Bezpieczeństwo danych w RODO a Polisa w Chmurze

Rozporządzenie o ochronie danych osobowych wprowadza nowe zasady gromadzenia i zarządzania danymi osobowymi obywateli UE przez firmy oferujące usługi i towary. Filary ochrony pozostają bez zmian, jednak RODO:

- zwiększa nacisk na bezpieczeństwo baz danych,

- poszerza katalog praw osób, których dane są przechowywane,

- nakłada nowe obowiązki na administratorów oraz kary za niewywiązanie się z nich.

Co to oznacza w praktyce i w jaki sposób Polisa w Chmurze odpowiada na te wymogi?

Polisa w Chmurze na Microsoft Azure

Polisa w Chmurze korzysta z technologii oferowanej przez Microsoft Azure, która zapewnia bezpieczeństwo procedury uwierzytelniania danych osoby, która loguje się do systemu. Bez trudu możemy też zarządzać uprawnieniami użytkowników i grup użytkowników, dzięki czemu bezpośredni dostęp do danych otrzymują tylko wybrane osoby, w zakresie ograniczonym do niezbędnego minimum.

Szyfrowanie protokołem TLS

Połączenia danych między klientami a centrami danych Microsoft są szyfrowane przy pomocy protokołu TLS (Transport Layer Security). Pozwala on na połączenie przeglądarki z serwerem o wzmocnionym bezpieczeństwie.

Bezpieczeństwo w centrach danych

Obsługa Polisy w Chmurze odbywa się w centrach danych wyposażonych w mechanizmy ochrony danych, w których nieautoryzowany ruch do i z baz danych jest automatycznie blokowany, a infrastruktura zabezpieczeń podlega nieustannym testom pod względem najwyższego poziomu bezpieczeństwa.

Monitoring bezpieczeństwa danych

Polisa w Chmurze zarówno w wersji w chmurze, jak i on-premise wyposażona jest w system monitorowania logowań, przepływu danych oraz ich statusu. Dzięki temu przy minimalnym nakładzie czasu pozwala wychwycić niepożądane zjawiska i zareagować na nie, np. ograniczając uprawnienia tych użytkowników, którzy nie postępują zgodnie z wytycznymi ochrony danych.

Kontrola nad danymi w RODO a Polisa w Chmurze

RODO będzie wymagało zagwarantowania obywatelom UE większej kontroli nad zebranymi informacjami na ich temat, czyli – funkcjonalnie – wdrożenia nowej polityki związanej z przechowywaniem danych osobowych. Konsument w każdej chwili będzie mógł zażądać pełnej

informacji o zakresie, celu i zarządcy danych, które go dotyczą, a także oczekiwać od administratora usunięcia jego danych z systemu i przekazania ich w celu np. przeniesienia do innego dostawcy usług.

Przejrzystość zarządzania danymi w Polisie w Chmurze

Polisa w Chmurze pozwala na zarządzanie rekordem danych w czasie rzeczywistym, przypisywanie mu celu i budowanie zamkniętych baz przeznaczonych do określonych działań. Odpowiedni poziom uprawnień umożliwia również na żądanie konsumenta dezaktywować określone drogi kontaktu z nim lub definitywnie usunąć jego dane z bazy.

RODO vs. Microsoft Azure

Microsoft Azure (chmura obliczeniowa, z której korzysta Polisa w Chmurze) jest skuteczną odpowiedzią na wymogi dotyczące gromadzenia i przetwarzania danych osobowych, które narzuci RODO. Pozwala na odpowiednie zabezpieczenie, klasyfikowanie i przetwarzanie danych osobowych zgodnie z wytycznymi dot. ich bezpieczeństwa. Umożliwia również zminimalizowanie ryzyka potencjalnych nadużyć oraz szybkie reagowanie w przypadku ich zaistnienia.

Microsoft został pierwszą na świecie firmą, która **uzyskała certyfikat zgodności** swoich usług **z normą ochrony danych osobowych** w chmurze ISO 27018.

Centra danych Microsoft, w których przechowywane są dane znajdują się na terenie państwa członkowskiego UE, gdzie zapewniony jest odpowiedni poziom ich ochrony. Szczegóły odnośnie poziomu bezpieczeństwa Microsoft Azure oraz zgodności z rozporządzeniami o ochronie danych GDPR (RODO) znaleźć można pod adresem: https://azure.microsoft.com/pl-pl/overview/trusted-cloud/