fundacja instytut
CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo w epoce RODO

– w jaki sposób jesteśmy chronieni i na co musimy uważać?

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Źródło: Flickr (CC 2.0)

Przyjęcie rozporządzenia RODO w kwietniu 2016 r., a następnie jego wejście w życie w maju 2018 r. stały się momentami przełomowymi dla całej internetowej społeczności mieszkańców Unii Europejskiej (UE) oraz ukróciły wiele nieuczciwych działań w tym zakresie. Mimo wszystko część cyberprzestępców i firm ryzykuje, wciąż aktywnie starając się nas oszukiwać.

Artykuł omawia, jakie możliwości ochrony wprowadziło w 2018 r. rozporządzenie o ochronie danych. Przedstawione zostaną praktyczne rozwiązania umożliwiające użytkownikom kontrolę nad danymi wrażliwymi. Ponadto zostały wskazane kierunki rozwoju przepisów wynikających bezpośrednio z RODO.

Nagłówki w tekście:

- Czym właściwie jest RODO?
- Jakie główne zmiany wprowadzono za pomocą RODO?
- Cyberprzestępcy a RODO – jakie praktyki są stosowane mimo istnienia przepisów?
- Jak ewoluuje RODO?
- Jakie prawne możliwości daje nam RODO?

Czym właściwie jest RODO?

Podpisując umowy czy akceptując regulaminy, często jesteśmy proszeni o zatwierdzenie klauzul wynikających z przepisów RODO (ang. GDPR), tylko czym w zasadzie jest owo prawo? RODO to powszechnie stosowany skrót dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, będące rozporządzeniem o ochronie danych obowiązującym w UE. Akt został przyjęty 27 kwietnia 2016 r., a wszedł w życie 28 maja 2018 r., wiążąc podmioty publiczne i prywatne w zakresie ochrony danych. Nie jest to pierwszy tego typu akt prawny w ogóle, ale pierwszy tak kompleksowy. Wejście w życie RODO sprawiło, że na całym świecie rozpoczęły się żywe dyskusje na temat wprowadzenia lokalnych rozwiązań w zakresie protekcji danych, czego efektem jest m.in. chińskie PIPL (ang. Personal Information Protection Law of the People's Republic of China) i DSL (ang. Data Security Law) – obydwa z 2021 r.

Rozporządzenie zobowiązuje wszystkie podmioty działające na terenie UE do administrowania danymi osobowymi w ściśle określonym rygorze pod groźbą wysokich kar – do 4 proc. światowego obrotu lub 20 mln euro. Czym jest administrowanie danymi osobowymi? W skrócie jest to zarządzanie posiadanymi danymi ludzi, tj. sposób przetrzymywania takich informacji, działania z nimi, a także publikowania ich. Podmioty zajmujące się tymi czynnościami formalnie zostały nazwane ADO (Administratorzy Danych Osobowych).

Mimo kompleksowego podejścia do ochrony danych niestety przepisy RODO wiążą się z pewną komplikacją dla użytkowników in-

ternetu, czyli dodatkowymi rozbudowanymi regulaminami na stronach podmiotów przetwarzających, które są najczęściej „przeklikiwane". Niemniej, owe często pomijane przez użytkowników dokumenty zawierają informacje m.in. o tym, kto, po co i w jakich okolicznościach przetwarza nasze dane. Świadomość tego może być pomocna w razie odkrycia przez nas pewnych odstępstw od norm.

Reasumując, wszelkie postanowienia rozporządzenia stawiają nas na samym szczycie priorytetowości ochrony i sprawiają, że nasze imię i nazwisko czy miejsce zamieszkania stały się jednym z najistotniejszych dóbr.

Jakie główne zmiany wprowadzono za pomocą RODO?

RODO nie jest zupełnie nowym pakietem rozwiązań, lecz wyłącznie uszczegółowieniem pewnych kwestii, które już wcześniej funkcjonowały w przestrzeni prawnej na terenie UE. Głównym aktem prawnym regulującym zagadnienia w zakresie ochrony danych osobowych do czasu wejścia w życie RODO była dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych z 13 grudnia 1995 r. Zobowiązała ona państwa członkowskie UE do wdrożenia odpowiednich przepisów do prawa krajowego najpóźniej do 24 października 1998 r. Polska nie była wówczas członkiem UE, została nim dopiero w maju 2004 r., pomimo tego nie była w tyle stawki dostosowywania przepisów do nowych warunków technologicznych. W Polsce już od 29 sierpnia 1997 r. funkcjonowała ustawa o ochronie danych osobowych, ważna aż do wprowadzenia norm wynikających z RODO.

Wśród głównych zmian zastosowanych w rozporządzeniu z 2016 r. należy wskazać m.in. szerszy dostęp użytkownika do swoich danych, większą kontrolę nad operowaniem danymi (urząd Inspektora Ochrony Danych czy Urząd Ochrony Danych Osobowych), wysokie kary za uchybienia w stosowaniu się do norm czy krytyczną weryfikację państw pozaeuropejskich pod kątem wykorzystywania naszych danych.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

Cyberprzestępcy a RODO – jakie praktyki są stosowane mimo istnienia przepisów?

Nowo wprowadzone przepisy i wiążące się z nimi ryzyko potencjalnych kar z całą pewnością ograniczyły przestępcze oraz wątpliwe moralnie działania w zakresie danych osobowych w przestrzeni internetowej. O ile przedsiębiorstwa – zwłaszcza o charakterze międzynarodowym – zazwyczaj wolą stosować się do przepisów z uwagi na ogromne kary oraz opinię publiczną (potencjalna utrata zaufania do usługi lub produktu), o tyle jednostki bądź małe podmioty nastawione na oszustwo internetowe jako główne źródło zarobku już niekoniecznie.

Wśród głównych praktyk o charakterze cyberprzestępczym nastawionych na pozyskanie danych osobowych bądź innych danych wrażliwych należy wymienić:

- *Phishing* – metoda cyberprzestępcza, której głównym celem jest pozyskanie naszych danych w nielegalny sposób, np. przez podszywanie się pod organ państwowy bądź podmiot oferujący nam pracę. W ramach tej aktywności dane są pozyskiwane z dowodów osobistych czy kart kredytowych. Przestępcy działają kreatywnie, fabrykując całe strony internetowe, adresy IP czy numery telefonów, wyłącznie w celu uwiarygodnienia wymierzonego w nas fortelu.
- Zdalna instalacja złośliwego oprogramowania, tzw. ***malware*** – w ramach tej aktywności cyberprzestępcy zdalnie instalują na naszym sprzęcie oprogramowanie, które wyszukuje oraz pozyskuje określone dane. Jego instalacja może rozpocząć się np. kliknięciem przez nas w niezweryfikowane linki.
- *Hacking* – działanie skoncentrowane na pojedynczym użytkowniku bądź infrastrukturze teleinformatycznej, może prowadzić do dużych wycieków danych, często stosowane względem banków czy stron internetowych.

Wskazane praktyki są tylko pewnymi wariantami nielegalnych aktywności w zakresie pozyskiwania danych osobowych i innych danych wrażliwych. Warto również pamiętać, że pozyskane od nas dane mogą być użyte m.in. w procederach kradzieży tożsamości, nielegalnej odsprzedaży danych, a także w celu czerpania innych korzyści. Głównymi metodami ochrony są tworzenie przez nas silnych i zróżnicowanych haseł oraz zwiększona ostrożność w zakresie odwiedzanych stron czy klikanych linków.

Jak ewoluuje RODO?

Internet to specyficzne medium, które ewoluuje w zasadzie każdego dnia. Prawo co do zasady jest raczej trwałe, procedowanie zmian w jego zakresie zwykle trwa dość długo. Wymagane są konsensusy na poziomie m.in. politycznym, aktów prawnych, interesów czy opinii publicznej. Przez naturę narzędzia, jakim jest globalna sieć internetowa, i sposób procedowania zmian prawodawcom trudno jest na gruncie prawa odpowiadać na wszelkie rozwiązania kreowane przez użytkowników sieci. Wspomniane już w artykule aktywności cyberprzestępców i ich kreatywność nie ułatwiają systemom prawnym w nadążaniu za rozwijającą się technologią. Decydenci mimo wszystko starają się łatać luki, nowelizując stare przepisy lub tworząc nowe. Od wejścia w życie RODO powstało na tym gruncie kilka wartych odnotowania rozwiązań, w tym m.in.:

- Rozporządzenie nr 2022/2065 w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych, AUC). Rozporządzenie jest zorientowane m.in. na ochronę świadomości użytkownika w zakresie nieświadomego wyrażania zgód, zakaz targetowania reklam na podstawie danych osobowych małoletnich, a także zakaz targetowania na podstawie danych wrażliwych.
- Dyrektywa UE nr 2019/2161 (tzw. dyrektywa Omnibus) w zakresie umów o dostarczanie treści cyfrowej (transakcja za pomocą danych osobowych).

Poza wskazanymi powyżej normami możemy spodziewać się kolejnych zmian na gruncie ochrony danych:

- akt w sprawie zarządzania danymi (rozporządzenie UE zacznie obowiązywać od dnia 24 września 2023 r.),
- projekt aktu w sprawie danych,
- projekt rozporządzenia w sprawie sztucznej inteligencji.

Jak przedstawiono, prawo w zakresie ochrony użytkowników internetu jest stale rozwijane, być może w najszybszym w historii tempie tworzenia umocowań prawnych.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

Jakie prawne możliwości daje nam RODO?

Głównym celem RODO jest ochrona naszych praw. Przepisy wynikające z rozporządzenia, a także następujących po nim aktów prawnych dają nam kompleksowy pakiet narzędzi do walki o nasze dobra osobiste. W przypadku zaistnienia pewnych niezgodności należy pamiętać przede wszystkim o:

- Wymogu wyszczególnienia w regulaminach RODO klarownego dla użytkownika prawa do usunięcia danych z baz administratorów (tzw. „prawo do bycia zapomnianym"). W dokumencie powinna zostać zawarta nazwa administratora bazy wraz z danymi umożliwiającymi zgłoszenie się do niego, a także sposób i cel jego działania na naszych danych.
- Możliwości przenoszenia danych między bazami – np. w momencie zmiany dostawcy usługi bądź wykrycia przez nas nieprawidłowości w zachowaniu administratora.
- Możliwości wycofania zgody na przetwarzanie danych.
- Ułatwionym dostępie do naszych danych oraz informacji w zakresie ich wykorzystywania przez administratorów i ew. strony trzecie. W każdej chwili, jeżeli takie dane są zawarte w regulaminie RODO, mamy możliwość zgłoszenia się do administratora z prośbą o określenie szczegółów związanych z operowaniem przez niego naszymi danymi.
- Prawie do niezwłocznego uzyskania informacji w razie ataków hakerskich bądź innych działań mogących sprawić, że nasze dane wycieką. W przypadku zaniechania przekazania nam takiej informacji przez podmiot, który administruje bazą z naszymi danymi, możemy zgłosić sprawę do odpowiednich służb, a także domagać się odszkodowania.

Ponadto w związku z wejściem w życie RODO powołano UODO (Urząd Ochrony Danych Osobowych), do którego możemy zgłosić naruszenia, a on pomoże nam w walce z nieuczciwymi praktykami. Jednak zanim się do niego udamy, musimy postarać się samodzielnie skontaktować z podmiotem zarządzającym naszymi danymi. Urząd może zainterweniować tylko w przypadku faktycznego braku woli współpracy.

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości