

# Alert dla ochrony danych

**Prawo** Unijna reforma wymaga w firmach mobilizacji i współpracy ich szefów, prawników, informatyków, szkoleniowców. I to jak najszybciej

Iwona  
Jackowska

i.jackowska@pb.pl • 22-333-98-59

Niech nikomu się nie wydaje, że 25 maja 2018 r. to odległa data. Z punktu widzenia przygotowań do wymagań nowych zasad ochrony danych osobowych to w zasadzie bliskie jutro – zdają się mówić autorzy związanych z tym regulacji, organ nadzorujący ich przestrzeganie, prawnicy, eksperci od bezpieczeństwa. Wszyscy zachęcają przedsiębiorców, aby nie czekali do ostatniej chwili z wdrożeniem odpowiednich narzędzi i już podjęli wiele innych działań, bo nie tylko trzeba pomyśleć o rozwiązaniach technicznych, ale też opracować i przyjąć w firmach przede wszystkim politykę tej ochrony, wynikającą z wyzwań stawianych przez unijną reformę.

## Rewolucyjne zmiany

Tę reformę przyniosło ogólne rozporządzenie Parlamentu Europejskiego i Rady o ochronie danych (RODO). Ono weszło już w życie i od 25 maja przyszłego roku musi być stosowane bezpośrednio przez wszystkie kraje członkowskie Wspólnoty. W Polsce trwają teraz prace nad stworzeniem uzupełniających przepisów krajowych spójnych z unijnymi normami, aby można je było wdrożyć w praktyce.

– Unijne rozporządzenie jest regulacją rewolucyjną, chociaż niektórzy bronią się przed takimi stwierdzeniami, i niemającą swojego odpowiednika do tej pory. Wynika to nie tylko ze skali zmian, czyli wielu aktów im poddanych, ale także zupełnie innego podejścia do ochrony danych – mówi Tomasz Osiej, radca prawny z Grupy Omni Modo.

72

**proc.** ▶ Tylu badanych chce zagwarantowania tajności ich e-maili i innej korespondencji online – wynika z ankiety Eurobarometru z końca 2016 r.

71

**proc.** ▶ A tylu nie akceptuje, gdy firmy dzielą się informacjami o użytkownikach bez ich pozwolenia, nawet jeśli ma to służyć tworzeniu nowych usług zgodnych z ich potrzebami.

Zwraca on uwagę, że RODO jest wyzwaniem interdyscyplinarnym, co oznacza, że zastosowanie się do niego nie jest zadaniem wyłącznie dla prawników czy informatyków, ale także osób zajmujących się zarządzaniem procesami, zarządzaniem zmianą, odpowiadających za ocenę ryzyka w firmie czy działów szkoleń. Jedną z głównych cech reformy jest bowiem nałożenie na przetwarzających dane osobowe obowiązku szacowania możliwości wystąpienia zagrożeń dla praw i wolności osób, których dotyczą pozyskiwane informacje, i to już na etapie planowania przedsięwzięć biznesowych, z którymi może wiązać się potrzeba ich gromadzenia.

W konsekwencji należy dostosować do tego odpowiednie zabezpieczenia, dając przy tym możliwość decydowania o wyłączeniu lub ograniczeniu mechanizmów chroniących prywatność osobom korzystającym z określonych narzędzi, których dane są przetwarzane. Nie bez znaczenia przy tym jest też pozostawienie przedsiębiorcom wyboru technicznych rozwiązań służących ochronie danych, ale nie będzie zarazem pobłażania dla tych, którzy nie zadbają o nią dostatecznie.

– RODO zmienia przede wszystkim podejście do ochrony danych, wymusza aktywne działania, oparte na zasadzie ciągłej analizy ryzyka. Nie wystarczy przygotować jakąś dokumentację i pozostawić sprawę swojemu biegowi. Sądzę, że administratorzy zbiorów danych i podmioty ich wspierające będą miały problem. Trzeba się z jednej strony przestawić na mocno proaktywne działanie, ale też, albo przede wszystkim, dać taką możliwość osobom zarządzającym ochroną danych, co nie zawsze było powszechną praktyką do tej pory – uważa radca.



▶ **WYZWANIE DLA MAŁYCH I DUŻYCH:** Według organu nadzorującego ochronę danych osobowych, którym kieruje generalny inspektor dr Edyta Bielak-Jomaa, przygotowanie się do stosowania unijnego rozporządzenia jest wyzwaniem zarówno dla dużych przedsiębiorstw, w których w ten proces będzie musiało być zaangażowanych wiele osób, jak i dla małych i średnich firm. W tych ostatnich pracować należy przede wszystkim nad niezbędną wiedzą o nowych rozwiązaniach prawnych dotyczących przetwarzania danych osobowych. [FOT. WMI]

## Analiza ryzyka

Radosław Kaczorek, prezes Immusec, także podkreśla, że zastosowanie się do unijnej reformy wymaga długofalowego podejścia do ochrony danych, opartego na ryzyku.

– Pozwala ono na podstawie wyników analizy ryzyka określić, jakie nakłady inwestycyjne, koszty pracy i zatrudnienia oraz wydatki na inne działania natury organizacyjnej, technologicznej i procesowej należy ponieść, aby dane zagrożenia ograniczyć do poziomu akceptowalnego przez kierownictwo przedsiębiorstwa – wyjaśnia Radosław Kaczorek.

Podkreśla on, że przedsiębiorca musi wiedzieć, czym dysponuje, czyli jakie dane

osobowe posiada, jakie procesy biznesowe i systemy informatyczne służą ich przetwarzaniu, kto w firmie realizuje poszczególne zadania przy użyciu tych narzędzi i przetwarzając te dane. Eksperci Immusec mówią, że podatność na zagrożenia, takie jak awarie, wyciek danych, ich wyłudzenia, wynika często z charakterystyki firmy – jej lokalizacji geograficznej, rozmiaru, obszaru działania, rodzaju przetwarzanych informacji, systemów informatycznych i wymagań prawnych.

– Aby ograniczyć skutki lub prawdopodobieństwo incydentów, należy takie zagrożenia przewidzieć wcześniej oraz ocenić ich wpływ na przedsiębiorstwo, zarówno pod względem

# osobowych

prawnym, finansowym jak i wizerunkowym. Na tej podstawie, stosując zasadę „lepiej zapobiegać, niż leczyć”, można dobrać pewne mechanizmy kontrolne, organizacyjne i techniczne, np. odpowiednio zdefiniowane procedury, szkolenia uświadamiające pracowników czy systemy zabezpieczające. Należy skupić się na incydentach będących źródłem największych strat dla przedsiębiorcy – wylicza Radosław Kaczorek.

Tomasz Osiej mówi, że brak konkretnych wymagań, do czego przyzwyczaiła przedsiębiorców ustawa o ochronie danych osobowych, trochę hamuje administratorów w planowaniu zadań.

## Wewnętrzne audyty

– Moim zdaniem, w pierwszej kolejności problemy będą miały te podmioty, które nie wykonają żadnych działań przygotowawczych, czekając na „sztywne” zalecenia po 2018 r. A taką tendencję obserwujemy – ocenia radca.

Uważa on, że firmy powinny powołać wewnętrzne, interdyscyplinarne zespoły zajmujące się RODO i zacząć od przeszkolenia czy zaznajomienia z tym rozporządzeniem osób kluczowych, a następnie przekazać niezbędne informacje jak największej liczbie ludzi zaangażowanych w procesy przetwarzania danych. Jego zdaniem, punktem wyjścia do dalszych działań powinien być audyt, na podstawie którego zostaną wyznaczone zadania i priorytety działań. Wtedy przyjdzie pora na przygotowanie procedur, ich wdrożenie i sprawdzenie w praktyce, jak działają.

Według Radosława Kaczorka, zarządzanie ryzykiem zgodne z RODO wymaga ciągłego monitoringu i szybkiej reakcji w sytuacji kryzysowej. Trzeba przygotować scenariusze działań, aby ograniczyć jej negatywne skutki i zapobiec np. paraliżowi firmy.

– Gdy nastąpi wyciek danych bądź atak hakerów, ważne jest również zabezpieczenie materiału dowodowego, co pomoże ekspertom informatyki śledczej w zbadaniu tego przyczyn – wyjaśnia prezes Immusecu.

Zwraca on też uwagę, że zgodnie z obowiązującą jeszcze ustawą o ochronie danych

osobowych lista wymaganych zabezpieczeń technicznych zawiera pięć pozycji, a w przypadku nowych regulacji unijnych zalecenia, zgodnie z normą ISO27001, określającą zarządzanie bezpieczeństwem informacji, dotyczą aż 114 zabezpieczeń.

Również generalny inspektor ochrony danych osobowych (GIODO) podkreśla, że przygotowanie firmy do unijnej reformy jest dużym wyzwaniem, i zachęca, by z tym nie zwlekać. Apeluje do przedsiębiorców, aby np. działający u nich administratorzy bezpieczeństwa informacji (ABI) już teraz podnosili wiedzę wszystkich osób uczestniczących w procesach przetwarzania danych, przygotowując ich tym samym do stosowania nowego prawa.

„Wykorzystaj czas, który pozostał do momentu stosowania rozporządzenia na rzetelny przegląd wszystkich prowadzonych czynności przetwarzania danych, tak by 25 maja 2018 r. móc już wykazać zgodność z nowymi przepisami” – czytamy w apelu GIODO. ©

## Nowe obowiązki, nowe prawa

Uprawnienia osób, których dane są przetwarzane, będą szersze. Już nie tylko mają być informowani o tym np., w jakim celu te informacje ktoś gromadzi, ale też przysługiwać im ma np.

- ▶ prawo do żądania usunięcia wszelkich danych dotyczących danej osoby, czyli tzw. prawo do bycia zapomnianym,
- ▶ prawo do niepodlegania profilowaniu.

Nowe obowiązki dla administratorów to m.in.:

- ▶ szacowanie ryzyka wystąpienia zagrożeń dla praw i wolności osób, których dane będą przetwarzane,
- ▶ zapewnienie użytkownikom narzędzi technologicznych maksymalnej ochrony, tzw. domyślnej,
- ▶ niezwłoczne zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu, a także zawiadamianie o tym osób, których dane dotyczą,
- ▶ prowadzenie rejestru czynności przetwarzania danych.