

# Ocena skutków pomoże w ochronie prywatności

**RODO** Firmy, które planują wprowadzenie innowacyjnych usług związanych z przetwarzaniem danych osobowych, powinny się pospieszyć. Za pół roku dojdzie im bowiem nowy obowiązek

Sławomir Wikariak  
slawomir.wikariak@infor.pl

Z licznych obowiązków, które pojawią się 25 maja 2018 r., kiedy zacznie być stosowane unijne rozporządzenie o ochronie danych osobowych (RODO), spore problemy może sprawić przedsiębiorcom nakaz przeprowadzania oceny skutków dla ochrony danych osobowych (ang. Data Protection Impact Assessment; dalej: DPIA). Będzie ona obligatoryjna wszędzie tam, gdzie pojawi się ryzyko naruszenia praw lub wolności osób. Chodzi nie tylko o duże banki czy firmy ubezpieczeniowe stosujące profilowanie podczas udzielania kredytów czy sprzedaży polis. Nawet mały start-up mający pomysł na nową usługę internetową może być zmuszony do przeprowadzenia DPIA. To samo dotyczy zresztą administracji publicznej, choćby w związku z prowadzonym przez gminę monitoringiem wizyjnym.

Formalnie DPIA jest wymagana tylko tam, gdzie mamy do czynienia z wysokim ryzykiem. Żeby jednak ustalić, czy ono faktycznie występuje, trzeba przeprowadzić jakąś analizę. A potem podjąć środki, żeby to ryzyko ograniczyć. Bez analizy nie będziemy wiedzieć, jakie środki ochrony danych są do tego ryzyka adekwatne – mówi Maciej Gawroński, partner zarządzający w kancelarii Gawroński & Partners s.k.a.

To poniekąd dodatkowe zabezpieczenie na wypadek wycieku danych. Organ badający taki incydent i decydujący o ewentualnej karze będzie m.in. badał, czy przeprowadzenie DPIA było wymagane i czy zastosowano środki adekwatne do zagrożeń – dodaje prawnik.

## Zalew wniosków?

Już samo przeprowadzenie DPIA może nie być łatwe. Powód – niewielu jest ekspertów, którzy mogą się podjąć tego zadania. Zdecydowana większość

administratorów sama zaś mu nie podda. Z pomocą przychodzi wytyczne Grupy Roboczej art. 29 (w październiku wyszła zaktualizowana wersja), jednak próżno w nich szukać odpowiedzi na wszystkie pytania.

Początkowo w Polsce może być z tym problem, bo dla firm to nieznany obszar, a ludzi o realnej wiedzy i doświadczeniu jest niewielu. Dotychczas DPIA przeprowadzano raczej w krajach Europy Zachodniej, takich jak Wielka Brytania czy Francja – zauważa dr Łukasz Olejnik, konsultant i badacz cyberbezpieczeństwa prywatności, afiliowany przy Center for Information Technology Policy Uniwersytetu Princeton, który ma doświadczenie w przeprowadzaniu DPIA w Europie.

Co więcej, nawet najlepiej przeprowadzona ocena nie musi oznaczać końca obowiązków. Jeśli bowiem okaże się, że przetwarzanie powoduje wysokie ryzyko, któremu trudno zapobiec, to niezbędne będą konsultacje z organem. Zgodnie z projektem nowej ustawy będzie nim Urząd Ochrony Danych Osobowych (UODO), który zastąpi dzisiejszego generalnego inspektora ochrony danych osobowych (GIODO).

W początkowym okresie może on zostać zalany wnioskami o konsultacje, co zresztą nałoży się także na inne kierowane do niego sprawy. Z oczywistych względów pojawi się więc ryzyko zatorów – zauważa Maciej Gawroński.

To zaś może oznaczać problemy dla firm. Dopóki bowiem UODO nie skończy konsultacji, nie będą one mogły wdrożyć usługi czy też rozpocząć sprzedaży produktu związanych z przetwarzaniem danych osobowych. To zaś wiąże się z ryzykiem wyprzedzenia przez konkurencję.

Wszystko zależy będzie od liczby wniosków.

Nie można wykluczyć, zwłaszcza w początkowym okresie, że będzie to spora liczba – przyznaje dr Edyta Bielak-Jomaa, GIODO.

Z tego m.in. względu złożyłam wniosek o zwiększenie budżetu GIODO, co pozwoli na zatrudnienie dodatkowych pracowników, a w konsekwencji na sprawną i efektywną realizację wszystkich obowiązków urzędu. Powinna się do tego również przyczynić planowana reorganizacja biura, nad którą właśnie pracujemy – dodaje.

## Niejasne wytyczne

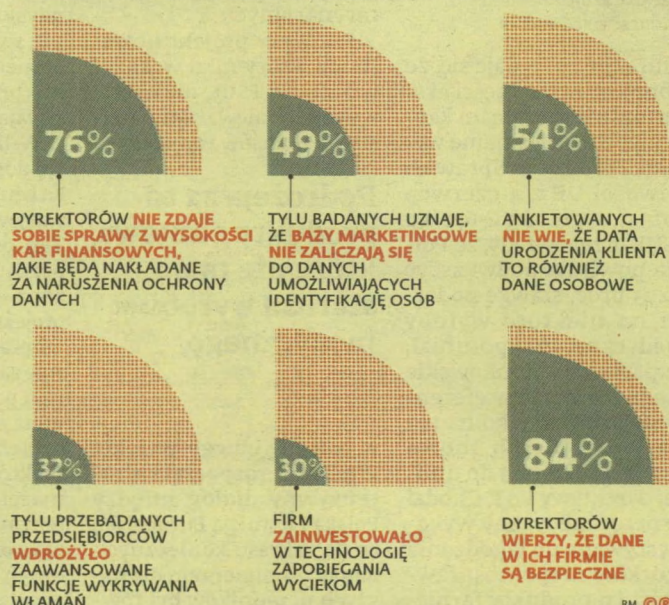
Przedsiębiorcy, którzy planują wprowadzenie jakichś szczególnie innowacyjnych rozwiązań, które wiążą się z wysokim ryzykiem dla przetwarzania danych osobowych, powinni więc zastanowić się, czy nie uda im się tego zrobić przed 25 maja 2018 r. Choć nie oznacza to, że będą zwolnieni z obowiązku przeprowadzenia DPIA, to jednak ryzyko związane z brakiem przejścia tych procedur będzie dużo mniejsze. Problem w tym, że nie wiadomo, czy wspomniana data może być traktowana jako graniczna. W aktualizacji do wytycznych Grupy Roboczej art. 29 pojawiło się zalecenie, by ocenę skutków przeprowadzać także dla operacji rozpoczętych przed 25 maja, choć jednocześnie zaznaczono, że nie zawsze będzie to niezbędne.

„Wymóg przeprowadzenia oceny skutków dla ochrony danych dotyczy istniejących operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, a w przypadku których nastąpiła zmiana rodzaju ryzyka, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych” – czytamy w wytycznych. Jak wyjaśnia GIODO, taka zmiana może wynikać m.in. z wykorzystania nowej technologii do przetwarzania danych lub dlatego, że dane osobowe zaczęły być wykorzystywane w innym celu.

## Rząd mógłby pomóc

A czym jest sama ocena skutków dla ochrony danych osobowych?

## FIRMY WCIĄŻ NIE SĄ PRZYGOTOWANE NA RODO



\* badanie Trend Micro przeprowadzone we współpracy z firmą Opinium od 22 maja do 28 czerwca 2017 r. na podstawie 102 wywiadów internetowych z osobami, które podejmują decyzje dotyczące technologii informatycznych w przedsiębiorstwach zatrudniających ponad 500 pracowników w Polsce

Odnosi się ona do ryzyka dla podstawowych praw i wolności użytkownika. Jednym z tych praw jest prywatność, dlatego nazywam to procesem pomiaru poziomu prywatności i ochrony danych. Kluczowym wymogiem jest identyfikacja i ustalenie ryzyka dla przetwarzanych danych, czemu zawsze towarzyszą rekomendacje – wyjaśnia dr Łukasz Olejnik.

W zależności od wielkości i złożoności projektu kluczowy zespół do przeprowadzenia DPIA składa się z od jednego do kilku ekspertów (czasem więcej). DPIA to proces ciągły, choć początkowe działania angażujące ekspertów mogą zająć tygodnie. W zależności od specyfiki projektu angażuje się prawników, ale też ekspertów z wiedzą technologiczną i regulacji, na Zachodzie zwanych inżynierami prywatności – dodaje.

Co ciekawe, w wielu sytuacjach państwo może zdjąć z przedsiębiorców ciężar przeprowadzania DPIA.

Przygotowując projekt przepisów dotyczących przetwarzania danych osobowych, projektodawca rządowy mógłby przeprowadzać DPIA w ramach oceny skutków regulacji. Wówczas zwolnieni byłoby już z tego

wszyscy administratorzy, którzy przetwarzają dane na podstawie tego przepisu. Zamiast ogromnej liczby DPIA przeprowadzanych indywidualnie wystarczyłoby tylko jedna ocena opracowana podczas prac legislacyjnych – podpowiada Grzegorz Sibiga, adwokat w kancelarii Traple Konarski Podrecki i Wspólnicy i kierownik Zakładu Prawa Administracyjnego w Instytucie Nauk Prawnych PAN.

Byłaby to też doskonała okazja do poprawienia jakości samego prawa. Na początku DPIA trzeba bowiem przeprowadzić ocenę niezbędności przetwarzania danych i proporcjonalności projektowanych w prawie operacji na danych. Stworzona zostałaby więc szansa, aby mniej przepisów w sposób nadmierny ingerowało w naszą prywatność – zaznacza ekspert.

Okazją ku temu mógł być już projekt przepisów wprowadzających ustawę o ochronie danych osobowych. Daje on pracodawcom prawo do przetwarzania danych biometrycznych. W wielu zakładach pracy może to jednak oznaczać konieczność przeprowadzenia DPIA. Gdyby zrobił to projektodawca, przedsiębiorcy nie mieliby już tego obowiązku. ©