RODO

Najistotniejsze zmiany w ochronie danych osobowych

Rozporządzenie o ochronie danych osobowych – inaczej RODO – nakłada więcej obowiązków na przedsiębiorców przechowujących dane osobowe oraz dotyczy praktycznie każdego przedsiębiorcy. Dostosować się do nowych przepisów musi się zarówno piekarz czy cukiernik, jak i ogromna firma zatrudniająca wielu pracowników.

Nowe przepisy RODO

Zakres obowiązków spoczywających na przedsiębiorcach w zakresie wprowadzenia RODO nie zależy od tego, jak duża jest firma, ale od tego, ile danych zgromadziła. Zasada wynikająca z przepisów RODO jest taka, że to przedsiębiorca będzie musiał wykazać, że zastosowane metody danych osobowych są wystarczające dla ich zabezpieczenia. Warto zatem przeprowadzić w firmie audyt – audytor może sprawdzić, czy firma posiada wszystkie wymagane prawem zgody na przetwarzanie danych oraz czy zawarła odpowiednie umowy, wskazujące odpowiedzialnych za zarządzanie danymi, a także czy umowy zlecające usługi na zewnątrz (np. obsługa kadrowo-płacowa) gwarantują bezpieczeństwo przepływu danych. Konieczne jest też sprawdzenie samej procedury przepływu informacji wewnątrz firmy, czyli czy dane osobowe są bezpieczne na każdym etapie ich przetwarzania. Warto również zamówić inwentaryzację danych, które firma posiada.

Po 25 maja 2018 r. firmy będą musiały udowodnić, że dane osobowe są odpowiednio zabezpieczone. Kary za niewdrożenie odpowiednich przepisów wewnętrznych są wysokie – maksymalnie mogą wynosić 4% obrotów rocznych firmy lub 20 mln euro.

Kara pieniężna

W przypadku niewdrożenia przez firmę odpowiednich procedur, które osoby kontrolujące ocenią jako zabezpieczające dane osobowe w sposób nienależyty, na przedsiębiorcę może być nałożona kara pieniężna – maksymalna wysokość takiej kary to 4% obrotów rocznych firmy lub nawet 20 mln euro. Wysokość kary zależy od decyzji urzędnika, który będzie analizował sprawę. Firma może zostać ukarana za sam fakt niepoinformowania osób, których dane przetwarza o tym, że posiada ich dane. Kara może zostać nałożona na przedsiębiorcę również w sytuacji „wycieku" danych osobowych z systemów firmy. Bardzo istotna w takiej sytuacji jest

warto wiedzieć

Regularna kontrola danych osobowych

Po dokonaniu audytu w firmie, a więc po zidentyfikowaniu, gdzie są przechowywane dane osobowe, należy zlecić ewentualną modernizację systemu informatycznego – np. zaszyfrować dyski czy pendrive'a używane przez pracowników lub też zakupić odpowiednie oprogramowanie. Poziom ochrony danych w formie, w myśl nowych przepisów, ma być kontrolowany regularnie. Działania w takim zakresie wykonują inspektorzy ochrony danych osobowych. Mniejsi przedsiębiorcy na pewno nie będą zatrudniać inspektorów ochrony danych, ale mogą „wynająć" takiego inspektora od wyspecjalizowanych firm.

przyczyna „wycieku" – jeżeli jest ona spowodowana zaniedbaniami – polegającymi np. na niewłaściwym zabezpieczeniu systemu informatycznego lub niezaszyfrowaniem pendrive'a z danymi, który niechcący zgubił pracownik – kara może być wysoka. Urzędnicy inaczej spojrzą na sytuacje, w których „wyciek" danych został spowodowany przez włamanie do systemu – wówczas powinno się raczej skoncentrować na jego uszczelnieniu – tak, aby takie zdarzenia nie miały miejsca w przyszłości.

Jak przedsiębiorcy powinni przygotować się do RODO?

Przepisy RODO są dość ogólne i mówią o potrzebie zapewnienia „odpowiedniego poziomu bezpieczeństwa", nie wskazują natomiast, jakie konkretne rozwiązania firma powinna wdrożyć, aby nie została ukarana. Zdaniem fachowców najważniejsze jest, aby systemy informatyczne używane w firmie zapewniały ochronę danych (uniemożliwiając m.in. ich wyciek i dostanie się „w ręce" osób niepowołanych), zarówno w związku z przechowywaniem danych, jak i zarządzaniem tymi danymi. Ważne jest, aby firma korzystała z serwera gwarantującego bezpieczne przechowywanie danych oraz ich odzyskanie w przypadku awarii. Firma powinna mieć system informatyczny, który chroni przed wyciekiem danych na zewnątrz oraz jest dobrze zabezpieczony przed ewentualnym atakiem (czyli próbą nielegalnego pozyskania z zewnątrz gromadzonych danych). Pomocne w tym celu będą albo specjalne aplikacje czy urządzenia, a nawet całe systemy służące zabezpieczeniu danych.

Jak zagwarantować bezpieczeństwo danych w firmie?

Przedsiębiorca powinien wdrożyć stosowne procedury, z których będzie wynikało, jakie osoby będą miały dostęp do danych, i jak będzie następowało uwierzytelnianie dostępu przez te osoby do systemu, w którym są gromadzone dane. Dotychczas stosowane hasła mogą okazać się niewystarczające – można więc używać tzw. tokenów (czyli haseł dynamicznych) lub specjalnych certyfikatów zapewniających wysoki poziom bezpieczeństwa danych. Należy pamiętać o tym, że samo zabezpieczenie sieci informatycznej nie wystarczy – kara może zostać nałożona jeżeli informacje, które powinny być chronione, wydostaną się na zewnątrz, np. z powodu kradzieży firmowego laptopa, zgubienia dysku czy pendrive'a, na którym są dane podlegające ochronie. Takie nośniki można odpowiednio zaszyfrować, aby nawet w przypadku ich utraty osoba nieuprawniona nie miała dostępu do danych.

Podsumowanie

Przepisy RODO zostały tak skonstruowane, aby były pomocne dla przedsiębiorców, którzy poważnie podeszli do obowiązku zabezpieczenia danych. Można mieć świetnie zabezpieczoną sieć IT w firmie, a do wycieku danych i w konsekwencji kary za incydent dojdzie z prozaicznego powodu – fizycznej kradzieży sprzętu czy zgubienia dysku lub innego przenośnego medium. Dlatego przy opracowywaniu koncepcji ochrony danych przed wejściem w życie RODO, warto rozważyć opcję zaszyfrowania dysków i innych urządzeń do przechowywania danych. Jeżeli zatem dojdzie do wycieku danych, to od razu należy poinformować osoby zainteresowane, jeżeli się tego nie zrobi w przeciągu 72 godz., to może zostać nałożona kara. ❑

Piśmiennictwo dostępne u autorki.

Tekst: Agnieszka Bagieńska-Petryka,
radca prawny, Petryka Kancelaria Prawna

warto wiedzieć

Dlaczego inwentaryzacja danych jest ważna?

W sytuacji, gdy osoba, której dane przetwarza firma zażąda ich usunięcia, do czego jest uprawniona zgodnie z przepisami RODO – przedsiębiorca jest zobowiązany do usunięcia tych danych ze wszystkich „miejsc", w których te dane się znajdują, tj. z papierowego archiwum, cyfrowej bazy danych i bazy klientów. Jeżeli firma nie wie, gdzie takie dane mogą się znajdować, to w przypadku kontroli może zostać nałożona na nią kara. Zgodnie z ogólnodostępnymi informacjami ogromna ilość zasobów zgromadzonych na serwerach to tzw. dane zapomniane, tj. takie, których przedsiębiorcy nie usunęli – często dlatego, że nie zdają sobie sprawy, że te dane, np. w określonych systemach informatycznych, są przechowywane.