Warszawa, 15.01.2024 r.

Po co mi retencja danych osobowych?

Jednym z obszarów ochrony danych osobowych, który nadal sprawia duże trudności przedsiębiorcom, jest obowiązek ustalenia i egzekwowania okresów retencji danych osobowych. Czyli tłumacząc z polskiego prawniczego na polski potoczny: chodzi o to, że danych osobowych (dokumentów, maili, plików, itp.) nie można trzymać w nieskończoność. Tylko dlaczego, jak się przed tym bronić i czy naprawdę trzeba to robić?
Nad tematem retencji danych pochylaliśmy się już na Blogu iSecure wcześniej: Marcin Stryszko pisał o retencji danych w sklepach internetowych, Agnieszka Dominiak w kontekście rekrutacji, a Maciej Łukaszewicz – analizując dopuszczalność utrzymywania skrzynki e-mail byłego pracownika.
Celem niniejszego tekstu jest pokazanie, dlaczego żadna firma nie może przechowywać danych w nieskończoność. I zwrócenie uwagi, że to nie tylko smutny obowiązek regulacyjny, ale działanie, które może przynieść korzyść firmie, a nawet przewagę konkurencyjną. Temat jest o tyle palący, że przez pierwszych 5 lat obowiązywania RODO wielu mówiło sobie „ten temat może poczekać, przecież RODO dopiero weszło w życie". Niestety od 25 maja 2018 r. minęło już pond 6 lat i jeżeli już nie zaczęliśmy usuwać starych danych, to możemy mieć problem.

Czy na pewno nie mogę trzymać dokumentów na wszelki wypadek w nieskończoność?

Art. 5 ust. 1 lit. e) RODO jest brutalnie jednoznaczny: „*Dane osobowe muszą być […] przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane*".
Z powyższego zapisu wynikają dwa istotne wnioski:

- żadnych danych osobowych nie można trzymać w nieskończoność;
- administrator danych (firma) może ustalić taki okres retencji, jaki jest mu potrzebny dla realizacji założonych celów.

Zatem każdy dokument w firmie, każdy e-mail musi mieć odpowiednik „daty przydatności do spożycia", po upływie której powinien zostać trwale usunięty, bądź zanonimizowany.

Ale może jednak to będzie kiedyś potrzebne?

To bardzo częsty argument w rozmowie o ustalaniu okresów retencji. A co będzie, jeżeli za 3 lata ktoś nas pozwie o złe wykonanie tego kontraktu i nie będziemy mieli maili, zleceń, dowodów zapłaty?[1] To oczywiście bardzo ważkie pytanie, którego nie można zignorować. Nawet osoby bez wykształcenia prawniczego mają świadomość, że sprawiedliwość sprawiedliwością, ale w sądach wygrywają ludzie z lepszymi prawnika... dowodami. A jeżeli klient pozywa firmę o to, że pomalowała mu biurowiec na różowo bo mu się kolor nie podoba, a firma nie mama maila w którym prezes napisał że tak, zdecydowanie i nieodwołanie chce cały budynek w kolorze „pudrowy róż cukierkowy", to sprawa będzie niezwykle trudna do wygrania.
RODO (jak i logika biznesowa) podpowiadają, by takie decyzje podejmować na podstawie twardych danych, a nie emocji. Zacznijmy zatem od pytania: jak często zdarza się, że firma potrzebuje wrócić do wiadomości e-mail sprzed 5 lat? A co, jeżeli pomimo mglistych obaw o mogący w każdej chwili przyjść odpis pozwu w ciągu ostatnich pięciu lat nie było ani jednego? A może firma działa w obszarze mocno regulowanym i w ciągu tylko ostatniego roku pięć razy mieliśmy kontrole różnych organów, którym trzeba było przedstawiać dowody na zgodność działań firmy z przepisami w 2017 roku? To oczywiście dwa lekko przerysowane przykłady, ale wskazują w jakim kierunku powinno iść rozumowanie. RODO

pozwala na pewną elastyczność działania. Jeżeli w razie kontroli możemy wykazać, że regularnie jesteśmy angażowani w procesy sądowe o tematy sprzed 5 lat, a KNF średnio raz do roku żąda od nas informacji o czynnościach, które realizowaliśmy 8 lat temu – to z punktu widzenia RODO z czystym sumieniem możemy ustalić taki okres retencji, żeby móc trzymać materiały „na wypadek kontroli/pozwu". Jeżeli jednak w 15 letniej historii firmy nie braliśmy udziału w żadnym procesie sądowym i nie działamy na rynku regulowanym – kontrola z UODO może nie uznać naszej potrzeby trzymania wszystkiego przez 10 lat „na wszelki wypadek".

Przewaga biznesowa?

Warto w tym momencie zaznaczyć, że uniknięcie potencjalnej kary za naruszenie RODO to nie jedyny zysk z przestrzegania okresów retencji danych. Jakie są inne?

1. Oszczędności na działalności operacyjnej
   Przechowywanie danych (czy to papierowych czy elektronicznych) kosztuje, zatem jeżeli trzymamy ich mniej, to mniej płacimy co miesiąc za ich składowanie.
2. Mniejsze skutki ewentualnego wycieku
   Jeżeli (odpukać) hakerzy włamią się do naszych systemów i skopiują wszystkie pliki, zgodnie z RODO mamy obowiązek powiadomić wszystkie osoby, których dane ukradzione. Jeżeli mamy mniej danych, to oznacza to mniej osób do powiadomienia (a więc niższe koszty całej operacji, mniejsze straty wizerunkowe i mniej pozwów od osób, których dane dotyczą).
3. Sprawniejsze funkcjonowanie firmy
   Pracownik będzie działał wydajniej, jeżeli jego skrzynka e-mail i system CRM nie będą obciążone dziesiątkami gigabajtów niepotrzebnych plików.
4. Zaufanie klienta
   Przejrzyste i zgodne z prawem zasady retencji danych osobowych mogą stanowić przewagę konkurencyjną, dzięki której klient wybierze nas, a nie konkurencję. Z niedawnych badań wynika, że 40 dorosłych Polaków obawia się wycieku ich danych osobowych, a około 1/3 z nich nie chce robić zakupów w sklepie internetowym, z którego wyciekły dane[2].
5. Ułatwione disaster recovery
   Jeżeli systemy nie są obciążone dziesiątkami tysięcy niepotrzebnych plików, przywrócenie ich z kopii bezpieczeństwa po katastrofie będzie dużo szybsze – a więc firma wcześniej będzie wrócić do normalnego funkcjonowania po ataku ransomware i czy powodzi.

Podsumowując i jakie mamy alternatywy

Ustalenie i egzekwowanie zgodnych z przepisami okresów retencji danych osobowych to nie tylko obowiązek każdego podmiotu działającego w Unii Europejskiej – to możliwość zyskania przewagi konkurencyjnej na rynku. Jest to też obszar, w którym dobry know-how pozwala zaoszczędzić sporo pracy – zgodnie z zasadą „work smarter, not harder".

Jak robić zasady retencji danych, żeby się nie narobić? Zasadniczo to materiał na osobną publikację, ale hasłowo warto wskazać na możliwość:

- Stosowania automatycznej anonimizacji/ usuwania dokumentów przy użyciu oprogramowania do obsługi poczty elektronicznej czy CRM,
- automatycznego archiwizowania zawartości skrzynek e-mail do osobnego, szyfrowanego zasobu [3],
- zalety regularnych audytów i badania zgodności.

Daniel Taberski – radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.

Przypisy

[1] Ogromne obciążenie pracą polskich sądów dokłada tu dodatkową warstwę problemów. Wyobraźmy sobie taką sytuację: mamy zrealizowany kontrakt, którego termin przedawnienia to 3 lata. Sprawa gospodarcza, a tymi zajmują się specjalne wydziały sądów, które należą do najbardziej obciążonych w kraju. Czyli jeżeli roszczenie uległoby przedawnieniu 31 grudnia 2024 r., całkiem niewykluczony jest następujący scenariusz: 30 grudnia nasz kontrahent złożył przeciwko nam pozew. Sędzia realnie spojrzy na niego marzec – kwiecień 2025 r. jak dobrze pójdzie. Jeżeli w pozwie są braki formalne, będzie wezwanie do ich uzupełnienia – uzupełnione w maju, ale sędzia spojrzy na niego około października i zarządzi doręczenie nam pozwu co nastąpi jakoś w listopadzie 2025 r. A my w tym czasie już usunęliśmy dane związane z tym kontraktem. A 3-4 miesiące od wpływu pisma do sądu do momentu jak sędzia weźmie je do ręki to wariant optymistyczny – autorowi znane są wydziały sądów, gdzie trwa to 6-9 miesięcy. W tej sytuacji przy ustalaniu okresów retencji ze względu na przedawnienie roszczeń realnie trzeba dodawać sobie około 12 miesięcy do okresów przedawnienia roszczeń z kodeksu cywilnego.
[2] https://www.bankier.pl/wiadomosc/Coraz-wiecej-Polakow-obawia-sie-wycieku-danych-osobowych-choc-sami-tez-jestesmy-sobie-winni-8710668.html [dostęp 07.01.2025 r.]
[3] Taką usługę dostajemy np. w ramach pakietu Google Workspace - https://workspace.google.com/intl/pl/products/vault/ [dostęp 07.01.2025 r.]