Retencja danych osobowych - czym jest i dlaczego warto o niej pamiętać

Każdy z Nas, na pewno niejednokrotnie, spotkał się ze stwierdzeniem *„Nie wyrzucaj tego dokumentu, może się jeszcze na coś przydać”.* W rezultacie, w firmach przechowywanych jest mnóstwo archiwalnych dokumentów. Takie podejście, oprócz tego, że powoduje zapychanie szuflad i szaf naraża Nas także na ryzyko naruszenia przepisów o ochronie danych osobowych.

Retencja danych w RODO

Zgodnie z przepisami Ogólnego rozporządzenia ochronie danych (RODO) dane osobowe powinny być przechowane **przez okres nie dłuższy niż jest to niezbędne** do celów, w których dane są przetwarzane. Od tej ogólnej zasady, są przewidziane pewne wyjątki zezwalające na dłuższe przechowanie danych np. do celów archiwalnych w interesie publicznym, celów badań naukowych, historycznych lub statystycznych. Wspominane wyjątki mają jednak dość ograniczone zastosowanie, dlatego też niezbędne jest, **aby każdy administrator danych ustalił „niezbędny” dla siebie okres przechowania danych. Okres ten zwany jest właśnie okresem retencji danych osobowych.**

Ustalenie okresu retencji jest uzależnione od celu dla jakiego przetwarzane są dane. Inny będzie okres retencji danych klientów sklepu internetowego, którzy kupili produkt, a inny dla danych z księgi wejść/wyjść gości prowadzonej przez recepcję firmy. Wskazówką dla wyznaczania okresu retencji, bardzo często będzie okres przedawnienia roszczeń jaki jest związany z daną czynnością, dla której zbierane są dane. W odniesieniu do sprzedaży produktów, często będzie to okres przedawnienia zobowiązań podatkowych. Okres retencji może być także wyznaczony przez przepisy prawa. Tak będzie np. w przypadku danych znajdujących w aktach osobowych pracowników lub nagrań z monitoringu wizyjnego stosowanego w zakładzie pracy.

Dlaczego ustalenie odpowiednich zasad retencji, a następnie ich respektowanie jest takie ważne?

Wyobraźmy sobie sytuację, że firma nie ustaliła okresów retencji i przechowuje na swoich serwerach dane sprzedażowe od początku swojego istnienia, czyli od 20 lat. Jeśli doszłoby do ataku hakerskiego na te serwery i wycieku danych z systemu, który zarządza tą bazą to wówczas tysiące, a nawet i dziesiątki tysięcy rekordów z danymi osobowymi mogłoby trafić do nieupoważnionych osób.

W takim przypadku, biorąc pod uwagę utratę kontroli nad bardzo dużą ilość danych, tego rodzaju incydent mógłby zostać zakwalifikowany jako naruszanie ochrony danych osobowych opisane w art. 33 RODO. Wiąże się z tym konieczność natychmiastowej reakcji ze strony administratora, czyli przede wszystkim obowiązek niezwłocznego (a nie później niż w ciągu 72 godzin) poinformowania o takim incydencie Prezesa Urzędu Ochrony Danych Osobowych. W zależności od okoliczności incydentu i jego skali, może nawet dojść do konieczności zawiadomienia o takim incydencie także osób, których dane zostały utracone (art. 34 RODO). Dalszą konsekwencją dla administratora, wywołaną tego rodzaju incydentem, mogłoby być także wszczęcie przez Prezesa Urzędu Ochrony Danych Osobowych postępowania kontrolnego – po to aby zweryfikować poziom przestrzegania przez tą firmę przepisów o ochronie danych osobowych. Nie można również wykluczyć powództw cywilnych składanych ze strony osób, których dane zostały naruszone.

Co w opisanej wyżej sytuacji zmieniłoby, gdyby ta firma miała odpowiednio ustalone okresy retencji?

Oczywiście nie sprawiłoby to, że do takiego ataku hakerskiego by nie doszło. **Jeśli jednak ustalone zostałyby okresy retencji i dla procesu sprzedażowego przyjętoby, jako okres przechowywania danych, termin przedawnienia roszczeń podatkowych, to w takiej sytuacji ilość przechowanych danych byłaby istotnie mniejsza.** Zgodnie bowiem z art. 70 § 1 ustawy Ordynacja podatkowa zobowiązanie podatkowe przedawnia się z upływem 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku.

Jeśli więc dane sprzedażowe, co do których okres przedawnienia zobowiązań podatkowych już upłynął, nie znajdowałby się na tym serwerze, to nie padłyby „ofiarą" ataku. Na tym przykładzie widać więc, że **ustalenie i przestrzegania zasad retencji oznacza ograniczenie ilości przechowanych danych, a tym samym także zmniejszenie ilości danych których mógłby dotyczyć potencjalny incydent.** Tak jak już zostało to opisane powyżej, ilość danych może mieć istotne znaczenie dla oszacowania skali incydentu oraz jego konsekwencji dla administratora.

Warto o tym pamiętać, szczególnie teraz, gdy zbliża się koniec roku kalendarzowego, a wraz z nim będą się przedawniały zobowiązania podatkowe z kolejnego roku.

Autor artykułu:

Marcin Szkutnik

Źródła:

- Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- Ustawa z dnia 29 sierpnia 1997 r.- Ordynacja podatkowa (tj.z dnia 23 marca 2018 r.Dz.U. z 2018 r. poz. 800)