Rozporządzenie UE o ochronie danych osobowych

29 stycznia 2016

Najważniejszym wydarzeniem dotyczącym ochrony danych osobowych w 2016 r. będzie oficjalne zakończenie trwającej od 2012 r. reformy ochrony danych osobowych w Unii Europejskiej. Choć na wejście w życie nowego prawa muszą się przygotować przede wszystkim państwa członkowskie, organy ochrony danych osobowych i podmioty przetwarzające dane, to także obywatele – by móc w pełni korzystać z przysługujących im uprawnień – powinni wiedzieć, jakie wprowadzi ono zmiany.

1. Jedna regulacja w 28 państwach UE. Od 2018 r. we wszystkich państwach Unii Europejskiej obowiązywać będą jednakowe przepisy dotyczące ochrony danych osobowych. Rozporządzenie nie wymaga implementacji, jednak jego wejście w życie spowoduje konieczność zmiany wielu polskich ustaw i rozporządzeń.

2. Te same przepisy obowiązujące wszystkie firmy. Unijna regulacja obejmie nie tylko krajowe instytucje publiczne (choć tu przewidziana jest możliwość wprowadzenia wielu wyjątków) i firmy z Unii Europejskiej, ale także podmioty z innych państw, które np. świadczą obywatelom UE usługi w Internecie

3. Więcej możliwości złożenia skargi do krajowego rzecznika ochrony danych. Po wejściu w życie rozporządzenia obywatele będą mogli składać skargi na podmioty przetwarzające ich dane do swoich krajowych rzeczników ochrony danych bez względu na to, gdzie mieści się siedziba danej firmy. Jeśli będziemy chcieli poskarżyć się np. na Facebook, nie będziemy musieli już zgłaszać się do irlandzkiego rzecznika ochrony danych osobowych – wystarczy skarga do polskiego GIODO.

4. Silniejsza współpraca rzeczników ochrony danych. Rzecznicy ochrony danych osobowych z 28 państw członkowskich UE będą

dysponowali silniejszymi narzędziami współpracy. Dzięki temu będą mogli współdziałać na rzecz lepszej ochrony danych osobowych, efektywniej wykorzystywać zasoby i doświadczenie.

5. Nowe sankcje. Rozporządzenie nie tylko przewiduje wzmocnienie współpracy rzeczników ochrony danych, ale także daje im więcej narzędzi oddziaływania na administratorów danych osobowych. GIODO będzie mógł nakładać kary administracyjne w wysokości do 20 000 000 euro lub aż do 4% rocznego światowego obrotu (w przypadku przedsiębiorstw). Odczuwalne sankcje mają pomóc w wymuszeniu przestrzegania przepisów.

6. Jasne informowanie o przetwarzaniu danych. Informacje o tym, jakie dane i w jakim celu są zbierane, kto jest ich administratorem (i jak się z nim skontaktować), jakim podmiotom mogą zostać udostępnione, oraz o prawach przysługujących osobom, których dane dotyczą, mają być przekazywane w zwięzłej, przejrzystej i łatwo dostępnej formie, z użyciem prostego i zrozumiałego języka. Czytanie regulaminów nie powinno dłużej stanowić udręki (nawet dla prawników), powinno faktycznie umożliwiać zrozumienie, na co wyrażamy zgodę. Jeśli nasze dane wykorzystywane będą w procesie automatycznego podejmowania decyzji, w tym profilowania, powinniśmy być również o tym wyraźnie informowani, tak aby móc poznać logikę działań podejmowanych na naszych danych i przewidywane konsekwencje takiego ich przetwarzania.

7. Możliwość przenoszenia danych. Po wejściu życie rozporządzenia nie tylko będziemy mogli zażądać od administratora danych informacji o tym, jakie dane o nas posiada, ale także – w przypadku danych przetwarzanych elektronicznie – otrzymać je zapisane w powszechnie wykorzystywanym formacie i bez przeszkód przenieść je do innego usługodawcy.

8. Ograniczenie profilowania. Zgodnie z rozporządzeniem

obywatele mają prawo nie podlegać decyzjom opartym w pełni na zautomatyzowanym przetwarzaniu danych, w tym profilowaniu, które powodować będzie skutki prawne lub w inny istotny sposób wpływać na ich sytuację. Profilowanie będzie dopuszczalne, jeśli administrator danych wykaże, że ma podstawę prawną do takiego działania (może to być niezbędne do realizacji umowy, wynikać z przepisów prawa lub można bazować na zgodzie osoby, której dane dotyczą). Będziemy mogli sprzeciwić się wykorzystywaniu naszych danych do profilowania, np. gdy związane jest ono z marketingiem bezpośrednim, a przed wyrażeniem zgody na ich przetwarzanie lub przed zawarciem umowy, której realizacja wymaga profilowania, powinniśmy otrzymać informacje o tym, co będzie się działo z naszymi danymi i jakie mogą być konsekwencje takiego procesu.

9. Ochrona prywatności by design i by default. Administrator danych już na etapie planowania swoich działań związanych z przetwarzaniem danych powinien wybierać rozwiązania i narzędzia najbardziej sprzyjające ochronie prywatności i danych osobowych, a jako domyślne wybierać takie ustawienia, które również temu służą. Może to osiągnąć, wykorzystując odpowiednie środki techniczne i procedury. Dotychczas zasady te stanowiły dobrą praktykę. Po wejściu w życie rozporządzenia będą obligatoryjnym standardem działania firm.

Autorstwo: Anna Walkowiak
Źródło: Panoptykon.org