JAK SAFETICA ZAPEWNIA ZGODNOŚĆ Z RODO

safetica

SPIS TREŚCI

WPROWADZENIE

Czym jest RODO?

RODO to rozporządzenie Unii Europejskiej nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. RODO weszło w życie w całej Unii 25 maja 2018 r. Zastąpiło ono zarówno dyrektywę 95/46/ES, jak i przepisy dotyczące ochrony danych osobowych obowiązujące w całej Unii w każdym państwie UE.

Najważniejsze wymogi RODO

- Ustanowienie podstawy prawnej dla przetwarzania danych osobowych.
- Określenie celu przetwarzania danych osobowych.
- Ustalenie odpowiedniego okresu przechowywania danych oraz praw dostępu do danych osobowych.
- Prowadzenie dokumentacji dotyczącej przetwarzania danych.
- Zapewnienie bezpieczeństwa danych osobowych.
- Wygenerowanie kompletnej dokumentacji wszystkich procedur organizacyjnych, które mogą być wykorzystywane jako wytyczne dla użytkowników i które posłużą jako punkt wyjścia podczas incydentu bezpieczeństwa.
- Szkolenie pracowników w zakresie wszystkich procesów związanych z danymi organizacyjnymi oraz bezpiecznej pracy z poufnymi danymi.
- Zapewnienie przestrzegania praw wszystkich osób, których dane dotyczą.
- W pewnych warunkach wyznaczenie inspektora ochrony danych.
- Ocena skutków (DPIA) (rozdział 4, sekcja 3) może być konieczna w przypadku, gdy przedsiębiorstwo prowadzi szeroko zakrojone zautomatyzowane przetwarzanie danych lub profilowanie zachowań.
- Zawarcie umów, zweryfikowanych zgodnie z RODO, z osobami, którym udostępniane są dane osobowe.
- Przekazanie pisemnego zawiadomienia osobom, których dane dotyczą (pracownikom), o przetwarzaniu ich danych osobowych zgodnie z prawem do informacji.

ZABEZPIECZENIE DANYCH I DZIAŁANIA NIEZBĘDNE DO ZGODNOŚCI Z RODO

Czym zajmuje się Safetica?

Rozwiązania Safetica zbudowane są w oparciu o technologię, która gromadzi rekordy rejestrowane na stacjach roboczych. Obejmują one informacje o korzystaniu z komputera, o aplikacjach, stronach internetowych, podłączonych urządzeniach, wiadomościach e-mail, drukowaniu, ruchu sieciowym, operacjach na plikach itp. Rekordy te są zapisywane w bazie danych, dlatego konieczne jest podjęcie kroków w celu zapewnienia zgodności rozwiązania Safetica jak i zabezpieczanego środowiska, z rozporządzeniem RODO.

Kluczowe kroki do osiągnięcia zgodności z RODO

Bezpieczeństwo środowiska

Zaleca się korzystanie z serwera dedykowanego dla usługi Safetica Management Service (SMS) w celu zwiększenia bezpieczeństwa i zmniejszenia ryzyka wystąpienia ewentualnych zagrożeń.

Zalecamy, aby dostęp administratorów do baz danych Safetica był ograniczony do minimalnej liczby niezbędnych administratorów, którzy będą mogli zapewnić sprawność działania i dostępność usług.

Po zainstalowaniu rozwiązania Safetica konieczne jest zdefiniowanie indywidualnych kont i uprawnień użytkowników zgodnie z rolami firmowymi i zalecanymi zasadami:

- Zasada najmniejszego uprzywilejowania (Principle of Least-Privilege) – Wszyscy użytkownicy powinni logować się na konto użytkownika, które ma absolutnie minimalne uprawnienia niezbędne do wykonania bieżącego zadania i nic poza tym.
- Podział ról – Każdy użytkownik powinien pełnić określoną rolę w systemie. Administrator powinien mieć uprawnienia do konfiguracji produktu, a nie do przeglądania rekordów, a kierownik dokładnie odwrotnie.
- Nie zalecamy używania konta w systemie Safetica do celów innych niż przypisywanie ról.

Rozwiązanie Safetica korzysta z produktu innej firmy (Microsoft SQL Server) do przechowywania swoich danych. Należy odpowiednio zarządzać jego funkcjonalnością i przechowywaniem danych, natomiast ustawienia bezpieczeństwa powinny minimalizować ryzyko naruszenia przechowywanych w rozwiązaniu danych osobowych. Więcej szczegółów można znaleźć w dokumencie „Rekomendacje powdrożeniowe".

Ogólne zalecenia dotyczące zapewnienia bezpieczeństwa danych:

- Zabezpieczyć fizyczny dostęp do wszystkich plików baz danych i serwerów
- Zapewnić poufność, integralność i dostępność przetwarzanych danych
- Opcjonalnie: MSSQL Enterprise Edition
- Opcjonalnie: wykorzystać protokół IEEE 802.1X

Zobowiązania prawne i obowiązki wynikające z RODO

Jeśli firma spełnia wymienione poniżej warunki, musi wyznaczyć inspektora ochrony danych. Inspektor ochrony danych odpowiada za nadzorowanie zarówno strategii ochrony danych, jak i jej

wdrażania w celu zapewnienia zgodności z wymogami RODO. Wyznaczenie inspektora ochrony danych jest obowiązkowe tylko w trzech sytuacjach:

- Organizacja jest organem władzy publicznej
- Podstawowa działalność organizacji polega na operacjach przetwarzania danych wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą.
- Na dużą skalę przetwarzane są specjalne kategorie danych (tj. dane wrażliwe, np. dotyczące zdrowia, religii, rasy, orientacji seksualnej itp.) oraz dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Rozwiązanie Safetica może, w wyjątkowych przypadkach, wymagać wyznaczenia inspektora ochrony danych, w zależności od rodzaju przedsiębiorstwa i zakresu stosowania. Zalecamy skonsultowanie się z prawnikiem korporacyjnym w celu uzyskania konkretnej oceny.

W przypadku szeroko zautomatyzowanego przetwarzania danych lub profilowania, należy przeprowadzić ocenę skutków (DPIA) (rozdział 4, sekcja 3) w celu określenia powagi ryzyka. Zalecamy, aby ocena DPIA została przeprowadzona w porozumieniu z przedstawicielami prawnymi. W wybranych przypadkach, gdy nie jest możliwe wystarczające ograniczenie ryzyka, administrator danych jest zobowiązany do poinformowania organu nadzorczego. W zależności od zakresu stosowania (na mocy art. 35 ust. 3 lit. a)) Safetica może wymagać przeprowadzenia oceny DPIA. Zalecamy skonsultowanie się z radcą prawnym w celu uzyskania konkretnej oceny.

Dokumentacja wymagana na mocy RODO

- Jeśli dane Safetica są przetwarzane przez podmiot zewnętrzny, taki jak partner Safetica, należy podpisać umowę o przetwarzaniu danych, jak omówiono w art. 28 RODO. Umowa powinna uwzględniać wszystkie niezbędne postanowienia opisane w rozporządzeniu.
- Jak w przypadku każdego oprogramowania zabezpieczającego stosowanego w firmie, informacje o rozwiązaniu Safetica powinny być zawarte w polityce bezpieczeństwa firmy.
- Firma musi przekazać pracownikom pisemne powiadomienie przed rozpoczęciem korzystania z rozwiązania Safetica. Powiadomienie to powinno zawierać informacje opisane w art. 13 RODO.
- W stosownych przypadkach obowiązkowe jest również prowadzenie rejestru czynności przetwarzania danych osobowych na mocy art. 30 RODO.

Prawa osób, których dane dotyczą

a. Prawo do informacji i prawo dostępu do danych osobowych (rozdział 3, sekcja 2, art. 13-15)
   - Jeśli osoba, której dane dotyczą, korzysta z prawa do informacji, można utworzyć dla niej tabelę strukturalną. Przykład takiej tabeli znajduje się w rozdziale „Dodatek". Wniosek o udzielenie informacji można również złożyć poprzez dostarczenie pisemnego zawiadomienia (jak wcześniej omówiono w części 6 lit. c) „Wymagana dokumentacja").
   - Oprócz przedstawienia przeglądu wszelkich przetwarzanych danych, należy również podać dane kontaktowe osoby, która jest odpowiedzialna za przetwarzanie danych.

	Stanowisko	Nazwisko	Imię	E-mail	Telefon
Administrator					
Zastępca administratora*					
Inspektor ochrony danych*					

*W stosownych przypadkach

- Przez pewien czas w okresie przechowywania danych można skorzystać z prawa dostępu, przekazując osobie, której dane dotyczą, konkretne informacje dotyczące przetwarzania danych w formie raportu Safetica lub pokazując dane w konsoli Safetica.

b. Prawo do przenoszenia danych (rozdział 3, sekcja 2, art. 20)

Prawo to nie ma zastosowania do Safetica ze względu na stosowaną podstawę prawną (uzasadniony interes w ochronie własności intelektualnej przedsiębiorstwa, wchodzący w zakres art. 6 ust. 1 lit. f) na podstawie motywu (49)).

c. Prawo do ograniczenia przetwarzania (rozdział 3, sekcja 3, art. 18)

Administrator może usunąć uprawnienia do przeglądania danych przetwarzanych przez Safetica ze wszystkich kont użytkowników, których dotyczy żądanie.

d. Prawo do sprostowania danych (rozdział 3, sekcja 3, art. 16)

Dane są powiązane z osobą, której dotyczą, poprzez nazwę jej domeny i nazwę komputera. Administrator może zmienić nazwę osoby, której dane dotyczą, w drzewie użytkowników.

e. Prawo do usunięcia danych (rozdział 3, sekcja 3, art. 17)

Aby zastosować się do tego prawa, należy usunąć użytkowników z drzewa użytkowników w konsoli Safetica. Dane zarchiwizowane powinny być usuwane po upływie okresu przechowywania. Zalecany jest sześciomiesięczny okres przechowywania. Można ustanowić inne okresy przedawnienia i odwołania, w niektórych krajach okres ten może wynosić nawet 15 lat lub więcej.

f. Prawo do sprzeciwu wobec przetwarzania (rozdział 3, sekcja 4, art. 21)

Partnerzy Safetica mogą świadczyć usługi (takie jak przeprowadzanie analizy bezpieczeństwa) na rzecz klientów Safetica. Jest to relacja umowna, która pozwala stronie trzeciej (partnerowi) na dostęp do danych Safetica w celu świadczenia usług.

Relacja ta musi być opisana w polityce bezpieczeństwa lub pisemnym zawiadomieniu.

W przypadku gdy osoba, której dane dotyczą, chce skorzystać z prawa do sprzeciwu wobec przetwarzania jej danych, zalecamy wskazanie na politykę bezpieczeństwa firmy i omówienie głównego celu produktu, jakim jest ochrona aktywów firmy i spełnienie wymogów RODO.

DODATEK: PRZYKŁADOWA TABELA PRZETWARZANIA DANYCH OSOBOWYCH

Osoba, której dane dotyczą		Pracownicy firmy / Zmodyfikować według danych firmy
Opis		Dane opisowe, zapisy dotyczące dostępu do danych i oprogramowania na hostach firmy, ogólne korzystanie z Internetu i sieci, korzystanie z drukarki i innych urządzeń wejścia/wyjścia, operacje wykonywane na hostach firmy, logi błędów i debugowania z hostów firmy i oprogramowania
Cel przetwarzania danych		Uzasadniony interes polegający na ochronie aktywów firmy, w tym między innymi własności intelektualnej i poprawie bezpieczeństwa firmy
Podstawa prawna (licencje) zgodnie z art. 6 i 9		Art. 6 ust. 1 lit. f) – prawnie uzasadniony interes
Właściciel (osoba odpowiedzialna wewnątrz firmy)		Określić zgodnie z wymaganiami firmy
Okres przechowywania		W czasie trwania umowy o pracę + 6 miesięcy / określić zgodnie z wymaganiami firmy
Metoda przechowywania danych		System Safetica, system bazodanowy, kopie zapasowe, archiwa
Proces przetwarzania danych		Zbieranie danych z hostów użytkowników korzystających z produktu Safetica. Przesłanie zebranych danych za pomocą zabezpieczonego połączenia na serwer i zapisanie w bazie danych. Dostęp do zgromadzonych danych możliwy jest z poziomu konsoli Safetica oraz bezpośrednio z samych baz danych.
Zewnętrzne podmioty przetwarzające dane		Można wykorzystać w przypadku obsługi technicznej lub innych usług świadczonych przez stronę trzecią / określić zgodnie z wymaganiami firmy
Przekazywanie danych poza UE		Może wystąpić w przypadku obsługi technicznej lub innych usług świadczonych przez stronę trzecią / określić zgodnie z wymaganiami firmy
Rola firmy (administrator / podmiot przetwarzający)		Administrator
Czy DPIA jest konieczna?		Określić zgodnie z procesem przetwarzania danych
Profilowanie?		Określić zgodnie z procesem przetwarzania danych
Przetwarzane automatycznie?		Tak
Prawo do	dostępu	Obowiązuje
	sprostowania danych	Obowiązuje
	usunięcia danych	Obowiązuje
	przenoszenia danych	Nie obowiązuje zgodnie z podstawą prawną (zob. odpowiednia sekcja w tekście powyżej)
	ograniczenia przetwarzania	Obowiązuje
Stosowane środki bezpieczeństwa		Kontrola dostępu, konfiguracja serwera SQL, osoby odpowiedzialne, logi dostępu / określić zgodnie z wymaganiami firmy

Praga | Republika Czeska | 23 stycznia 2018 r.