RODO od strony IT: czy to naprawdę rewolucja?

Wdrożenie zasad unijnego rozporządzenia RODO to obecnie niezwykle gorący temat. Przepisy, które zaczną obowiązywać 25 maja, stanowią wyzwanie o charakterze prawnym i organizacyjnym. Wiele firm nie do końca jednak zdaje sobie sprawę z tego, jak od strony informatycznej podejść do wprowadzenia w życie nowego rozporządzenia. Co powinniśmy wiedzieć o RODO, żeby uniknąć przykrych niespodzianek?

RODO a zabezpieczenia IT

Celem unijnego rozporządzenia jest ujednolicenie przepisów dotyczących ochrony danych osobowych we wszystkich krajów członkowskich, ale nie tylko, bowiem RODO swoim zasięgiem będzie dotyczyć również firm spoza Europejskiego Obszaru Wspólnoty Gospodarczej, które przetwarzają dane osobowe obywateli Unii. Dla niektórych podmiotów gospodarczych RODO może okazać się rewolucją, bowiem oparte jest na analizie ryzyka danych osobowych, co bez wątpienia jest nowością.

Jak zwraca uwagę Damian Dziuba – ekspert z zakresu ochrony danych osobowych w Spółce Serwis Personalny Sp. z o.o. – jednym z największych wyzwań wprowadzonych przez nowe rozporządzenie w branży IT będzie określenie miejsca położenia serwera – na terenie UE, czy poza nią, co będzie mieć wpływ na transgraniczne przetwarzanie danych osobowych, szczególnie gdy korzystamy z usług chmurowych. RODO wprowadza konieczność realizacji nowych praw osób fizycznych, chociażby prawa do bycia zapomnianym, prowadzenia rejestr czynności przetwarzania, czy zgłaszanie naruszeń odpowiedniemu organowi nadzorczemu, a także w niektórych przypadkach współpracy z Inspektorem Ochrony Danych Osobowych. Zgodnie z RODO najważniejszy jest wysoki poziom bezpieczeństwa danych osobowych, w tym m.in. kontroli nad miejscami ich przechowywania, czasem i celem przetwarzania, stworzenia systemu udostępniania informacji, czy zawiadamiania o naruszeniach bezpieczeństwa; burzliwa dyskusja o RODO wywiązała się także w środowiskach związanych z sektorem IT. Firmy korzystające z systemów informatycznych już od dawna powinny mieć odpowiednie zabezpieczenia, zwłaszcza w dobie Internetu Rzeczy, rozwiązań chmurowych i przy ogromnym ryzyku cyberataków. RODO jest ostatnim dzwonkiem do modernizacji infrastruktury informatycznej, tym bardziej, że za nieprzestrzeganie prawa grożą wysokie kary, sięgające nawet 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa.

Jak wdrożyć zasady RODO w swojej firmie?

Branża IT jest bardzo dynamiczna. Co roku pojawiają się nowe rozwiązania systemowe, możliwości ochrony danych, ale i nowe zagrożenia. Unijne rozporządzenie ma być niezależnie od rozwoju technologii, dlatego właśnie nie zawiera konkretnych wytycznych dotyczących ochrony danych osobowych, poza sugerowanym szyfrowaniem oraz pseudonimizacją danych osobowych i zapewnieniem ciągłości działania. Oznacza to, że firmy muszą dostosować zabezpieczenia do charakteru swojej działalności. *Adaptacja infrastruktury IT do nowych przepisów musi opierać się na audycie przeprowadzonym przez specjalistę się w ochronie danych osobowych, pożądany byłby audytor Systemu Zarządzania Bezpieczeństwem Informacji normy ISO: 27001* – mówi Maciej Pokrzywiński, dyrektor generalny IT Company. Prawidłowo przeprowadzony audyt powinien oceniać funkcjonowanie obecnego systemu ochrony danych osobowych, ze wskazaniem, które elementy wymagają dostosowania do RODO i w jaki sposób należy te zmiany wprowadzić. Zadaniem specjalistów z dziedziny ochrony danych osobowych konieczne jest także przygotowanie niezbędnej dokumentacji (w tym polityki prywatności, oceny skutków przetwarzania danych, umów powierzenia dla Procesorów, itp.), łącznie około 60 dokumentów wraz z wdrożonymi procedurami, co powinno zapewnić nam tzw. rozliczalność z RODO. Dokonanie oceny danych osobowych przy współpracy z wybraną firmą IT może zająć się wdrożeniem procedur i adaptacją infrastruktury do nowych przepisów. Wybierając odpowiedniego partnera należy postępować niezwykle ostrożnie, ponieważ na rynku nie brakuje osób chcących skorzystać na niewiedzy innych. Jeśli otrzymamy ofertę wprowadzenia zmian bez wcześniejszej analizy zjawisk przetwarzania danych osobowych w danej firmie, bez uprzednich konsultacji i wstępnego audytu, w naszej głowie powinno zapalić się ostrzegawcze światełko. Po wdrożeniu zmian zaplanowanych po przeprowadzonym audycie należy jeszcze upewnić się, że wszystko poszło zgodnie z planem. W tym celu trzeba zweryfikować wprowadzone zmiany i jeszcze raz dokonać analizy systemu ochrony danych osobowych. *Należy także pamiętać o bieżącym monitorowaniu funkcjonalności systemu i utrzymywaniu zgodności z zasadami RODO. Aby zapobiec wszelkim nieprawidłowościom, nad systemem ochrony danych osobowych musi czuwać odpowiednio przeszkolony zespół. Ponadto, system powinien podlegać cyklicznym ocenom dokonywanym przez niezależnych specjalistów* – podsumowuje Maciej Pokrzywiński, bowiem *RODO to proces, a nie stan*, jak dodaje Damian Dziuba, zwracając jeszcze uwagę na konieczność edukowania pracowników w zakresie ochrony danych osobowych, bowiem to oni są najsłabszym ogniwem w polityce ochrony danych.

***

IT Company Sp. z o.o.

Firma IT Company powstała w 2007 roku w Poznaniu. Specjalizujemy się w outsourcingu IT dla średnich i dużych firm z oddziałami w całej Polsce.

Kontakt dla mediów
Maciej Pokrzywiński
Dyrektor Generalny

biuro 61 668 27 49
kom. 501 039 194
e-mail: maciej.pokrzywinski@itcompany.pl