

Biznes „as usual”?

RODO może to zmienić

RODO w dużym stopniu odnosi się do zasad przechowywania danych osobowych. Przedsiębiorcy mogą się ograniczyć do zakupu pancernych szaf, w których będą trzymać dokumenty i nośniki informacji. Spełnią wymagania, ale nie jest to działanie rozwojowe.

Jednym z kluczowych celów RODO było wprowadzenie zmian mających wpłynąć na sposób myślenia o ochronie danych, a nie tylko „podrasować” narzędzia. Za błędy w przechowywaniu danych, odpowiedzialny jest przede wszystkim człowiek, jego świadomość i dbałość. Rozporządzenie RODO dyscyplinuje w zakresie odpowiedzialności, wymieniając cały wachlarz kar dla tych, którzy nie planują poddać się temu procesowi w odpowiedni sposób.

Problemy ze spełnieniem wymogów RODO generuje również dług technologiczny (technologiczne zapóźnienie). Często w firmach nie do końca było wiadomo, jak ruszyć wszystkie „nagromadzone” technologie, żeby nie „zawaliła się” cała struktura informatyczna. Konsekwencji tego problemu najczęściej obawiali się przedsiębiorcy, z którymi prowadziłam rozmowy o ochronie danych.

RODO to impuls do tego, aby zadbać o ochronę danych nie tylko doraźnie, ale też na przyszłość. Wielu przedsiębiorców wspomina w rozmowach, że chcieliby prowadzić swoje biznesy „as usual” (jak dotychczas), ale czy to jest jeszcze możliwe, gdy wszystko dynamicznie się zmienia? Sami też oczekują zmian: ma być szybko, nowoczesnie, bezpiecznie i tanio. Ale jak to zrobić? Wybór tanich, niesprawdzonych lub darmowych „zabezpieczeń” kończy się ostatecznie na złych doświadczeniach np. z wirusami szyfrującymi dane i żądaniami okupu w zamian na ich odzyskanie czy też nieskuteczną ochroną przed innymi atakami hakerskimi.

Wejście w życie RODO dało firmom szansę na zweryfikowanie swoich procedur, dokumentacji, systemów informatycznych, zabezpieczeń infrastruktury IT oraz kompetencji osób, które się tym zajmują. Na co dzień nie robi się tego na taką skalę. RODO zainicjowało dyskusję o tym, jakie mamy skuteczne narzędzia, a czego nam brakuje, aby stworzyć bezpieczne warunki przechowywania danych.

RODO już jest i w związku z tym przedsiębiorcy mają nowe zadania. Jednym z nich jest potrzeba wprowadzania spójnych rozwiązań, które długoterminowo zabezpieczą przechowywane dane. Kolejnym, powinna być większa

otwartość na dyskusję o nowych technologiach i nowych dostawcach, którzy specjalizują się w przechowywaniu danych i dają gwarancję na świadczone przez siebie usługi. Ochrona danych w cyberprzestrzeni nie może być realizowana przez jedną osobę zatrudnioną w dziale IT. Sprawa jest na tyle poważna, że tą odpowiedzialność ceduje się na firmy, które się w tym specjalizują. Nie wystarczy już zastosowanie tego samego podejścia jak dotychczas, żeby długofalowo spełnić wymagania w zakresie ochrony danych. W cyfrowym świecie każdego dnia rośnie liczba ataków, które mają na celu wejście w posiadanie danych w sposób nieuprawniony. Dobrym i bezpiecznym rozwiązaniem w zakresie ich ochrony jest prywatna chmura obliczeniowa. Usługa ta jest świadczona przez profesjonalne serwerownie, których w Polsce jest kilkadziesiąt. Taki wybór gwarantuje, że przedsiębiorca zawsze będzie wiedział, w jakim konkretnym miejscu są przechowywane jego dane, a nie jak to jest w przypadku np. chmur publicznych, że dane przechowywane są „gdzieś” na świecie. Poza tym, z polskim dostawcą prywatnej chmury, przedsiębiorca może omówić specyfikę swojego biznesu i podjąć decyzję o wprowadzeniu dodatkowych rozwiązań zabezpieczających. Nie należy mieć oporów przed korzystaniem z takich usług, ponieważ to dostawca przejmuje na siebie znaczną odpowiedzialność za stosowane zabezpieczenia, mając do tego odpowiednie narzędzia i często ogromne doświadczenie.



Jola Uzdzička

Dyrektor sprzedaży i marketingu w Sinersio Polska. Związana z rynkiem IT od ponad 12 lat. Posiada dużą wiedzę i doświadczenie z zakresu procesów biznesowych, doboru i wdrażania systemów klasy ERP, technologii chmury obliczeniowej oraz bezpiecznego przetwarzania danych. Wspiera procesy cyfryzacji w firmach z sektora MSP.