Ochrona Danych Osobowych – nowe przepisy w 2018 r.

Kategoria: Aktualności
Opublikowano: piątek, 14, kwiecień 2017 16:39
Sylwia Cyrankiewicz-Gortyńska
Odsłony: 41542

Pozostało już tylko 13 miesięcy do wejścia w życie regulacji UE RODO (Ogólne rozporządzenie o ochronie danych osobowych), które odmienią sytuacje podmiotów przetwarzających dane osobowe. Dotyczyć to będzie wszystkich bez względu na wielkość.

Zmiana ta niesie za sobą poważne sankcje, jakimi będą objęte podmioty, które nieskutecznie będą chronić dane osobowe. Trzeba wskazać kary te są niemałe! Odczuwalne dla sektora publicznego i prywatnego. Ważnym jest to, że jeżeli firma posiada oddział w innym z krajów członkowskich Unii, organy tego państwa mają możliwość weryfikowania prawidłowości przetwarzania danych osobowych. A co za tym idzie, mogą nakładać kary za m.in. „brak zastosowania odpowiednich do ryzyk i zagrożeń środków organizacyjnych i technicznych, zabezpieczających przetwarzanie danych w tym braku szyfrowania".

Kary będą mogły wynieść odpowiednio do 10 000 000 euro i do 20 000 000 euro, a w przypadku przedsiębiorstw nie więcej niż odpowiednio do 2% lub 4% światowego obrotu.

Jest to wyzwanie – dla każdej organizacji, w tym JST. A dziś należy stwierdzić bez przesady, wręcz jednoznacznie - zostało naprawdę mało czasu, a pracy w procesie sprostania wymogom, sporo!

Podstawy prawne

Więc przypomnijmy, akty prawne regulujące zagadnienie. W Dzienniku Urzędowym Unii Europejskiej L 119 z dnia 4 maja 2016 r. opublikowano teksty aktów prawnych, które składają się na kompleksową reformę ochrony danych osobowych, tj.

- 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/WE (ogólne rozporządzenie o ochronie danych), zwane dalej „rozporządzeniem";
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w z związku przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, zwana dalej „dyrektywą".

Rozporządzenie w założeniu ma przyczynić się do zwiększenia harmonizacji prawa na poziomie UE. Będąc stosowanym we wszystkich państwach UE, rozporządzenie umożliwi łatwiejsze, czytelniejsze i mniej kosztowne prowadzenie działalności gospodarczej w UE. A dla sektora publicznego i samorządowego zwiększa transparencję i zaufanie obywateli.

Do najważniejszych regulacji zawartych w rozporządzeniu można zaliczyć:

- zdefiniowanie pojęcia „danych wrażliwych". W definicji tego rodzaju danych wskazano pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne pozwalające na identyfikację osoby, dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
- lepszą kontrolę, jaką obywatele mają nad własnymi danymi, np. poprzez wzmocnienie obowiązku informacyjnego, wprowadzenie prawa do przenoszenia danych, czy też „prawa do bycia zapomnianym".

Phoca PDF

Przepisy rozporządzenia przewidują, iż możliwe będzie zażądanie od administratora danych informacji o tym, jakie dane o nas są w jego posiadaniu, jak również otrzymania danych zapisanych w powszechnie wykorzystywanym formacie i przeniesienie ich do innego administratora bez przeszkód ze strony obecnego, któremu dostarczono te dane („prawo do przenoszenia danych"). W przypadku „prawa do bycia zapomnianym" nałożono m.in. na administratora danych osobowych, który dokonał ich upublicznienia obowiązek ich usunięcia i podjęcia działań, mających na celu poinformowanie innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, aby administratorzy usunęli wszelkie łącza do tych danych, czy też kopie tych danych osobowych;

- objęci e europejskimi przepisami z zakresu ochrony danych także organizacji spoza UE, które oferują swoje towary i usługi w UE, bądź monitorują na tym terytorium zachowanie internautów. Takie rozwiązanie ma zagwarantować osobom na terytorium UE jednolitą ochronę, niezależnie od tego, skąd pochodzi podmiot przetwarzający ich dane;
- wzmocnienie ochrony danych osobowych przekazywanych z terytorium UE do państw trzecich przy jednoczesnym usankcjonowaniu nowych instrumentów ułatwiających transgraniczne przekazywanie danych (tj. wiążących reguł korporacyjnych oraz standardowych klauzul umownych);
- zmniejszenie obciążeń administracyjnych, w szczególności poprzez zniesienie obowiązku wcześniejszego zawiadamiania organów ochrony danych o przetwarzaniu danych oraz wprowadzenie tzw. „podejścia opartego na ocenie ryzyka", zgodnie z którym obciążenia regulacyjne będą uzależnione od ryzyka, jakie wynika z danego przetwarzania;
- wprowadzenie obowiązku zwiększonej współpracy pomiędzy krajowymi organami ochrony danych, co wpłynie na ujednolicenie stosowania przepisów o ochronie danych na terenie wszystkich państw UE i ułatwi funkcjonowanie przedsiębiorcom prowadzającym działalność w więcej niż jednym państwie członkowskim. Współpraca na bazie jednolitych regulacji przyczyni się do efektywnego wykorzystania posiadanych przez te organy zasobów oraz doświadczenia;
- wprowadzenie nowej funkcji, tzw. „Inspektora Ochrony Danych" , w miejsce obecnie funkcjonującego ABI (Administratora Bezpieczeństwa Informacji), który będzie wyznaczany w jednostkach publicznych oraz gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania danych na dużą skalę;
- promowanie mechanizmów zwiększających ochronę praw i wolności osób fizycznych w związku z przetwarzaniem danych poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych, które są zgodne z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń ochrony danych;
- wyposażenie organów ochrony danych w uprawnienie do nakładania kar pieniężnych za nieprzestrzeganie przepisów rozporządzenia, co ma w założeniu wpłynąć na zwiększenie skuteczności ich stosowania.

Dyrektywa jest bezpośrednio powiązana z projektem rozporządzenia, którego wdrożenie będzie wymagało zmiany podstaw prawnych krajowego systemu ochrony danych osobowych.

Zmiany w przepisach krajowych, implementujące dyrektywę, będą zapewne zmianami wynikowymi do nowego krajowego systemu ochrony danych osobowych.

Implementacja

Phoca PDF

W przypadku rozporządzenia, nie jest ono aktem harmonizacji prawa jak to ma miejsce w przypadku dyrektywy, lecz jest instrumentem unifikacji prawa na terytorium Unii Europejskiej. Rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich przez sektor publiczny i prywatny. Konieczne jest tu dokonanie przeglądu i *de facto* zmiana regulacji w zakresie ochrony danych osobowych .

W przypadku dyrektywy – określenie sposobu wdrożenia pozostawia się danemu państwu członkowskiemu. Zasadniczą formą implementacji w tym przypadku będzie ustawa (czy raczej szereg ustaw), a zmiany będą jednocześnie skorelowane.

Skala zmian jest na tyle duża, iż koniecznym będzie opracowanie nowej ustawy o ochronie danych osobowych wraz z określoną grupą aktów wykonawczych do niej. Ponadto należy dokonać przeglądu innych przepisów o charakterze sektorowym. Korelacja wdrażania obu regulacji UE jest o tyle ważna, że implementacja dyrektywy powinna maksymalnie wpisywać się w krajowy porządek prawny i być na tyle precyzyjna, aby nie było konieczności sięgania do treści samej dyrektywy przy stosowaniu przepisów prawa krajowego, w odróżnieniu od rozporządzenia, którego „dostosowanie" do krajowego porządku prawnego powinno być ograniczone do minimum, a przepisy rozporządzenia były podstawowymi treściami w regulowanej dziedzinie.

Co z tego wynika dla każdej organizacji w sektorze publicznym i prywatnym, aby nie potrzeba było grona prawników, dla analizy treści i obowiązków z jakimi maja się zmierzyć? Bezwzględnie należy wystartować już teraz !

Jak powinien wyglądać czas przygotowań?

Zgodnie z art. 99 ust. 2 rozporządzenia – ma ono zastosowanie od dnia 25 maja 2018roku.

W przypadku dyrektywy, zgodnie z art. 66 ust. 1, państwa członkowskie przyjmują i publikują do dnia 6 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania tej dyrektywy.

Zwiększenie możliwości kontroli danych osobowych przyczyni się do wzrostu zaufania do usług świadczonych przez podmioty prywatne i publiczne. Osoby, mając poczucie, iż ich dane są lepiej chronione, częściej i chętniej będą korzystali z usług i aplikacji społeczeństwa informacyjnego.

Źródło: IKG Techonology, autorzy: Kamil Galicki i Joanna Bańkowska

Phoca PDF