online można pomóc zapobiegać wyciekaniu przez pocztę elektroniczną, w trybie online i offline, informacji wrażliwych zawartych w wiadomościach przesyłanych pocztą elektroniczną i załącznikach.
- Mobile Device Management (MDM) na platformie Office 365 pozwala konfigurować procedury i reguły pomagające zabezpieczyć i zarządzać zarejestrowanymi iPhonami, iPadami, urządzeniami systemu Android i telefonami Windows Państwa użytkowników. Na przykład, można zdalnie usunąć urządzenie i uzyskać podgląd szczegółowych raportów na temat poszczególnych urządzeń. Na platformie Office 365, w celu zapewnienia dodatkowego zabezpieczenia, wykorzystuje się także uwierzytelnianie wielopoziomowe (multi-factor authentication).

SQL Server i Azure SQL Database

SQL Server i Azure SQL Database zapewniają mechanizmy zabezpieczające służące do zarządzania dostępem do bazy danych i uprawnieniami na wielu poziomach:

- Zapora ogniowa Azure SQL Database ogranicza dostęp do poszczególnych baz danych w ramach serwera Azure SQL Database poprzez ograniczenie dostępu wyłącznie do uprawnionych połączeń. Można tworzyć reguły zapory ogniowej na poziomie serwera i bazy danych, określając zakresy IP, z których połączenia są dozwolone.
- Uwierzytelnienie SQL Server pomaga zapewnić, aby wyłącznie uprawnieni użytkownicy posiadający aktualne dane uwierzytelniające mogli uzyskać dostęp do Państwa serwera bazodanowego. SQL Server zapewnia obsługę zarówno uwierzytelnienia w systemie Windows, jak i loginów SQL Server. Uwierzytelnienie w systemie Windows zapewnia zintegrowany system zabezpieczeń i jest zalecane jako bardziej bezpieczna opcja, gdzie proces uwierzytelnienia jest całkowicie zaszyfrowany. Azure SQL Database zapewnia obsługę uwierzytelnienia Azure Active Directory, które oferuje funkcjonalność pojedynczego logowania i jest realizowane w przypadku domen zarządzanych i zintegrowanych.

- Autoryzacja SQL Server umożliwia zarządzanie uprawnieniami według zasady najniższego poziomu uprawnień. W SQL Server i SQL Database wykorzystywany jest mechanizm zabezpieczeń na poziomie ról, który obsługuje kontrolę uprawnień dostępu do danych na poziomie poszczególnych użytkowników poprzez zarządzanie mechanizmami role memberships i object-level permissions.
- Dynamic data masking (DDM) to wbudowana funkcjonalność, która może być wykorzystywana do ograniczenia wycieku danych wrażliwych poprzez maskowanie danych w przypadku uzyskiwania do nich dostępu przez użytkowników lub aplikacje nie posiadające stosownych uprawnień. Określone pola danych są na bieżąco („w locie") maskowane w odsyłanych odpowiedziach na zapytania, natomiast dane w bazie danych pozostają niezmienione. Konfiguracja DDM jest prosta i nie wymaga zmian w aplikacji. W przypadku użytkowników Azure SQL Database, funkcja dynamicznego maskowania danych może automatycznie odkrywać potencjalnie wrażliwe dane i proponować zastosowanie odpowiednich masek.
- Row-level security (RLS) (zabezpieczenie na poziomie rzędów) to dodatkowa wbudowana funkcjonalność umożliwiająca klientom korzystającym z SQL Server i SQL Database wprowadzanie ograniczeń dostępu do rzędów danych. Mechanizm RLS może być wykorzystywany w celu umożliwienia dostępu na poziomie poszczególnych użytkowników do rzędów w tablicy bazy danych, co pozwala uzyskać większą kontrolę nad tym, którzy użytkownicy mogą uzyskać dostęp, do których danych. Ze względu na fakt, że układy logiczne ograniczające dostęp znajdują się na poziomie bazy danych funkcjonalność ta znacznie upraszcza projekt i wdrożenie zabezpieczenia aplikacji.

SQL Server i SQL Database oferują bogaty zbiór wbudowanych funkcji zapewniających ochronę danych i sygnalizację przypadków naruszenia ochrony danych osobowych:

- Transparentne szyfrowanie danych zabezpiecza dane w spoczynku poprzez szyfrowanie bazy danych, powiązanych kopii zapasowych oraz plików rejestrów transakcji na poziomie warstwy fizycznych układów pamięci masowej. To szyfrowanie jest transparentne z punktu widzenia aplikacji oraz wykorzystuje rozwiązania przyspieszające realizowane na poziomie sprzętowym celem podniesienia poziomu wydajności pracy aplikacji.
- Transport Layer Security (TLS) zabezpiecza dane w ruchu - przesyłane połączeniami SQL Database.
- Always Encrypted to pierwsze takie rozwiązanie dostępne na rynku, którego zadaniem jest ochrona wysoce wrażliwych danych w SQL Server i SQL Database. Always Encrypted pozwala stacjom klienckim szyfrować dane wrażliwe wewnątrz aplikacji klienckich i nigdy nie ujawniać kluczy szyfrowania silnikowi bazy danych (database engine). Mechanizm jest transparentny z punktu widzenia aplikacji, gdyż szyfrowanie i rozszyfrowywanie danych jest realizowane w sposób transparentny w sterowniku stacji klienckiej obsługującym funkcję Always Encrypted.
- Auditing for SQL Database i SQL Server audit śledzą zdarzenia dotyczące bazy danych i zapisują je w rejestrze rewizyjnym (audit log). Funkcja audytu umożliwia zrozumienie bieżących działań dotyczących bazy danych, jak również analizowanie i badanie działań historycznych celem zidentyfikowania potencjalnych zagrożeń lub zweryfikowania podejrzenia wystąpienia nadużyć i naruszeń bezpieczeństwa.
- SQL Database Threat Detection wykrywa anomalie w działaniach dotyczących bazy danych, wskazując potencjalne zagrożenia dla bezpieczeństwa bazy danych. Threat Detection wykorzystuje zaawansowany zbiór algorytmów celem ciągłego uczenia się i profilowania zachowania aplikacji oraz zawiadamia o nietypowych lub podejrzanych działaniach bezzwłocznie po ich wykryciu. Threat Detection może pomóc Państwu spełnić wymaganie RODO dotyczące powiadamiania o naruszeniach ochrony danych osobowych.

Windows i Windows Server

Windows 10 i Windows Server 2016 zawierają najlepsze na rynku technologie szyfrowania, oprogramowanie do wykrywania i usuwania oprogramowania złośliwego (antimalware) oraz rozwiązania do kontroli tożsamości i dostępu, które umożliwiają Państwu przejście od haseł do bardziej bezpiecznych sposobów uwierzytelniania:

- Windows Hello to wygodna, przeznaczona dla dużych przedsiębiorstw (enterprise-grade) alternatywa dla haseł, wykorzystująca naturalną (biometryczną) lub znaną (PIN) metodę weryfikacji tożsamości, zapewniająca zalety kart inteligentnych (smartcards) w zakresie bezpieczeństwa bez konieczności stosowania dodatkowych urządzeń peryferyjnych.
- Windows Defender Antivirus to silne rozwiązanie typu antimalware, gotowe od razu (out of the box) do pracy, aby pomóc Państwu zachować bezpieczeństwo. Windows Defender Antivirus zapewnia szybkie wykrywanie i ochronę przed nowo powstającym oprogramowaniem złośliwym (malware) oraz może pomóc w bezzwłocznym zabezpieczeniu Państwa urządzeń, kiedy po raz pierwszy zostanie zaobserwowane zagrożenie w jakiejkolwiek części Państwa środowiska.
- Device Guard pozwala na zablokowanie Państwa urządzeń i serwerów celem zabezpieczenia przed nowymi i nieznanymi odmianami oprogramowania złośliwego oraz atakami typu APT (advanced persistent threats). W odróżnieniu od rozwiązań nastawionych na wykrywanie zagrożeń, takich jak programy antywirusowe wymagające ciągłej aktualizacji celem wykrywania najnowszych zagrożeń, Device Guard blokuje urządzenia, aby mogły obsługiwać wyłącznie uprawnione, wybrane przez Państwa aplikacje, co stanowi skuteczny sposób zwalczania oprogramowania złośliwego.
- Credential Guard to funkcja izolująca i zabezpieczająca Państwa tajemnice na urządzeniu, takim jak tokeny do pojedynczego logowania (single sign-on), przed dostępem, nawet w przypadku całkowitego złamania bezpieczeństwa systemu operacyjnego Windows. To rozwiązanie w zasadzie zapobiega stosowaniu trudnych do obrony (hard-to-defend) ataków, takich jak "pass the hash."
- BitLocker Drive Encryption w Windows 10 i Windows Server 2016 zapewnia spełniające wymagania dużych przedsiębiorstw (enterprise-grade) szyfrowanie, które pomaga zabezpieczyć Państwa dane w przypadku zgubienia lub kradzieży urządzenia. BitLocker całkowicie szyfruje dysk komputera i pamięci flash celem zapobiegania uzyskiwaniu dostępu do Państwa danych przez nieuprawnionych użytkowników.
- Windows Information Protection przejmuje zadanie zapewnienia bezpieczeństwa od miejsca, w którym swoją pracą kończy BitLocker. Podczas gdy BitLocker zabezpiecza cały dysk urządzenia, Windows Information Protection chroni dane przed uruchamianiem nieuprawnionych użytkowników i aplikacji na maszynie. Ponadto, pomaga zapobiegać przeciekom danych z dokumentów biznesowych do dokumentów nie związanych z działalnością firmy albo do lokalizacji w Internecie.
- Shielded Virtual Machines pozwalają na wykorzystanie narzędzia BitLocker do szyfrowania dysków i maszyn wirtualnych (virtual machine - VM) pracujących w środowisku Hyper-V, celem zapobiegania atakom na treści znajdujące się na zabezpieczonych maszynach wirtualnych (VM) ze strony administratorów, których zabezpieczenia zostały złamane lub administratorów złośliwych.
- Just Enough Administration i Just in Time Administration pozwala administratorom na wykonywanie swoich normalnych zadań i działań, przy jednoczesnym umożliwienia Państwu ograniczenia zakresu funkcjonalności i czasu pracy administratorów nad danym projektem. W przypadku złamania danych uwierzytelniających zakres potencjalnych szkód ulega znaczącemu ograniczeniu. Ta technika zapewnia administratorom jedynie taki poziom dostępu, jaki jest im niezbędny w okresie pracy nad danym projektem.

Wykrywanie naruszeń bezpieczeństwa danych i reagowanie na nie

W określonych sytuacjach RODO wymaga, aby w przypadku wystąpienia naruszenia ochrony danych osobowych, organizacje musiały szybko powiadamiać regulatorów. W niektórych przypadkach organizacje będą musiały również powiadamiać osoby, których dane dotyczą, a których ochrona danych została naruszona. Aby spełnić to wymaganie przydatna dla organizacji będzie możliwość monitorowania i wykrywania włamań do systemu.

Dla zdarzeń, w przypadku których ponosimy część lub całą odpowiedzialność za podjęcie stosownych działań, stworzyliśmy szczegółowe procesy Security Incident Response Management, które zostały opisane w odniesieniu do platform Azure i Office 365.

Ponadto, wyjaśniamy, w jaki sposób współpracujemy z naszymi klientami w ramach modelu Shared Responsibility Model opisanego w opracowaniu: Shared Responsibilities in Cloud Computing.

Po wykryciu potencjalnego naruszenia, zalecamy zastosowanie procesu obejmującego cztery kroki, który stosujemy również w ramach naszego własnego programu reagowania na zdarzenia:

- Ocena skutków i stopnia zagrożenia stwarzanego przez dane zdarzenie. W zależności od dowodów ocena może lub nie prowadzić do dalszej eskalacji i przekazania sprawy do zespołu reagującego Cybersecurity / Data Protection.
- Przeprowadzenie dochodzenia technicznego lub kryminalistycznego oraz zidentyfikowanie strategii ograniczenia szkód, zmniejszenia skutków i obejścia problemu (workaround). Jeżeli zespół Cybersecurity / Data Protection uzna, że dane osobowe mogły zostać ujawnione w sposób nielegalny lub osobie nieuprawnionej, wówczas równolegle rozpoczyna się proces powiadamiania, o którym jest mowa w RODO.
- Opracowanie planu przywrócenia stanu sprzed naruszenia celem zmniejszenia skutków problemu. Kroki mające na celu ograniczenie szkód spowodowanych przez kryzys, takie jak kwarantanna dotkniętych systemów, powinny być podejmowane bezzwłocznie i równolegle do działań mających na celu zdiagnozowanie problemu.Warto także planować działania mające na celu zmniejszenie skutków problemu w dłuższej perspektywie, które zostaną wykonane po ustąpieniu bezpośredniego zagrożenia.
- Sporządzenie analizy post-mortem, zawierającej szczegółowy opis zdarzenia, którego celem będzie weryfikacja polityki, procedur i procesów mających na celu zapobieżenie ponownemu wystąpieniu danego zdarzenia. Ten etap jest zgodny z Artykułem 31 RODO mówiącym o zarejestrowaniu faktów związanych z naruszeniem ochrony danych osobowych, jego skutków oraz podjętych działań naprawczych.

Azure

Ochrona danych osobowych w Państwa systemach oraz raportowanie i weryfikowanie pod kątem zgodności z obowiązującymi przepisami stanowią kluczowe wymagania RODO. Następujące usługi i narzędzia dostępne na platformie Azure pomogą Państwu spełnić obowiązki wynikające z RODO:

- Usługi zintegrowane z platformą Azure umożliwiają szybsze i łatwiejsze zrozumienie ogólnej metodologii w zakresie utrzymania bezpieczeństwa jak również wykrywanie i badanie zagrożeń dla środowiska chmurowego. Azure Security Center wykorzystuje zaawansowane narzędzia w zakresie analityki bezpieczeństwa. Przełomowe technologie w zakresie analizy dużych zbiorów danych (big data) i sztucznej inteligencji (machine learning) są wykorzystywane do oceny zdarzeń w skali całej matrycy chmury – do wykrywania zagrożeń, które byłyby niemożliwe do zidentyfikowania przy zastosowaniu metod ręcznych oraz przewidywania ewolucji ataków. Wspomniane narzędzia w zakresie analityki bezpieczeństwa obejmują:

    - Zintegrowany wywiad dotyczący zagrożeń, który pozwala wyszukiwać znanych złych „aktorów" przy wykorzystaniu globalnego wywiadu dotyczącego zagrożeń tworzonego przez produkty i usługi oferowane przez Microsoft, Microsoft Digital Crimes Unit (DCU), Microsoft Security Response Center (MSRC) oraz z wykorzystaniem danych pozyskiwanych ze źródeł zewnętrznych.
    - Analityka behawioralna, w ramach której do wykrywania zachowań złośliwych wykorzystywane są znane prawidłowości (schematy) zachowań.
    - Wykrywanie anomaliów, które wykorzystuje profilowanie statystyczne celem budowania opartego na danych historycznych scenariusza bazowego (baseline). Sygnalizuje odchylenia od ustalonych scenariuszy bazowych, które są zgodne z wektorem potencjalnego ataku.

Ponadto, Security Center generuje alarmy bezpieczeństwa, z uwzględnieniem ich poziomu priorytetu, które zapewniają Państwu wgląd w dane dotyczące kampanii ataku, w tym powiązane zdarzenia i zaatakowane zasoby.

- Azure Log Analytics zapewnia konfigurowalne opcje audytowania i rejestrowania działań w zakresie bezpieczeństwa, które pomagają gromadzić i analizować dane generowane przez zasoby znajdujące się zarówno w Państwa środowisku chmurowym, jak i lokalnym. Zapewnia wgląd w dane w czasie rzeczywistym przy wykorzystaniu zintegrowanych narzędzi do wyszukiwania i zindywidualizowanych kokpitów menedżerskich, celem łatwego analizowania milionów rekordów w skali wszystkich realizowanych zadań i serwerów, bez względu na ich fizyczną lokalizację. Ułatwia szybkie reagowanie i gruntowne badanie dowolnych zdarzeń dotyczących bezpieczeństwa.

Dynamics 365

Regularnie serwisujemy i uaktualniamy system Dynamics 365 (za pośrednictwem sieci) celem zapewnienia bezpieczeństwa, wydajności i dostępności systemu oraz wprowadzania nowych mechanizmów i funkcji. Ponadto, okresowo reagujemy na zdarzenia występujące w trakcie eksploatacji. W przypadku każdego takiego działania, administrator systemu Dynamics 365 w Państwa organizacji, otrzymuje zawiadomienia pocztą elektroniczną. W przypadku zdarzenia występującego w trakcie eksploatacji przedstawiciel zajmujący się obsługą klientów korzystających z systemu Dynamics 365 (online) może również zadzwonić i prowadzić dalszą korespondencję w tej sprawie za pośrednictwem poczty elektronicznej. Szczegółowe informacje na temat naszych procedur i komunikacji dotyczącej systemu Dynamics 365 są dostępne na TechNet.

Enterprise Mobility +Security (EMS)

Nasz kompleksowy wywiad dotyczący zagrożeń wykorzystuje najnowsze technologie w zakresie analityki behawioralnej i wykrywania anomalii celem wykrywania podejrzanych działań oraz namierzania zagrożeń – zarówno w systemach lokalnych (on-premises), jak i w chmurze. Działanie te obejmują znane ataki złośliwe (takie jak Pass the Hash, Pass the Ticket) i luki bezpieczeństwa w Państwa systemie. Mogą Państwo podejmować bezzwłoczne działania kierowane przeciwko wykrytym ataków oraz optymalizować proces przywracania stanu sprzed naruszenia korzystając z zapewniającego bogate możliwości wparcia. Uzupełnieniem naszego wywiadu dotyczącego zagrożeń jest narzędzie Microsoft Intelligent Security Graph, zasilane dużą liczbą zbiorów danych i wspomagane technologią sztucznej inteligencji (machine learning) w chmurze:

- Microsoft Advanced Threat Analytics (ATA) to produkt przeznaczony do zastosowań lokalnych (on-premises), mający za zadanie zapewnienie pomocy specjalistom w zakresie bezpieczeństwa systemów informatycznych w zabezpieczeniu ich organizacji przed zaawansowanymi, nakierowanymi atakami poprzez automatyczne analizowanie, uczenie się i identyfikowanie normalnego i nienormalnego zachowania obiektu (użytkownika, urządzeń i zasobów). ATA identyfikuje ataki typu APT (Advanced Persistent Threats) w danej lokalizacji, wykrywając podejrzane zachowanie użytkownika i obiektu (urządzeń i zasobów), korzystając z technologii sztucznej inteligencji (machine learning) oraz informacji przechowywanych w lokalnych systemach Active Directory, SIEM i rejestrach zdarzeń Windows Events. Wykrywa również znane ataki złośliwe (takie jak Pass the Hash). Wreszcie, zapewnia prostą chronologię ataku, zawierającą jasne i istotne informacje na temat ataku, aby mogli Państwo szybko skoncentrować się na tym, co jest ważne.
- Cloud App Security zapewnia zabezpieczenie przed zagrożeniami dla Państwa aplikacji chmurowych, uzupełnione oferowanym przez Microsoft bogatym wywiadem i badaniami dotyczącymi zagrożeń. Umożliwia zidentyfikowanie użytkowania stwarzającego wysoki poziom ryzyka, zdarzeń zagrażających bezpieczeństwu i wykrywanie nienormalnych zachowań użytkowników celem zapobiegania zagrożeniom. Dostępne w ramach Cloud App Security zaawansowane, oparte na technologii sztucznej inteligencji techniki heurystyczne uczą się, w jaki sposób każdy użytkownik korzysta z każdej aplikacji SaaS oraz dzięki analizie zachowań (behawioralnej), dokonują oceny ryzyk związanych z każdą transakcją. Do takich nietypowych zachowań należą: jednoczesne logowanie się w dwóch krajach, nagłe pobranie terabajtów danych lub wielokrotne, nieudane próby zalogowania się, które mogą oznaczać brutalny, siłowy atak na system.

- Azure Active Directory (Azure AD) Premium zapewnia wykrywanie zagrożeń na poziomie tożsamości w chmurze. Azure AD monitoruje korzystanie z aplikacji oraz zabezpiecza Państwa firmę przed zaawansowanymi zagrożeniami dzięki raportowaniu i monitorowaniu stanu bezpieczeństwa. Raporty na temat dostępu i użytkowania zapewniają podgląd spójności (nienaruszalności) i bezpieczeństwa katalogu Państwa organizacji. Ponadto, Azure AD zapewnia ochronę tożsamości za pomocą powiadomień, analizy i zalecanych środków naprawczych.

Office i Office 365

Platforma Office 365 zapewnia szereg funkcji, które pomagają Państwu zidentyfikować i zareagować, kiedy nastąpi naruszenie ochrony danych osobowych:

- Threat Intelligence pomaga proaktywnie odkrywać i chronić przed zaawansowanymi zagrożeniami na platformie Office 365. Szczegółowa wiedza na temat zagrożeń—dostępna częściowo dzięki globalnej skali działalności Microsoft, narzędziu Intelligent Security Graph, oraz informacjom dostarczanym przez osoby śledzące cyber zagrożenia (cyber threat hunters) – pomagają szybko i skutecznie uruchamiać alarmy, dynamiczne procedury i rozwiązania w zakresie bezpieczeństwa.
- Advanced Security Management umożliwia zidentyfikowanie użytkowania stwarzającego wysoki poziom ryzyka i nienormalnych zachowań, sygnalizując Państwu potencjalne naruszenia. Ponadto, pozwala na skonfigurowanie procedur dotyczących działań mających na celu śledzenie i reagowanie na czynności stwarzające wysoki poziom ryzyka i podejrzane postępowanie. Można użyć narzędzia do wykrywania wydajności aplikacji, które pozwala Państwu korzystać z informacji znajdujących się w plikach rejestrów Państwa organizacji celem zrozumienia i podejmowania działań na podstawie sposobu użytkowania aplikacji przez użytkowników na platformie Office 365 i innych aplikacji chmurowych.
- Advanced Threat Protection for Exchange Online pomaga zapewnić ochronę poczty elektronicznej przed atakami ze strony nowego, wyrafinowanego oprogramowania złośliwego w czasie rzeczywistym. Pozwala również tworzyć procedury, które pomagają zapobiegać uzyskiwaniu przez użytkowników dostępu do złośliwych załączników lub witryn internetowych przesyłanych pocztą elektroniczną.

SQL Server i Azure SQL Database

SQL Server i SQL Database zapewniają bogaty zbiór wbudowanych funkcji sygnalizujących, kiedy wystąpi naruszenie ochrony danych osobowych:

- Auditing for SQL Database i SQL Server audit śledzą zdarzenia dotyczące bazy danych i zapisują je w rejestrze rewizyjnym (audit log). Audyt umożliwia zrozumienie bieżących działań dotyczących bazy danych, jak również analizowanie i badanie działań historycznych celem zidentyfikowania potencjalnych zagrożeń lub zweryfikowania podejrzenia wystąpienia nadużyć i naruszeń bezpieczeństwa.
- SQL Database Threat Detection wykrywa anomalie w działaniach dotyczących bazy danych, wskazując potencjalne zagrożenia dla bezpieczeństwa bazy danych. Threat Detection wykorzystuje zaawansowany zbiór algorytmów celem ciągłego uczenia się i profilowania zachowania aplikacji oraz zawiadamia o nietypowych lub podejrzanych działaniach bezzwłocznie po ich wykryciu. Threat Detection może pomóc Państwu spełnić wymaganie RODO dotyczące powiadamiania o naruszeniach ochrony danych osobowych.

Windows i Windows Server

Windows Defender Advanced Threat Protection (ATP) umożliwia Państwu wykrywanie, badanie, ograniczanie szkód i reagowanie na naruszenia ochrony danych osobowych w Państwa sieci. Dzięki Windows Defender ATP uzyskują Państwo dostęp do zaawansowanej funkcjonalności w zakresie wykrywania naruszeń, badania i reagowania - obejmującej Państwa wszystkie urządzenia końcowe - wraz z maks. 6 miesiącami danych historycznych, nawet wtedy, kiedy urządzenia końcowe nie są podłączone do sieci (*offline*), znajdują się poza domeną sieci, obraz ich oprogramowania został zmieniony lub już nie istnieją. Windows Defender ATP pomaga Państwu spełnić wymaganie RODO dotyczące jasnych procedur w zakresie wykrywania, badania i raportowania naruszeń ochrony danych osobowych.

Raportowanie: podejmowanie działań w odpowiedzi na wnioski o udostępnienie danych, raportowanie naruszeń danych osobowych oraz prowadzenie niezbędnej dokumentacji

RODO wyznacza nowe standardy w zakresie przejrzystości, rozliczalności i ewidencji. Będą Państwo musieli działać w sposób bardziej transparentny w zakresie nie tylko przetwarzania danych osobowych, ale również sposobu aktywnego prowadzenia dokumentacji definiującej stosowane przez Państwa procesy i wykorzystanie danych osobowych.

Ewidencja

Organizacje przetwarzające dane osobowe będą musiały prowadzić ewidencję w zakresie celów przetwarzania; kategorii przetwarzanych danych osobowych, tożsamości osób trzecich, którym udostępniane są dane, czy (i które) inne kraje otrzymują dane osobowe oraz podstawy prawnej takiego przekazywania danych, działań organizacyjnych i technicznych związanych z bezpieczeństwem oraz terminów zachowywania danych dotyczących poszczególnych zbiorów danych. Jednym ze sposobów na osiągnięcie tego celu jest korzystanie z narzędzi do audytowania, które mogą pomóc w zapewnieniu, aby wszelkie przetwarzanie danych – bez względu na to, czy jest to gromadzenie, wykorzystywanie, udostępnianie lub inne – było śledzone i rejestrowane.
W ramach usług chmurowych Microsoft dostępne są usługi w zakresie audytowania, które mogą pomóc Państwu spełnić ten standard.

Azure, Office 365 i Dynamics 365

Na portalu Service Trust Portal można znaleźć wyczerpujące informacje na temat poszczególnych rozwiązań Azure, Office 365 i Dynamics 365 w zakresie zapewnienia zgodności z obowiązującymi przepisami, bezpieczeństwa, ochrony danych osobowych i powiezenia danych, w tym raportów i poświadczeń (certyfikatów) zgodności. Sporządzane przez osoby trzecie, niezależne raporty z audytu i raporty na temat oceny ładu korporacyjnego (zarządzania), zarządzania ryzykiem i zapewnienia zgodności z obowiązującymi przepisami (GRC – governance, risk management, compliance) pomagają Państwu otrzymywać aktualne informacje na temat zgodności usług chmurowych Microsoft z globalnymi standardami, które są istotne dla Państwa organizacji. Dokumenty dostępne na portalu mogą pomóc Państwu zrozumieć, w jaki sposób usługi chmurowe Microsoft zabezpieczają Państwa dane oraz w jaki sposób mogą Państwo zarządzać bezpieczeństwem danych i zapewnieniem zgodności z obowiązującymi przepisami Państwa usług chmurowych.

Azure

Audytowanie i rejestrowanie zdarzeń dotyczących bezpieczeństwa oraz powiązanych z nimi alarmów stanowią ważne elementy skutecznej strategii w zakresie bezpieczeństwa danych.
Funkcjonalność platformy Azure w zakresie rejestrowania i audytowania umożliwia Państwu:

- Tworzenie ścieżki rewizyjnej dla aplikacji uruchamianych na platformie Azure i maszyn wirtualnych tworzonych za pomocą Azure Virtual Machines Gallery.
- Wykonywanie scentralizowanej analizy dużych zbiorów danych poprzez gromadzenie zdarzeń dotyczących bezpieczeństwa pobieranych z infrastruktury Azure funkcjonującej jako usługa (IaaS) i platformy funkcjonującej jako usługa (PaaS). Następnie za pomocą narzędzia Azure HDInsight można agregować i analizować te zdarzenia oraz eksportować je do lokalnych systemów SIEM celem bieżącego monitorowania.
- Monitorowanie raportów na temat dostępu i użytkowania poprzez wykorzystywanie rejestrowania przez platformę Azure działań administracyjnych, w tym dostępu do systemu, celem tworzenia ścieżki rewizyjnej na wypadek nieuprawnionych lub przypadkowych zmian. Mogą Państwo pobierać rejestry rewizyjne (audit logs) dotyczące użytkownika Azure Active Directory oraz korzystać z podglądu raportów na temat dostępu i użytkowania.
- Eksportowanie alarmów bezpieczeństwa do lokalnych systemów SIEM za pomocą narzędzia Azure Diagnostics, które może zostać skonfigurowane do gromadzenia rejestrów zdarzeń dotyczących bezpieczeństwa w systemie Windows oraz innych rejestrów związanych z bezpieczeństwem.
- Pozyskiwanie za pomocą platformy Azure Marketplace, oferowanych przez inne firmy, narzędzi w zakresie monitorowania bezpieczeństwa, raportowania i alarmowania.

Microsoft Azure Monitor zapewnia organizacjom łatwy podgląd i zarządzanie wszystkimi zadaniami w zakresie monitorowania danych za pomocą centralnego kokpitu menedżerskiego. Uzyskują Państwo dostęp do szczegółowych, aktualnych danych na temat wydajności i wykorzystania zasobów, dostęp do rejestru działań, który śledzi każde wywołanie API oraz rejestrów diagnostycznych, które pomagają śledzić problemy pojawiające się w Państwa zasobach na platformie Azure. Ponadto, można konfigurować alarmy i podejmować zautomatyzowane działania. Azure Monitor współpracuje z Państwa dotychczas używanymi narzędziami, więc w wyniku połączenia Azure Monitor z już Państwu znanymi narzędziami analitycznymi, uzyskają Państwo bogatą, kompleksową (end-to-end) funkcjonalność w zakresie monitorowania i analityki.

Office i Office 365

- Service Assurance w ramach Office 365 Security & Compliance Center zapewnia Państwu dostęp do dogłębnej wiedzy potrzebnej do przeprowadzania ocen ryzyka, obejmującej szczegółowe informacje na temat raportów Microsoft na temat zgodności z obowiązującym przepisami i transparentny status zaudytowanych mechanizmów kontrolnych, w tym:
  - Stosowane przez Microsoft praktyki w zakresie bezpieczeństwa danych klientów przechowywanych na platformie Office 365.
  - Sporządzane przez osoby trzecie niezależne raporty z audytu platformy Office 365.
  - Szczegółowe dane na temat wdrożenia i testowania zabezpieczeń, ochrony danych osobowych i mechanizmów kontroli zgodności z obowiązującymi przepisami, które pomagają klientom zapewnić zgodność ze standardami, przepisami prawa i regulacjami dotyczącymi rożnych branż, takimi jak ISO 27001 i ISO 27018, jak również z ustawą Health Insurance Portability and Accountability Act (HIPAA).
- Rejestry rewizyjne (audit logs) Office 365 pozwalają na monitorowanie i śledzenie działań użytkowników i administratorów w przekroju poszczególnych zadań realizowanych na platformie Office 365, co pomaga wcześniej wykrywać i badać problemy dotyczące bezpieczeństwa i zapewnienia zgodności z obowiązującymi przepisami. Aby rozpocząć rejestrowanie działań użytkowników i administratorów w Państwa organizacji należy użyć strony wyszukiwania rejestru rewizyjnego Office 365. Po sporządzeniu rejestru rewizyjnego przez Office 365 można przeszukiwać ten rejestr celem wyszukiwania szerokiej gamy działań, w tym przesłań danych do OneDrive lub SharePoint Online lub resetów haseł użytkowników. Program Exchange Online można skonfigurować pod kątem śledzenia zmian wprowadzanych przez administratorów i w ten sposób śledzić, kiedy dostęp do skrzynki pocztowej uzyskuje ktoś inny niż osoba będąca właścicielem skrzynki pocztowej.
- Customer Lockbox zapewnia Państwu kontrolę nad sposobem uzyskiwania dostępu do Państwa danych przez inżyniera serwisowego Microsoft w trakcie sesji pomocy serwisowej. W przypadku, gdy inżynier potrzebuje uzyskać dostęp do Państwa danychw celu usunięcia usterek i rozwiązania problemu, narzędzie Customer Lockbox pozwala Państwu na zatwierdzenie lub odrzucenie wniosku o uzyskanie dostępu. Jeżeli Państwo zatwierdzą wniosek, wówczas inżynier może uzyskać dostęp do danych. Każdy wniosek ma termin wygaśnięcia, a kiedy problem zostanie rozwiązany, wniosek jest zamykany i prawo dostępu zostaje cofnięte.

Enterprise Mobility + Security (EMS)

Azure Information Protection zapewnia bogatą funkcjonalność w zakresie rejestrowania i raportowania w celu umożliwienia przeprowadzania analiz wskazujących, w jaki sposób są rozprowadzane dane wrażliwe. Funkcja śledzenia dokumentów pozwala użytkownikom i administratorom na monitorowanie działań dotyczących udostępnianych danych oraz cofanie praw dostępu w przypadku wystąpienia nieoczekiwanych zdarzeń. Azure Information Protection zapewnia również funkcjonalność w zakresie analizowania nieuporządkowanych danych przechowywanych na dyskach sieciowych, stronach i bibliotekach SharePoint, repozytoriach sieciowych oraz na dyskach komputerów stacjonarnych lub przenośnych. Mając dostęp do plików można skanować zawartość każdego pliku i zdecydować, czy określone klasy danych osobowych występują w pliku. Następnie można sklasyfikować i oznaczyć każdy plik etykietą w zależności od rodzaju zawartych w nim danych. Ponadto, można generować raporty na temat tego procesu, zawierające informacje na temat przeskanowanych plików, procedur klasyfikacyjnych, które okazały się zgodne z zawartością plików oraz zastosowanej etykiety.

Windows i Windows Server

Windows Event Log zapewnia bogatą funkcjonalność w zakresie rejestrowania, która umożliwia administratorom uzyskanie podglądu zarejestrowanych informacji na temat działań systemu operacyjnego, aplikacji i użytkowników. Ten system rejestrów można skonfigurować pod kątem audytu szczegółowych działań użytkowników i aplikacji, w tym, na przykład, dostępu do plików, użytkowania plików oraz zmian procedur. Ponadto, Windows Event Log umożliwia administratorom przekazywanie zdarzeń przesyłanych przez stacje klienckie i serwery do centralnej lokalizacji w celach związanych z raportowaniem i audytowaniem.

Narzędzia do raportowania i dokumentacja usług chmurowych

Podobnie jak w przypadku każdej innej bazy danych lub systemu przetwarzającego dane osobowe, korzystanie przez Państwa z usług chmurowych powinno być dobrze rejestrowane i dobrze rozumiane przez Państwa organizację. Na przykład, Państwa organizacja będzie musiała rozumieć rolę danych osobowych przechowywanych przez dostawców usług w imieniu Państwa organizacji; relację kontraktową dotyczącą współpracy z tymi dostawcami usług; oraz co się stanie z danymi, kiedy relacja usługowa się zakończy.
Pomagamy Państwu zarządzać tymi informacjami poprzez utrzymywanie prostych i jasnych narzędzi do raportowania na temat Państwa konta w chmurze Microsoft, wraz z bogatą dokumentacją na temat naszych usług chmurowych opisującą, w jaki sposób funkcjonują oraz na temat naszej kontraktowej relacji z Państwem.

Powiadamianie osób, których dane dotyczą

RODO zmieni wymagania w zakresie ochrony danych i wprowadzi bardziej restrykcyjne obowiązki dla podmiotów przetwarzających dane i administratorów danych w zakresie powiadamiania o naruszeniach ochrony danych osobowych skutkujących ryzykiem naruszenia praw i wolności osób fizycznych. Na mocy nowego rozporządzenia, zgodnie z Artykułami 17, 31 i 32, podmiot przetwarzający dane musi powiadomić administratora danych o każdym takim naruszeniu ochrony danych osobowych bez zbędnej zwłoki - po uzyskaniu informacji o takim fakcie.

Po uzyskaniu informacji o naruszeniu ochrony danych osobowych, administrator danych musi powiadomić stosowny organ nadzorczy w ciągu 72 godzin. Jeżeli naruszenie może powodować duże ryzyko naruszenia praw i wolności osób fizycznych, wówczas administratorzy danych będą również mieli obowiązek powiadomienia, bez zbędnej zwłoki, osoby, których dane dotycz.. Oznacza to, że jeżeli jako administrator danych, korzystają Państwo z usług podmiotu przetwarzającego dane, musice zapewnić w umowach jasno sformułowane oczekiwania dotyczące powiadomień o ewentualnych naruszeniach ochrony danych osobowych.

W odniesieniu do zdarzeń za które Microsoft ponosi część lub całą odpowiedzialność za podjęcie działań, opracowaliśmy szczegółowe procesy Incident Security Incident Response Management,opisane dla platform Azure, Office 365 i Dynamics 365. Ponadto, nasze zobowiązania wynikające z RODO znajdują potwierdzenie w naszych umowach.

Oferowane przez Microsoft produkty i usługi – takie jak Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 i Windows 10 – są już dzisiaj wyposażone w rozwiązania, które pomogą Państwu wykrywać i oceniać zagrożenia i naruszenia ochrony danych osobowych oraz spełnić wynikające z RODO obowiązki w zakresie powiadamiania o naruszeniach ochrony danych osobowych.

Obsługa wniosków osoby, której dane dotyczą

Do najważniejszych elementów RODO, należą prawa „osoby, której dane dotyczą" określone w artykułach rozdziału 2: Informacje i dostęp do danych osobowych, rozdziału 3: Sprostowanie i usunięcie danych, oraz rozdziału 4: Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach.

Powyższe obowiązki mogą wpływać na Państwa środowisko informatyczne i Państwa działalność jako administratora danych oraz na środowisko informatyczne a także na działalność dowolnych dostawców usług, których Państwo zaangażują w roli podmiotów przetwarzających dane.

Właściwe zarządzanie danymi stanowi kluczowy element przepisów prawa dotyczących ochrony danych osobowych i jest zalecane w większości przepisów prawa i regulacji (rozporządzeń) w zakresie zabezpieczenia danych i ochrony danych osobowych. Kluczowym elementem zarządzania danymi na mocy RODO, jest powołanie Inspektora Ochrony Danych (IOD) w szczególnych okolicznościach określonych w artykułach 35, 36 i 37. IOD musi być zaangażowany we wszystkie sprawy związane z ochroną danych osobowych.

Drugim ważnym elementem zarządzania danymi zgodnie RODO, jest przeprowadzenie weryfikacji zgodności z obowiązującymi przepisami w zakresie ochrony danych osobowych celem dokonania oceny skutków dla ochrony danych osobowych (DPIA) pod kierunkiem IOD. Artykuł 33a w szczególności mówi o wymogu przeprowadzenia przez administratora danych, w ciągu dwóch lat od dokonania oceny skutków dla ochrony danych osobowych, weryfikacji zgodności z obowiązującymi przepisami celem wykazania, że przetwarzanie danych osobowych jest realizowane zgodnie z oceną skutków dla ochrony danych osobowych (DPIA).

Microsoft Trust Center udostępnia informacje, w jaki sposób możemy zapewnić Państwu wsparcie na Państwa drodze do RODO, w tym rozdział specjalny przedstawiający poglądy i zobowiązania Microsoft dotyczące RODO.