Zabezpieczenia techniczne już nie wystarczą

Poziom automatyzacji procesów w działalności firm rośnie z roku na rok. Oznacza to również coraz częstsze wykorzystanie systemów informatycznych w celu przetwarzania danych osobowych – począwszy od danych pracowniczych po szeroko rozumiane dane dotyczące klientów czy kontrahentów.

W czasie obowiązywania ustawy o ochronie danych osobowych z 1996 r. zasady zabezpieczania takich systemów określało rozporządzenie. RODO nie wprowadziło podobnego rozwiązania, dlatego administratorzy po 25 maja 2018 r. stanęli przed problemem oceny adekwatności zabezpieczeń systemów IT.

Wiem, co mam i jak to działa

RODO jednoznacznie sprecyzowało tylko trzy rodzaje zabezpieczeń, które są związane z ochroną danych osobowych, tj.

- pseudonimizacja,

- szyfrowanie danych, oraz

- testy bezpieczeństwa.

Pozostałe zabezpieczenia, jakie wymieniono w przepisach, są raczej zasadami postępowania niż jasnymi wytycznymi i każdy może je wdrożyć w inny sposób. Zatem skąd wiedzieć, jakie działania będą właściwe?

Firmy przede wszystkim powinny wykonać inwentaryzację systemów i określić, jakie dane i w jaki sposób przetwarzają. Zakres przetwarzania określają funkcjonalności systemów – program do fakturowania pozwala na inne przetwarzanie niż system do obsługi reklamacji klientów. Dopiero gdy te kwestie są jasne, można przejść do weryfikacji zabezpieczeń (audytu bezpieczeństwa systemów).

Z jednej strony mamy procedury – zasady logowania się do systemu, pracy poza firmą. Z drugiej strony istnieją techniczne aspekty działania danego systemu oraz urządzeń i sieci, w jakich uruchamiane jest oprogramowanie.

Przykład

Firma ma sieć wewnętrzną bez dostępu do internetu oraz system zainstalowany na komputerach stacjonarnych. Z założenia bezpieczeństwo danych powinno być w niej większe niż systemu, który obsługuje sklep internetowy z logowaniem z każdego miejsca na świecie. Decyduje o tym ograniczony dostęp do systemu i mniej mobilny sprzęt.

Większe bezpieczeństwo na start to mniej procedur czy programów zabezpieczających, które trzeba przygotować. Kluczowe dla ustalenia listy niezbędnych zabezpieczeń technicznych jest znalezienie słabości systemów, które mogłyby być źródłem incydentów związanych z ochroną danych osobowych, oraz sposobów na „załatanie" tych dziur, jak np. dodatkowe oprogramowanie, nowy sprzęt czy zmiana zasad pracy. Firmy, które nie monitorowały dotychczas swoich systemów pod tym kątem, muszą polegać na wiedzy i doświadczeniu osób, którym powierzą taką analizę.

Bezpieczny = dobrze zaprogramowany

Najlepszy sprzęt czy oprogramowanie monitorujące nie wystarczy, jeżeli sam system jest nieszczelny. Nie musi to oznaczać braków technicznych.

RODO wprowadza obowiązek domyślnej ochrony danych osobowych (privacy by default). W praktyce oznacza to, że systemy powinny automatycznie zapewniać bezpieczeństwo danych.

Ta ochrona ma kilka aspektów. Jeden z nich dotyczy ograniczenia ilości danych do takich, które są niezbędne do działania firmy. Na przykład do wysyłki paczki nie ma potrzeby przetwarzania numeru PESEL; system nie powinien w ogóle pozwolić na jego wprowadzenie. Niezbędne są również mechanizmy, które ochronią zebrane w systemach dane przed dostępem osób nieuprawnionych. Jak to zrobić? Wprowadzić blokowanie konta użytkownika po kilkukrotnym wpisaniu nieprawidłowego hasła czy zablokować możliwość wysyłania wiadomości e-mail zawierających określone słowa do osób spoza firmy.

Zasada domyślnej ochrony obejmuje też obowiązek ograniczenia do niezbędnego minimum operacji, jakim dane są poddawane, a także czasu, przez jaki są przechowywane. Każde konto w systemie powinno mieć uprawnienia tylko do takich działań, które mieszczą się w obowiązkach jego właściciela. Wymusza to odpowiednie skonfigurowanie systemu – najczęściej dodaje się alerty lub wyskakujące okienka, które ostrzegają o wykonywaniu niewłaściwych czynności, informują o możliwości skasowania danych czy przesłania ich między systemami. Jeżeli oprogramowanie jest właściwie zaprojektowane, automatycznie wykryje, czy to, co robimy, jest dozwolone (zgodne z RODO), czy nie, i poinformuje o możliwym problemie.

Najpierw analiza bezpieczeństwa danych

Ochrona danych osobowych w systemach przed RODO często była sprowadzana do problemu checkboxów ze zgodami albo linków do polityki bezpieczeństwa. Teraz przy aktualizacji lub wymianie systemów ten aspekt trzeba uwzględniać w pełnym zakresie już na samym początku. Taki obowiązek wynika z zasady prywatności w fazie projektowania (privacy by design). Zgodnie z nią, projektowanie zmian w systemach musi poprzedzać analiza wprowadzanych funkcjonalności pod kątem bezpieczeństwa przetwarzanych danych. Administrator musi być w stanie wykazać, że zapewnił ochronę danych osobowych. Wykonana weryfikacja powinna być więc właściwie utrwalona, np. w dokumentacji dotyczącej przygotowania zamówienia. Brak właściwej oceny przetwarzania danych osobowych przed uruchomieniem systemu może być dotkliwy w skutkach. Przekonała się o tym jedna ze szwedzkich szkół, której tamtejszy organ ochrony danych osobowych wytknął naruszenie RODO we wdrożonym systemie sprawdzania obecności uczniów na podstawie rozpoznawania ich twarzy. W tym przypadku błędne były założenia dotyczące dopuszczalności przetwarzania danych biometrycznych na podstawie zgody uczniów (brak realnej swobody uczniów co do wyrażenia zgody).

Do liftingu lub wymiany

Dostosowanie systemów do nowych wymogów to nie tylko proste wciśnięcie guzika. Niewielu przedsiębiorców w ubiegłym roku objęło audytem RODO przetwarzanie w systemach informatycznych. Jednak na rynku coraz bardziej widać zainteresowanie tym obszarem.

Należy pamiętać, że czym innym jest możliwość uruchomienia danej funkcjonalności, a czym innym dostosowanie do niej już posiadanych baz danych. Tym bardziej, że RODO wymusiło trochę nowości, np. konieczność przypisania do poszczególnych danych podstawy ich przetwarzania czy dokumentowania realizacji obowiązków informacyjnych.

Większość przedsiębiorców decyduje się dostosowywać swoje systemy stopniowo – partiami przenosi stare dane i uzupełnia brakujące informacje. Ten proces cały czas trwa, bo z reguły oznacza koszty. W przypadku systemów, które już są w użyciu, kluczowe znaczenie ma treść umowy zawartej z dostawcą. Jeżeli rozwiązanie było opracowywane w modelu, który nie zakładał systematycznej aktualizacji w razie zmian wymogów prawnych, to koszt dostosowania systemu musiała ponieść firma, która z niego korzystała.

Nie każdy system da się dostosować. Część systemów wycofano więc z użycia, zmieniając je w archiwum danych. W tym obszarze konieczna jest weryfikacja, jak długo dane mogą być przechowywane, żeby nie narazić się na kary za naruszenie zasady minimalizacji danych.

Prawo do zapomnienia

Ważnym tematem jest też obsługa żądań osób, których dane dotyczą. Na razie nie rośnie lawinowo liczba pytań o przetwarzane dane. Najpopularniejszym tematem jest ciągle prawo do zapomnienia.

Przedsiębiorcom nie zawsze jest łatwo ustalić, jakie dane poszczególnych osób przetwarzają, bo systemy nie przewidują wyszukiwania takich informacji. To problem, który muszą rozwiązać, żeby właściwie realizować obowiązki administratora danych – ręczne wyszukiwanie danych w systemach na dłuższą metę na pewno się nie sprawdzi. Wdrożenie nowych funkcjonalności wymaga odpowiedniego przygotowania. Firmy muszą mieć pewność, że wprowadzone ustawienia systemów będą działać właściwie.

Automatyczna anonimizacja czy skasowanie niewłaściwych danych stanowią incydent ochrony danych, który może prowadzić nie tylko do utraty wizerunku, ale także powstania roszczeń finansowych. Dlatego dostosowanie systemów to jeden z tematów, który w kontekście RODO nie traci na aktualności.

Skasowanie niewłaściwych danych to incydent ochrony danych, który może skończyć się roszczeniami finansowym.

Autor: Monika Bogdał, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.