24 maja 2018 roku zacznie obowiązywać Rozporządzenie Ogólne o Ochronie Danych, na podstawie którego Unia Europejska ujednolica przepisy dotyczące przetwarzania danych osobowych dla wszystkich 28 państw członkowskich. W praktyce oznacza to konieczność wdrożenia przez polskie przedsiębiorstwa szeregu zmian o charakterze prawnym i informatycznym, które usprawnią zarządzanie danymi osobowymi oraz pozwolą uniknąć drakońskich kar za naruszenie nowych przepisów. Jak skutecznie przygotować firmę do nowych wyzwań i nie narazić jej budżetu na finansowe straty? Odpowiedzi na te pytania znaleźli uczestnicy wrześniowego Vtorku Technologicznego, czyli cyklu bezpłatnych webinarów, organizowanych przez warszawską spółkę informatyczną VECTO.

Dotychczas, Unia Europejska pozostawiała państwom członkowskim dużo swobody w zakresie zarządzania danymi osobowymi, ale już wkrótce ta wolność się skończy. Dla firm, które przetwarzanie danych osobowych traktowały dotąd po macoszemu, RODO może być szokiem. Za nieco ponad pół roku, wszystkie firmy, które gromadzą tego typu informacje będą musiały wykazać, że zrozumiały i wdrożyły m.in. procedury oceny ryzyka przetwarzania danych (ang. Data Protection Impact Assessment) oraz umożliwiły rozszerzenie formuły zgody na przetwarzanie danych. Administratora Bezpieczeństwa Informacji zastąpić ma Inspektor Ochrony Danych, a na firmy zostanie nałożony obowiązek raportowania o własnych naruszeniach.

W istocie, zmiany te oznaczają konieczność weryfikacji rozwiązań informatycznych, które w polskich firmach są obecnie stosowane. Po 24 maja przyszłego roku, przetwarzanie danych osobowych będzie możliwe wyłącznie po przeprowadzeniu analiz przetwarzania i ochrony danych osobowych. Kluczową będzie tu ocena ryzyka prywatności danych, za którą odpowiedzialność poniesie bezpośrednio zarząd. Odpowiedzialność ta sięga również innych obszarów. Zgodnie z RODO, to przedsiębiorcy poniosą wszystkie koszty doboru i wdrożenia procedur bezpieczeństwa. To oni również muszą ocenić zakres zmian, przy czym muszą one być adekwatne do charakteru i celu przetwarzania danych oraz odpowiadać na zagrożenia wynikające, np. z cyberprzestępczości. Ryzyko kradzieży danych, czy wycieku informacji o klientach, które w Polsce przecież zdarzają się dość często, w świetle nowych przepisów powinno być zminimalizowane, a nawet jeśli do nich dojdzie, to wdrożone rozwiązania umożliwiać będą błyskawiczną reakcję.

Za podjęcie działań wyjaśniających i naprawczych odpowiedzialny będzie Inspektor Ochrony Danych. Jego obowiązkiem będzie również zgłoszenie organowi nadzorczemu wszelkich naruszeń w terminie 72 godzin od ich wystąpienia.

W przypadku incydentów, które mogą naruszać prawa lub wolności osób fizycznych, Inspektor będzie musiał poinformować o tym samych zainteresowanych, również poprzez media.

„Coraz częściej otrzymujemy zapytania ze strony polskich firm, jak od strony informatycznej skutecznie zabezpieczyć procesy pozyskiwania i zarządzania danymi osobowymi. Oznacza to, że RODO powoli zadamawia się w świadomości zarządów. Zachęcam jednak do tego, by nie zostawiać dostosowywania procedur do nowych regulacji prawnych na ostatnią chwilę. To zawsze rodzi dodatkowe koszty oraz ryzyko wprowadzenia rozwiązań, które mogą być nieadekwatne

do realnych potrzeb." – podsumowuje Kuba Wychowański, członek zarządu VECTO.

Jeśli przedsiębiorca ma wątpliwości odnośnie słuszności zapisów RODO, do ich przestrzegania zachęci go… system kar. Stwierdzenie nieprawidłowości w zabezpieczeniu danych osobowych może skutkować grzywną w wysokości do 20 mln euro lub 4% obrotu z poprzedniego roku.

Zapis wideo webinaru (dostęp bezpłatny):
TSUNAMI RODO - CZĘŚĆ WPROWADZAJĄCA DO NOWEGO ROZPORZĄDZENIA (GDPR)
Link:
http://vtorektechnologiczny.pl/archiwum/11_tsunami-rodo---czesc-wprowadzajaca-do-nowego-rozporzadzenia-gdpr

VECTO