GDPR (General Data Protection Regulation), a po polsku RODO (Ogólne Rozporządzenie o Ochronie Danych Osobowych) wejdzie w życie 25 maja 2018 r. Unijne rozporządzenie wprowadzi nowe przepisy dotyczące bezpieczeństwa danych i ich przetwarzania, które już teraz przerażają niektórych przedsiębiorców. Co ulegnie zmianie i jakie mogą być kary za niestosowanie się do nowych zaleceń? O czym w szczególności warto pamiętać?
Najważniejszym elementem przy rozpatrywaniu RODO jest definicja określająca czym są dane osobowe. W skrócie, są to wszelkie informacje pozwalające na identyfikację osoby bezpośrednio lub pośrednio. Danymi osobowymi jest nie tylko imię, nazwisko czy pesel, ale także identyfikator internetowy, dane o lokalizacji oraz czynniki pozwalające określić fizyczną, psychiczną czy kulturową tożsamość osoby. RODO zwraca również uwagę na szczególną ochronę danych wrażliwych. Zaliczają się do nich informacje o pochodzeniu rasowym, etnicznym, zdrowiu oraz dane genetyczne (dotyczące odziedziczonych lub nabytych cech genetycznych) i dane biometryczne (związane z cechami fizjologicznymi i behawioralnymi).

Przetwarzanie danych, czyli co?

Czym jest samo przetwarzanie danych? Są to wszelkie operacje wykonywane na danych – ich użycie, zbieranie, utrwalanie, przechowywanie, porządkowanie, modyfikowanie czy niszczenie. Według rozporządzenia RODO, przetwarzanie musi podlegać określonym zasadom.
Zasada legalności – do każdego rodzaju danych, które przetwarzamy konieczne jest uzasadnienie prawne. Przetwarzanie nie może być bezpodstawne, ponieważ generuje zbędne ryzyko.
Zasada ograniczonych celów – związana z zasadą legalności. Dane muszą być zbierane i przetwarzane w konkretnych celach. Ponowne wykorzystanie danych niezgodnie z tymi celami jest zabronione.
Minimalizacja danych – organizacja powinna minimalizować ilość danych przetwarzanych w konkretnym celu. Jak to wygląda w praktyce? Do mailingów nie potrzebne są informacje takie jak pesel czy nazwiska rodowe.
Zasada prawidłowości – każda osoba, której dane są przetwarzane musi mieć w nie wgląd oraz możliwość modyfikacji.
Ograniczenie przetwarzania – przechowywanie danych nie może być dłuższe, niż jest to niezbędne do konkretnych celów. Wyjątek występuje wtedy, gdy informacje zostaną zanimizowane i wykorzystane do celów archiwalnych (w interesie publicznym), naukowych, historycznych lub statystycznych.

Zapewnienie bezpieczeństwa danych – dane osobowe muszą być odpowiednio zabezpieczone, względem zasad RODO. Rozporządzenie zachęca też do posiadania odpowiednich certyfikatów.
Należy pamiętać, że przetwarzanie danych szczególnych kategorii, czyli ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne i światopoglądowe czy innych danych w celu jednoznacznego zidentyfikowania osoby fizycznej jest zabronione. Występuje od tego wiele wyjątków. Jakich? Można je przetwarzać, gdy niezbędne jest to do ochrony życia danej osoby lub związane jest z ważnym interesem publicznym.

Administrator i podmiot

Według RODO za bezpieczeństwo danych osobowych odpowiadają Administrator Danych Osobowych i Podmiot Przetwarzający. Administrator jest osobą fizyczną lub prawną, organem publicznym lub innym, który ustala cele i sposoby przetwarzania danych osobowych. Innymi słowy jest to właściciel, przedsiębiorca lub spółka. Podmiotem przetwarzającym jest natomiast dostawca platformy lub architektury przetwarzającej dane. Robi to w imieniu administratora. Do ich zadań należy wdrażanie odpowiednich rozwiązań technicznych, polityk ochrony danych, stosowanie kodeksów postępowań, mechanizmów certyfikacyjnych czy też zgłaszanie naruszeń. Ogólne Rozporządzenie o Ochronie Danych Osobowych wprowadza wiele zmian w stosunku do dzisiejszych zasad. Na kilka z nich w szczególności należy zwrócić uwagę.

10 najważniejszych zmian RODO

1. RODO obowiązuje nie tylko w Europie. Każda firma, nawet gdy nie ma osobowości prawnej, przetwarzając dane obywateli UE lub osób znajdujących się na terenie UE podlega rozporządzeniu.
2. Odpowiedzialność przetwarzającego dane. Organizacje przetwarzające dane osobowe innych firm (przykładem mogą być firmy hostingowe) będą bezpośrednio odpowiedzialne za złamanie regulacji.
3. Podejście oparte na ryzyku. To organizacja ma udowodnić, że dysponuje odpowiednimi zabezpieczeniami i technologiami, a jej zasady bezpieczeństwa są zgodne z RODO.
4. Jawność przetwarzania danych. Każda osoba, musi mieć pełną świadomość o tym, że jej dane są przetwarzane. Organizacja musi podać pełne informacje na temat swoich działań i celów, do których dane są potrzebne.
5. Indywidualność i prawo do zapomnienia. Osoby, których dane są przetwarzane, będą miały nad nimi większą kontrolę, poprzez wgląd i dostęp do nich. Będą mogły też przenieść dane, a

także wycofać zgodę na ich przetwarzanie.
6. Natychmiastowe zgłoszenie naruszenia. W przypadku naruszeń, Administrator Danych Osobowych będzie miał 72 godziny od wykrycia na zgłoszenie incydentu do odpowiedniego organu. Może wystąpić konieczność poinformowania podmiotu, którego dane zostały naruszone.
7. Ograniczone profilowanie. Organizacja chcąca profilować dane (przetwarzać, aby prognozować zachowania) przed rozpoczęciem zbierania danych musi otrzymać zgodę i poinformować podmioty o profilowaniu.
8. Ocena skutków dla ochrony danych. Przed wykonaniem operacji „wysokiego ryzyka" takich jak profilowanie na dużą skalę czy wykorzystanie danych mogących naruszyć prawa i wolności osoby fizycznej, niezbędna jest ocena skutków planowanych operacji.
9. Wymiana z innymi krajami. Transfer danych poza kraje Europejskiego Obszaru Gospodarczego będzie dopuszczony tylko wtedy, gdy kraj ten zapewnia równy poziom bezpieczeństwa. Dodatkowo RODO zabrania ujawniania jakichkolwiek danych organizacji spoza Unii Europejskiej, chyba że umowa międzynarodowa stanowi inaczej.
10. Powołanie Inspektora Ochrony Danych. Organizacje publiczne (z wyjątkiem sądów) oraz firmy, których główną działalnością jest przetwarzanie danych będą musiały wyznaczyć Inspektora Ochrony Danych dysponującego wiedzą ekspercką z zakresu danych osobowych. Będzie on informował administratora i podmioty przetwarzające o ich obowiązkach, doradzał, monitorował przestrzeganie zasad oraz będzie punktem kontaktowym dla organu nadzorczego w kwestiach przetwarzania danych.

Dotkliwe konsekwencje

Niestosowanie się do zasad RODO może prowadzić do ogromnych sankcji. Naruszenia mogą wiązać się z nałożeniem na organizację maksymalnych kar w wysokości 20 milionów euro lub 4% całkowitego światowego rocznego obrotu z poprzedniego roku. Zastosowanie ma oczywiście wyższa kwota, nie oznacza to jednak, że nawet za najmniejsze naruszenie, organizacja będzie musiała zapłacić najwyższą karę. Wysokość kar zależy od wielu czynników – tego, czy nastąpiło zgłoszenie naruszenia, działań podjętych przez administratora, kategorii danych osobowych, stosowania kodeksów i innych. Sankcje zasilać będą budżet państwa.
Źródła:
Konferencja GDPR Roadshow, prelekcja „Co to jest GDPR i w jakim stopniu nas dotyczy", Piotr Niedźwiedź, AVNET
http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679

https://www.algoodbody.com/media/TheGDPR-Top10KeyChanges1.pdf
https://www.pwc.pl/pl/artykuly/2017/10-najwazniejszych-zmian-ktore-wprowadza-rodo.html
http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR
Raport Fidelis Cybersecurity „Czy Twoja firma jest gotowa na reformę europejskich przepisów o ochronie danych”