BIURO PORAD PRAWNYCH ZACHARSKI

Oskar Zacharski
Prawnik, inspektor ochrony danych, audytor ISO 27001, autor publikacji branżowych. Od 2014 r. świadczy usługi doradcze przedsiębiorcom i placówkom publicznym w zakresie ochrony danych osobowych."

ePrivacy – nowe wymogi dla administratorów danych

Podczas gdy, niektóre organizacje inwestują w ochronę danych osobowych i środki ochrony prywatności, aby – mniej lub bardziej – osiągnąć „zgodność z RODO", a inne wciąż próbują zrozumieć swoje obowiązki jako administratorzy danych, to już za chwilę mogą być zobligowani do dostosowania się do „RODO 2".

Czym jest rozporządzenie ePrivacy?

Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego i ochrony danych osobowych w łączności elektronicznej oraz uchylające dyrektywę 2002/58 / WE (rozporządzenie o prywatności i łączności elektronicznej to nowe przepisy UE, które zastąpią obecną dyrektywę o prywatności i łączności elektronicznej z 2002 r.

Jaka jest różnica między dyrektywą a rozporządzeniem?

Dyrektywa o prywatności i łączności elektronicznej jest aktem, który nakłada na państwa członkowskie UE obowiązek osiągnięcia określonego rezultatu bez wskazywania środków do jego osiągnięcia, co skutkuje tym, że w każdym z krajów Unii Europejskiej przepisy te przybrały inną postać, często różniąc się od siebie. W przeciwieństwie do dyrektywy rozporządzenie obowiązuje w niezmienionej formie w każdym państwie członkowskim. Nie ma potrzeby, aby państwa członkowskie tworzyły przepisy krajowe implementujące te unijne.

Czy rozporządzenie o prywatności i łączności elektronicznej zastąpi RODO?

Rozporządzenie ePrivacy zostało zaprojektowane, aby uzupełnić, a nie zastąpić RODO. Pierwotnie te dwa akty prawne miały zacząć obowiązywać w tym samym momencie. Jednak ze względu na przewlekły proces legislacyjny, pandemię COVID19 i lobbing reklamodawców internetowych, którzy sprzeciwiali się niektórym zapisom, proces opracowania ostatecznego tekstu ePrivacy uległ wydłużeniu.

Obecnie projekt ma już akceptację Komisji Europejskiej i Rady Unii Europejskiej, i oczekuje na pierwsze czytanie w Parlamencie Europejskim.

Rozporządzenie ePrivacy ma uzupełnić i uszczegółowić przepisy RODO w wybranych obszarach, jednocześnie stanowi wobec niego regulację

lex specialis, w przypadku, gdy dane pozyskiwane w związku ze świadczeniem usług łączności są danymi osobowymi.

Co i dla kogo się zmienia?

W związku z rozwojem technologii bezprzewodowych, rozporządzenie rozszerza definicję danych pochodzących z łączności elektronicznej i włącza do niej nie tylko przesyłane treści, ale także informacje o użytkownikach końcowych, dane służące do śledzenia i zidentyfikowania źródła, miejsca łączności, lokalizację geograficzną, datę, godzinę, czas trwania i rodzaj łączności. Wszystkie te dane powinny być traktowane jako poufne, a ingerencja przez osoby inne niż użytkownicy końcowi została zakazana.

Rozporządzenie ma zapewnić ochronę przetwarzania danych osobowych pochodzących z łączności elektronicznej – m.in. Internetu, usług telefonii, poczty elektronicznej, więc to, kogo dotyczą zmiany zależy od tego czym dana organizacja zajmuje się na co dzień.

ePrivacy dotyczy w szczególności:

- przedsiębiorców świadczących usługi telekomunikacyjne (operatorzy telekomunikacyjni, dostawcy Internetu, ale także firm świadczących usługi wideokonferencji, czatów, platform pracy grupowej),
- osób zajmujących się marketingiem, wysyłających wiadomości mailowe lub wykonującym telefony marketingowe,
- właścicieli stron internetowych monitorujących ruch na stronie lub wykorzystujących zaawansowane pliki cookie,
- przedsiębiorców zbierających i wykorzystujących informacje o urządzeniach końcowych tj. telefonach, laptopach w celach marketingowych (np. profilowanie behawioralne użytkowników końcowych w oparciu o pliki cookie).

Pliki cookie

ePrivacy ma także zapewnić ochronę danych osobowych w zakresie wykorzystywania plików typu cookie, dlatego też czasami nazywane jest „rozporządzeniem ciasteczkowym". Informacje przechowywane na urządzeniu końcowym użytkownika (np. pliki cookie) stanowią część jego prywatnej sfery, która podlega ochronie. Techniki służące do monitorowania działań użytkowników końcowych (śledzenie aktywności, lokalizacja urządzenia itp.) stanowią, zgodnie z rozporządzeniem, poważne zagrożenie prywatności i są zakazane, o ile użytkownik nie wyrazi na nie zgody. Przy czym zgoda ta powinna być jasna, jednoznaczna i możliwa do odwołania w każdym momencie (tak jak w RODO). Metody uzyskania zgody powinny być przyjazne, a w momencie, gdy użytkownik decyduje się udostępnić dane w zamian za konkretną usługę, musi mieć wiedzę o warunkach takiej współpracy.

Marketing

Rozporządzenie określa zasady prowadzenia marketingu bezpośredniego, który jest definiowany jako **wsz**ystkie formy reklamy, w ramach których przedsiębiorca wysyła materiały marketingowe z użyciem łączności elektronicznej. Zgodnie z jego zapisami:

- Możliwe jest rozsyłanie ofert za pomocą usług łączności elektronicznej, gdy klienci wyrazili na to zgodę.
- W przypadku uzyskania od klienta danych kontaktowych w związku ze sprzedażą produktu lub usług, przedsiębiorca może wykorzystać te dane do komunikacji marketingowej. Klientom przysługuje prawo do rezygnacji z otrzymywania treści marketingowych w prosty sposób, bezpłatnie i przy każdym wysyłaniu wiadomości.
- Przedsiębiorcy stosujący marketing bezpośredni mają obowiązek ujawnić swoją tożsamość, a także podać dane do kontaktu i jasną informację o możliwości wycofania zgody na otrzymywanie wiadomości.
- Operatorzy mają obowiązek dbać o bezpieczeństwo użytkowników,

a także informować ich o możliwych środkach, które mogą podjąć w celu ochrony bezpieczeństwa swojej łączności (lub swoich połączeń).

Identyfikacja rozmów

ePrivacy daje użytkownikom prawo do kontrolowania łączności elektronicznej poprzez możliwość decydowania o identyfikacji rozmów przychodzących i wychodzących (nie tylko w ramach UE, ale także w odniesieniu do połączeń z państw trzecich). Możliwości te zapewnia się bezpłatnie. Wyjątkami są np. połączenia do służb ratunkowych.

Dostawcy usług mają obowiązek zapewnić użytkownikom bezpłatną możliwość blokowania rozmów przychodzących z konkretnych numerów lub z anonimowych źródeł, a także możliwość zatrzymania automatycznych przekierowań połączeń na urządzenia końcowe.

Użytkownicy mają również prawo decyzji, czy ich numer zostanie włączony do publicznie dostępnego spisu numerów i na jakich zasadach. W każdej chwili użytkownik może zażądać dostępu do swoich danych, ich modyfikacji, uaktualnienia, a także wykreślenia ze spisu.

Zasięg terytorialny ePrivacy

ePrivacy jako akt UE, będzie miało taki sam zakres terytorialny jak RODO

i będzie miało bezpośrednie zastosowanie we wszystkich państwach członkowskich UE. Ponadto ePrivacy będzie działało eksterytorialnie dla organizacji spoza EOG, które:

- przetwarzają treści lub metadane dotyczące łączności elektronicznej mieszkańców UE;
- przetwarzają informacje o urządzeniach końcowych mieszkańców UE;
- oferują usługi mieszkańcom UE; lub
- wysyłają bezpośrednie komunikaty marketingowe do mieszkańców UE.

Wysokość kar za nieprzestrzeganie przepisów

Rozporządzenie ePrivacy będzie podlegać identycznemu systemowi kar jak RODO, z maksymalnymi grzywnami w wysokości 20 mln euro lub 4% całkowitego rocznego światowego obrotu organizacji nieprzestrzegającej przepisów, w zależności od tego, która z tych kwot jest wyższa.

Użytkownicy końcowi, którzy ponieśli „szkodę majątkową lub niemajątkową" z powodu naruszenia rozporządzenia ePrivacy, mają również prawo do otrzymania odszkodowania od sprawcy naruszenia.

ePrivacy – regulacja niezbędna w XXI w.

ePrivacy to odpowiedź UE na postępujący rozwój technologii, ma być złotym środkiem pomiędzy rozwojem usług cyfrowych i prywatnością użytkowników. Nowe algorytmy, chatGPT, portale społecznościowe, pliki cookie – z tych źródeł zbieranych jest coraz więcej danych osobowych użytkowników, które w 2023 r. stanowią niejako walutę. W 2020 r. Polski Instytut Ekonomiczny przeprowadził badanie pod nazwą „Ile warte są nasze dane?". Według raportu wartość danych polskich użytkowników dla Google wynosiła 4,025 mld zł, a dla Facebooka 2,196 mld zł. Aż 87 proc. uczestników badania twierdziło, że firmy technologiczne wiedzą o nas za dużo, a 84 proc. uważało, że działalność firm technologicznych powinna podlegać większej kontroli. ePrivacy ma być odpowiedzią także na problemy zauważone przez uczestników badania.

Rozporządzenie ePrivacy będzie stosowane bezpośrednio we wszystkich krajach UE a ustawodawcy krajowi będą zobowiązani dostosować wewnętrzne regulacje tak, aby były one zgodne z nowym rozporządzeniem.

Rozporządzenie ePrivacy będzie stosowane bezpośrednio we wszystkich krajach UE a ustawodawcy krajowi będą zobowiązani dostosować wewnętrzne regulacje tak, aby były one zgodne z nowym rozporządzeniem. Warto już teraz zastanowić się jak ePrivacy wpłynie na funkcjonowanie firm jak i użytkowników.