techstep

Techstep Essentials MDM

Przewodnik po RODO

Data: 18/10/2023

Spis treści

OPUBLIKOWANY PRZEZ:

Techstep Poland S.A.

Ul. Wajdeloty 12A

80-437 Gdańsk

1 Czym jest RODO?

GDPR (General Data Protection Regulation), w polskim prawodawstwie zwana RODO (Rozporządzenie o Ochronie Danych Osobowych) lub Ogólnym Rozporządzeniem o Ochronie Danych to Rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE1.

Unijne ogólne rozporządzenie o ochronie danych osobowych (RODO), które zacznie być bezpośrednio stosowane od 25 maja 2018 r., zobowiązuje administratorów danych do właściwego zabezpieczania danych osobowych.

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

art. 5 ust. 1 lit. f RODO

Każdy, kto przetwarza dane osobowe, musi więc wdrożyć – podobnie jak dotąd – odpowiednie środki techniczne i organizacyjne zabezpieczające dane osobowe, tak by uniemożliwić ich nieuprawnione udostępnienie, utratę czy uszkodzenie bądź zniszczenie.

2 Kiedy można przetwarzać dane osobowe?

Następujące sytuacje mogą być podstawą przetwarzania danych:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem

3 Rozwinięcie definicji danych osobowych

Jedną z głównych zmian w regulacjach dotyczących ochrony danych osobowych jest rozwinięcie definicji "danych osobowych". **Od tej chwili do zbioru danych osobowych należą także adresy IP, identyfikatory cookies, numery identyfikacyjne urządzeń mobilnych czy inne tego typu wirtualne identyfikatory.** Podobnie jak inne informacje mogące przyczynić się do identyfikacji tożsamości osoby (imię, nazwisko, data urodzenia, adres, dane biometryczne etc.) muszę one zostać objętą szczególną ochroną.

4 Kary

Rozporządzenie ujednolica oraz znacząco podwyższa kary finansowe za naruszenie przepisów o ochronie danych osobowych. Maksymalna wysokość kar przewidzianych w Rozporządzeniu jest wielokrotnie wyższa niż wysokość kar nakładanych obecnie przez GIODO. Sankcje mogą wynieść do 20.000.000 EUR lub do 4% całkowitego światowego obrotu za rok poprzedni za uchybienia w ochronie danych osobowych.

5 Wymagane standardy techniczne

RODO nie określa minimalnych standardów technicznych mających na celu zabezpieczenie danych ani nie podaje konkretnych przykładów najlepszych rozwiązań. Wskazuje jedynie, że:

- uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem – *art. 24 ust. 1,*
- jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa wyżej, powinny obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych – *art. 24 ust. 2*,
- należy regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Od 25 maja 2018 r. każdy administrator - biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych - będzie musiał samodzielnie zdecydować, jakie zabezpieczenia, dokumentację i procedury przetwarzania danych wdrożyć.

Jak stanowi art. 32 ust. 1 ogólnego rozporządzenia, administrator danych w zarządzaniu bezpieczeństwem przetwarzanych danych powinien uwzględnić stan wiedzy technicznej w zakresie zarządzania bezpieczeństwem danych w środowisku, w jakim przetwarza dane, oraz koszty wdrożenia i utrzymania zastosowanych środków. Przepis ten wskazuje również, że w stosownym przypadku środkami, które należy wdrożyć, aby złagodzić występujące ryzyko, tj. osiągnąć odpowiedni poziom bezpieczeństwa, powinny być:

- pseudoanonimizacja i szyfrowanie danych osobowych;
- środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

6 Zasady bezpieczeństwa, a urządzenia mobilne w przedsiębiorstwie

Stosowane zasady bezpieczeństwa powinny odnosić się do wszystkich urządzeń wykorzystywanych do przetwarzania danych, w tym do urządzeń mobilnych, z odpowiednim uwzględnieniem dodatkowych ryzyk, jakie są związane z mobilnością (zgubienie urządzenia, kradzież itp.).

W zależności od środowiska przetwarzania i celów odpowiednie polityki mogą przewidywać np. obowiązek szyfrowania danych przechowywanych na urządzeniach mobilnych, wyposażenia w nakładki polaryzujące na monitor, które utrudniają podgląd informacji pod kątem, czy wyposażenie w przycisk bezpieczeństwa, którego w przypadku zagrożenia można użyć w celu usunięcia lub zaszyfrowania aktualnie przetwarzanych informacji.

Administrator danych powinien również uwzględnić fakt, że coraz więcej pracowników używa dla celów służbowych swoich własnych urządzeń typu smartfony, tablety, a nawet laptopy, które jeśli chodzi o zainstalowane na nich systemy ochrony antywirusowej czy antywłamaniowej mogą znacznie odbiegać od tych udostępnianych służbowo, znajdujących się pod kontrolą administratora danych. Stąd powszechną praktyką wielu firm dopuszczających wykorzystywanie prywatnego sprzętu w celach służbowych stało się przygotowywanie specjalnych wytycznych dla pracowników.

7 W jaki sposób system Techstep Essentials MDM pozwala spełnić wymagania RODO?

7.1 Backup I archiwizacja

Backup i archiwizacja to jedne z podstawowych regulacji prawnych uwzględnionych w RODO. Właściciele firm niezależnie od tego, czy jest to firma państwowa czy prywatna, będą zobligowani do prowadzenia specjalnych rejestrów czynności przetwarzania, w których będzie musiał potwierdzić stosowanie polityki backupu i archiwizacji.

7.2 Integracja z infrastrukturą Wi-Fi

Dzięki integracji z infrastrukturą sieciową (m.in. Extreme Networks, Cisco, Checkpoint) Techstep Essentials MDM kontroluje dostęp do firmowych sieci Wi-Fi, pozwalając na dostęp jedynie zarządzanym i zgodnym z politykami bezpieczeństwa urządzeniom. Rozwiązanie takie stanowi dodatkową barierę zabezpieczającą dane przechowywane w sieci firmowej przed potencjalnym wykradaniem danych.

Dla aplikacji firm trzecich system Techstep Essentials MDM oferuje moduł External Compliance Checker, który pozwala dowolnemu rozwiązaniu IT na weryfikację poziomu bezpieczeństwa urządzenia mobilnego, które stara się o dostęp do danych. Jedynie urządzenia zaufane, spełniające odpowiednie polityki bezpieczeństwa, z wymuszonym szyfrowaniem danych, otrzymają pełen dostęp do zgromadzonych informacji.

7.3 Kontrola dostępu do danych z urządzeń mobilnych

Techstep Essentials MDM wraz z integracją Samsung KNOX pozwala na rozgraniczenie między prywatnymi danymi, a danymi korporacyjnymi przechowywanymi na urządzeniu mobilnym. Firma nie ma dostępu do plików i informacji zawartych w części prywatnej urządzenia.

Ponadto system Techstep Essentials MDM wymusza zaufany dostęp do usług biznesowych. Nieautoryzowane próby dostępu mogą zostać zablokowane.

Wykorzystując system Techstep Essentials MDM zabezpieczamy dostęp do informacji zintegrowanych z samym systemem Techstep Essentials MDM (np. Poczta firmowa, kalendarz itp.). Dzieję się to dzięki wykorzystaniu naszego rozwiązania do bezpiecznego dostępu do danych (Techstep Essentials VPN). Po zastosowaniu Techstep Essentials VPN dostęp do wszelkich danych firmowych jest w odpowiedni sposób kontrolowany.

7.4 Wsparcie w przypadku wystąpienia wycieku danych

Kolejną ważną zmianą jest konieczność zgłaszania bez zwłoki (w ciągu 72h po stwierdzeniu naruszenia) incydentu związanego z wyciekiem danych do organu

nadzorczego (Urzędu Ochrony Danych Osobowych, który zastąpi Generalny Inspektorat Ochrony Danych Osobowych).

Tutaj również swoje zastosowanie ma system Techstep Essentials MDM. Zbiera on logi, które pozwalają zidentyfikować nieprawidłowości i podjąć natychmiastowo odpowiednie działania. Innym przykładem jest umożliwienie użytkownikom błyskawicznego zgłoszenia faktu zgubienia lub kradzieży urządzenia mobilnego przez system Techstep Essentials MDM oraz prewencyjne zdalne wyczyszczenia danych z urządzenia.

System Techstep Essentials MDM wysyła ponadto alerty w przypadku wykrycia instalacji złośliwego oprogramowania, wykrycia jailbreaka lub zrootowanego urządzenia, braku zgodności z polityką bezpieczeństwa.

Dodatkowo zabezpiecza potencjalnie wrażliwe dane na smartfonach i tabletach poprzez możliwość automatycznego usunięcia danych w przypadku wykrycia zagrożenia (np. kilkukrotne wpisanie niepoprawnego hasła, wymiana karty SIM czy brak łączności z serwerem MDM przez dłuższy czas)