Nie ma RODOodpornych

Rozporządzenie o Ochronie Danych Osobowych dotyczy wszystkich firm, od międzynarodowych korporacji do działających w pojedynkę freelancerów. Nie ma wyjątków i każda firma może stanąć przed koniecznością zapłacenia 20 milionów euro kary – mówi Piotr Fabiański, prezes Infonet Projekt SA.

▪ Jakie firmy powinny się przygotować na nadejście Rozporządzenia o Ochronie Danych Osobowych?
Najkrócej mówiąc – wszystkie. Z aktu prawnego wyraźnie wynika, że swoją politykę ochrony danych muszą dostosować firmy, które je przetwarzają. Nie wskazuje przy tym na konkretny obrót, jaki muszą posiadać czy ilość zatrudnionych pracowników. RODO obowiązuje zarówno banki i fundusze inwestycyjne, jak i działającego w pojedynkę programistę czy grafika.

▪ W jaki sposób więc można dostosować swoją firmę do tych wymagań?
RODO jest zupełnie innym aktem prawnym niż Ustawa o ochronie danych osobowych, wprowadzająca, między innymi, obowiązek zmiany hasła do systemu co 30 dni. Na jej podstawie można było stworzyć listę z punktami do „odhaczenia", by mieć pewność, że firma działa zgodnie z prawem.

Tymczasem na szczeblu unijnym ustawodawca stworzył akt prawny, który wymaga od przedsiębiorcy „zapewnienia możliwie najlepszej możliwej ochrony" w ramach „dostępnej wiedzy". Brakuje ścisłych wymagań.

▪ To mało precyzyjne.
Dlatego RODO bywa określane „inteligentnym" aktem prawnym, gdyż może być stosowane uniwersalnie,

niezależnie od wielkości firmy, a nawet rodzaju stosowanej technologii. Obecnie rozwój technologii jest tak szybki, że być może za kilka lat komputery kwantowe będą w kwadrans łamały najlepsze obecnie dostępne szyfry. W takiej sytuacji zapisanie w ustawie sztywnych wymagań dotyczących hasła i technologii szyfrowania nie ma sensu. Dla przedsiębiorcy konieczność wyboru między zapewnieniem firmie realnego bezpieczeństwa a zgodnością z prawem to jeden z najgorszych koszmarów, zwłaszcza jeśli te wymagania się wzajemnie wykluczają.

▪ Co więc w praktyce oznaczają te sformułowania?
To konieczność stworzenia odpowiednich procedur dotyczących bezpieczeństwa informacji, pilnowania ich przestrzegania, a w razie incydentu, na przykład wycieku danych – wykazania, że faktycznie wszystkie możliwe narzędzia ochrony zostały wykorzystane. Tylko tyle i aż tyle.

▪ Czy może Pan podać jakiś przykład?
Oczywiście. Duża firma z sektora medycznego przetwarza dane wrażliwe, których wyciek będzie stanowił dla ludzi ich dotyczących ogromne zagrożenie. Ma też środki, by zakupić skanery bezpieczeństwa lub wynająć specjalistów od cyberbezpieczeństwa. Jeśli dojdzie do wycieku, a śledztwo wykaże, że firma nie przeprowadziła w swojej historii ani jednego testu bezpieczeństwa, będzie to oczywisty przykład zaniedbania.

Z drugiej strony mamy kilkuosobowe studio projektowe pracujące głównie dla firm. Oni również przetwarzają dane osobowe, choćby dotyczące własnych pracowników. Jednak firma dysponuje znacznie skromniejszym budżetem niż wspomniana spółka medyczna i zwyczajnie jej nie stać na wynajęcie specjalisty od zabezpieczeń. W takiej sytuacji powinna opracować jasną politykę ochrony informacji oraz znaleźć bezpiecznego dostawcę usług, który w razie potrzeby może potwierdzić zgodność wszystkich swoich działań z RODO. Takim dostawcą jest choćby Microsoft. Jeśli wszystkie dane klientów trzymane są w chmurze Azure, a dostęp do nich kontrolowany, mało prawdopodobne, by inspektorzy podważyli sens takiego działania. Jest to oczywiście uproszczony przykład.

▪ Jakie są największe wyzwania związane z zarządzaniem danymi w większych organizacjach?
Nasze doświadczenia wskazują, że pierwszym krokiem powinno być wprowadzenie ładu w danych i systemach informatycznych. Konieczna jest ich inwentaryzacja, być może ujednolicenie oraz wskazanie, kto jest za dany system informatyczny lub zbiór danych odpowiedzialny. Następnym krokiem jest skontrolowanie, kto ma do nich dostęp, czy faktycznie go potrzebuje oraz do czego je wykorzystuje.

Ważne jest także ustalenie, co się dzieje z komputerami, na których te dane są przechowywane. Być może wszystkie procedury są zachowane, jednak użytkownik zainstalował niedozwolone oprogramowanie, które zostało zainfekowane i wykrada informacje. Jeśli komputerów w firmie jest 5, to wykrycie tego nie jest problemem. Jeśli jest ich 200, intruz może pozostać niezauważony tygodniami i doprowadzić do katastrofy.

Jednym z rozwiązań jest ITManager, oferowane przez Infonet Projekt narzędzie do zarządzania procesami oraz infrastrukturą IT.

▪ Jakie problemy to oprogramowanie rozwiązuje?
Przede wszystkim daje administratorowi szybki dostęp do wszystkich wykorzystywanych w firmie komputerów. Można łatwo sprawdzić, kto jest użytkownikiem komputera, jakie aplikacje zainstalował, jakie strony WWW przeglądał oraz czy nie kopiuje na zewnętrzne nośniki danych wrażliwych.

Narzędzie pozwala również kontrolować uprawnienia użytkowników, zarządzać ich nadawaniem oraz odbieraniem. Podstawową korzyścią wynikającą z zastosowania systemu jest bieżące posiadanie wiedzy kto, do jakich danych oraz systemów informatycznych ma dostęp, kiedy został on dodany, kto na to wyraził zgodę. Gdy wiadomo, kto ma dostęp do informacji, można zweryfikować, czy faktycznie go potrzebuje, a w przypadku ewentualnego wycieku łatwiej zidentyfikować jego miejsce.

Wszystkie te informacje dostępne są przy kilku kliknięciach. Tym samym nie ma potrzeby przekopywania się przez sterty dokumentacji. Narzędzie pozwala wygenerować szybki raport dotyczący bezpieczeństwa infrastruktury, który załączony do dokumentacji jest wystarczający na potrzeby zgodności z RODO.

▪ Czy takie zabezpieczenia wystarczą?
Wszystko zależy od skali działalności, branży i specyfiki firmy. W wielu organizacjach konieczna może być weryfikacja umów z podwykonawcami. Jednak w zakresie kontroli dostępu do danych osobowych oraz uprawnień pracowników z całą pewnością mogę powiedzieć – tak. To wystarczy.