

# Nie zgodzimy się na powszechne stosowanie biometrii

**Dr Edyta Bielak-Jomaa:** Jeśli firma będzie przetwarzać dane bez racjonalnego uzasadnienia i bez podstawy prawnej, to będziemy karać za naruszenie ochrony danych osobowych

**Rozporządzenie RODO, które wejdzie już za 14 miesięcy, to rewolucja i dla przedsiębiorców, i dla samego GIODO. Pani urząd stanie się tak silny, jak Urząd Ochrony Konkurencji i Konsumentów!**  
Nie wiem, czy nawet nie silniejszy. Chociaż chciałabym zauważyć, że GIODO działa nieco inaczej niż UOKiK, bo stoi na straży podstawowych praw człowieka, takich jak prawo do prywatności, prawo do ochrony danych osobowych. Ogólne rozporządzenie Parlamentu Europejskiego i Rady z 27 kwietnia 2016 r. [UE] nr 2016/679 o ochronie danych osobowych (RODO) daje nam możliwość zapewnienia efektywniejszej niż dotychczas ochrony danych osobowych, i to obywateli nie tylko polskich, lecz także pozostałych krajów UE.

**No właśnie, czy są państwo już przygotowani?**  
Nie mam wątpliwości, że do 25 maja 2018 r. będziemy gotowi. Niemniej jednak czeka nas jeszcze dużo pracy, by przygotować urządy do nowych zadań. Rozpoczęliśmy już szkolenie językowe pracowników, będziemy podnosić ich kwalifikacje nie tylko w tym zakresie. Konieczne jest też zatrudnienie dodatkowych specjalistów, m.in. w dziedzinie informatyki, audytu i certyfikacji. Tylko silny i niezależny organ będzie w stanie zapewnić nadzór nad prawidłowością przetwarzania danych osobowych, zarówno przez sektor administracji publicznej, jak i przez podmioty prywatne. W tym celu GIODO musi zostać prawnie, finansowo i organizacyjnie wzmocniony. Bez tego niemożliwe będzie np. realizowanie przez organy z państw UE wspólnych kontroli czy nakładanie przez GIODO wysokich kar finansowych na tych, którzy nie stosują się do przepisów.

**I rzeczywiście będzie pani nakładać wysokie kary, chociażby na gigantów branży elektronicznej?**  
Wierzę, że organ nadzorczy w każdym kraju członkowskim nie będzie miał kompleksów, żeby mierzyć się z gigantami. Oczywiście będziemy współpracować z innymi urzędami, np. przy wypracowywaniu polityki kontroli oraz metodyki nakładania kar finansowych. Proszę pamiętać, że dzięki RODO każdy urząd państwa członkowskiego stojący na straży danych osobowych będzie równie silny i będzie mógł nałożyć karę wynoszącą aż do 4 proc. całkowitego rocznego światowego obrotu lub 20 mln euro. Wobec takiej groźby nawet giganci zaczną traktować dane europejskich obywateli z należytą troską.

**Prezes UOKiK ma prawo nałożyć karę w wysokości do 10 proc. rocznego obrotu przedsiębiorcy. W praktyce stosowanie tego maksymalnego pułapu ostatnio zakwestionował nawet Sąd Najwyższy. Jak będzie w przypadku kar nakładanych przez GIODO?**  
Rozporządzenie przewiduje maksymalne limity kar. Nie oznacza to jednak, że będziemy sięgać najwyższego pułapu. Nie zależy nam, żeby właściciele firm przyprowadzić o zawał serca, a mediom dawać pożywkę. Tak wysokie pułapy kar są przerażające dla większości przedsiębiorców, ale – choć nie chcę

przedwcześnie uspokajać – mają one działać głównie mobilizująco. Będziemy nakładać kary, ale będą one miarkowane.

**Co to oznacza?**  
Przesądząją o tym przepisy RODO, które wprost stanowią, że kary mają być skuteczne, proporcjonalne i odstraszaające, ale jednocześnie przy wymierzaniu ich wysokości decydować musi indywidualna ocena naruszeń. Będzie więc miało znaczenie, jakie dane są przetwarzane, to, czy naruszenie miało charakter umyślny czy też nie, warunki, w jakich do niego doszło, liczba poszkodowanych osób oraz rozmiar poniesionej przez nich szkody. Liczyć się też będzie, czy chodzi o pierwsze naruszenie, czy też kolejne, jak zachował się administrator – czy sam zgłosił np. wyciek danych. Istotne będzie też to, jak administrator postąpił w stosunku do osób, których dane dotyczyły, np. czy poinformował je o wycieku. Jest wiele różnych okoliczności i każda z nich powinna być uwzględniona przy ustalaniu wysokości kary. Z pewnością też polityka oraz metodyka nakładania kar będą przedmiotem ustaleń na poziomie UE. Jednolite reguły w tym zakresie są niezbędne, by zapewnić jednakowy poziom przestrzegania przepisów i uniknąć przenoszenia działalności do państw, w których sankcje za naruszenie tych samych wymogów byłyby niższe.

**Czy karane będzie migrowanie danych do krajów o bardziej liberalnym podejściu do danych osobowych? Czy tolerowane będą wymówki, że dana spółka technologiczna ma siedzibę poza Unią Europejską?**  
Koniec z takimi tłumaczeniami. Jeżeli wykorzystuje się dane obywateli UE, to wszystko, co się z nimi robi, musi być zgodne z postanowieniami RODO. Miejsce przetwarzania będzie miało zdecydowanie mniejsze znaczenie. Najistotniejsze będzie to, czyje dane są przetwarzane. Za każdym razem w przypadku transgranicznego ich przesyłania będziemy bezwzględnie domagać się wskazania podstawy działania. Przypominam, że już obecnie za brak podstawy prawnej do przetwarzania grozi kara pozbawienia wolności do 2 lat.

**A co z danymi biometrycznymi? Coraz więcej przedsiębiorców je przetwarza, w klubach fitness szafki otwiera się na odbitkę kciuka. Co na to GIODO?**  
Mamy z tym wielki problem. Firmom wydaje się, że RODO jeszcze nie ma, ale to przekonanie złudne, bo akt prawny wszedł w życie – i dlatego już teraz odwołujemy się do jego postanowień. Wprowadzona została w nim legalna definicja danych biometrycznych, której brakowało w polskim ustawodawstwie. Dane biometryczne stanowią szczególną kategorię, bo przypisane są do danego człowieka i nie da się ich zmienić. To może być odcisk palca, skan siatki oka czy próbka głosu. Ich kradzież lub utrata może mieć katastroficzne, nieodwracalne skutki. Wydaje nam się zatem, że przedsiębiorcy nie powinni ich masowo gromadzić, zwłaszcza gdy nie ma to żadnego racjonalnego uzasadnienia i podstawy prawnej.



DR EDYTA BIELAK-JOMAA  
generalny inspektor ochrony danych osobowych

**Czyli jak w praktyce będą podchodzić państwo do przedsiębiorstw stosujących biometrię?**  
Absurdalne jest, by przykładowo dziecko musiało udostępniać odcisk palca do szafki na siłowni czy basenie, skoro można mu po prostu dać kluczyk. Nikt mnie nie przekona, żeby w tego typu przypadkach konieczne było gromadzenie danych biometrycznych. Nie pomoże tłumaczenie, że są dobrze zabezpieczone. Być może – ale ryzyko ich utraty jest mimo wszystko zbyt duże. Powszechne używanie biometrii wytworzyłoby przekonanie o małej wartości tych danych. Nie ma na to zgody – jeśli firma będzie przetwarzać dane bez podstawy prawnej i racjonalnego uzasadnienia, to będziemy zakazywać takiego działania i karać za naruszenie ochrony danych osobowych. Kwestie bezpieczeństwa technicznego będą brane pod uwagę dopiero w drugiej kolejności.

**W jakich przypadkach zbieranie danych biometrycznych może być zatem adekwatne do celu?**  
Uzasadnione może być ono w służbach specjalnych, albo wtedy, gdy chcemy zapewnić, by dostęp do określonych miejsc, np. skarbcza w banku, mennicy czy pomieszczeń, w których gromadzone są tajne informacje istotne z punktu bezpieczeństwa państwa, miały wyłącznie określone osoby. Zdecydowanie nie zgadzam się na ewidencjonowanie czasu pracy przy użyciu odcisku palca albo wykorzystywaniu go do logowania się przy korzystaniu z aplikacji społecznościowej. Nawet jeśli jest to wygodne i wszyscy się na to godzą – bo to byłoby szaleństwo. Poza tym wciąż nie jestem przekonana, czy np. odcisk palca jest takim świetnym rozwiązaniem. Przecież są ludzie, których opuszki nie nadają się do skanowania – sama miałam problem z wyrobieniem paszportu biometrycznego. A i domowe środki chemiczne podczas częstego stosowania mogą zniszczyć opuszki palców. I co wtedy? Zapewne przedsiębiorcy chcieliby wprowadzić kolejne zabezpieczenia biometryczne – np. weryfikację próbki głosu. Przy dzisiejszym stanie postępu technicznego zaciągnięcie w czymś imieniu pożyczki przez internet może okazać się banalnie proste – w zasadzie wystarczy do niego zadzwonić i skopiować jego próbkę głosu.

**No cóż, to właśnie pokrzyżowała pani szlaki wszystkim start-upom technologicznym**

**i serwisom aukcyjnym. Także fintechom, które wdrażając dyrektywę PSD II, mogą chcieć wprowadzać biometrię do autoryzacji transakcji finansowych.**  
Mam świadomość, że w erze nowych technologii trudno będzie uciec od tego typu rozwiązań. Jednak rolę organu nadzoru nie jest dawanie zielonego światła dla wszystkich technologicznych nowinek, tylko ochrona danych obywateli. Będziemy musieli analizować wszelkie propozycje przedsiębiorców na bieżąco. Ważne są szczegóły: po co gromadzone są dane, komu udostępniane i w jaki sposób zabezpieczone. Co zaś do dyrektywy PSD II, to po pierwsze – jest to dyrektywa, a zatem akt, który inaczej niż unijne rozporządzenie, takie jak RODO, wymaga implementacji. Musimy więc poczekać na przepisy krajowe. Bo może się okazać, że Ministerstwo Cyfryzacji uwzględni to zagadnienie w przygotowywanych nowelizacjach. Jeśli chodzi o funkcjonowanie firm fintech, to aktywnie uczestniczymy w dyskusjach z przedstawicielami tego sektora.

**A co ze szkoleniami dla administratorów bezpieczeństwa informacji?**  
Szkolenia dla obecnych ABI, przyszłych inspektorów ochrony danych, organizujemy przede wszystkim dla tych sektorów, w których naruszenie przepisów byłoby bardzo niebezpieczne dla obywateli. Do tej pory przeprowadziliśmy szkolenia dla sektora publicznego oraz szkół wyższych. Ankiety oceny z tych wydarzeń potwierdzają, że spotkania z GIODO są bardzo potrzebne i w dużym stopniu spełniają oczekiwania uczestników. Ostatnio zorganizowaliśmy dwa jednodniowe szkolenia dla czterystu ABI z sektora medycznego. Planujemy więcej tego typu spotkań z przedstawicielami konkretnych branż, np. w najbliższym czasie z ABI z instytucji wymiaru sprawiedliwości. Jednak mając bardzo ograniczone możliwości osobowe i finansowe, rozpatrując rocznie blisko 3 tysiące skarg, jesteśmy zbyt zapracowani, by móc organizować dużą liczbę szkoleń. Uczestniczymy też w wielu konferencjach, na których przedstawiamy istotę reformy unijnych przepisów w zakresie ochrony danych osobowych. Proszę nie liczyć na to, że organ nadzorczy będzie edukował od podstaw wszystkich przedsiębiorców.

**Problem w tym, że z relacji jednego z uczestników szkolenia dla sektora medycznego**

wyłania się niezbyt pozytywny obraz. Według niego brakowało konkretów, nie można było się dowiedzieć nic na temat planowanych form kontroli i przedstawiciele urzędu sprawiali wrażenie nieprzygotowanych.  
Być może takie wrażenie miał wybitny specjalista z zakresu ochrony danych osobowych, który spodziewał się usłyszeć odpowiedzi na wszystkie szczegółowe pytania. Albo wręcz przeciwnie, była to osoba niemająca wiedzy na ten temat, a spodziewająca się dostać nie informacje, lecz kompletną instrukcję obsługi. Tymczasem nie możemy opracować dokładnych scenariuszy postępowania, bo RODO celowo zostało skonstruowane na tyle ogólnie, by było elastyczne i umożliwiało odpowiednie zastosowanie w konkretnych przypadkach. Jeśli ktoś liczy na otrzymanie instrukcji obsługi podanej na tacy, to znaczy, że kompletnie nie rozumie, czym jest ochrona danych osobowych pod rządami RODO. To administrator danych jest odpowiedzialny za przestrzeganie przepisów rozporządzenia i ma wykazać, że właściwie spełnia określone w nim wymogi. Rolą organu nadzorczego jest zaś weryfikowanie i egzekwowanie ich przestrzegania.

**Wielu ekspertów narzeka na kontakt z GIODO. Przykład: nie ma infolinii.**  
To prawda, ale potrzeby informacyjne staramy się zaspokajać za pośrednictwem naszej strony internetowej. Jest ona bardzo dobra, czytelna, zawiera dużo informacji i cieszy się największym zaufaniem spośród stron wszystkich instytucji publicznych. Nie mamy wystarczających środków, żeby odpowiadać na każde pytanie, a jako organ nadzorczy nie udzielamy porad prawnych. W praktyce często jest tak, że radcowie prawni woleliby anonimowo do nas zadzwonić i o coś zapytać niż spojrzeć w przepisy czy przeanalizować orzecznictwo albo wydawane przez GIODO decyzje. Osoby lub przedsiębiorcy, którzy chcą wiedzieć, co dzieje się w ich sprawie, zawsze są obsługiwani. Chętnie poznałabym nazwiska ekspertów, którzy nie mogą się z nami skontaktować.

**Rozporządzenie RODO przewiduje też wprowadzenie certyfikacji podmiotów przetwarzających dane przez firmy prywatne, wcześniej certyfikowane przez GIODO. Kiedy taka certyfikacja mogłaby ruszyć?**  
Na temat certyfikacji trwa wciąż dyskusja, również na spotkaniach w Grupie Roboczej Artykułu 29. Na chwilę obecną nic więcej na ten temat jeszcze nie mogę powiedzieć. Czekamy również na propozycje Ministerstwa Cyfryzacji w tym zakresie.

**Mają już państwo założoną skrzynkę e-mailową na donosy? Dlaczego mielibyśmy to robić?**

**To może być świetny sposób na pozbywanie się konkurencji: nastać fiskusa, służbę celną, UOKiK i GIODO.**  
My nie działamy na podstawie donosów, więc nie będziemy zakładać skrzynki na donosy. Ja wciąż wierzę w ludzi. ☺☺

Rozmawiał Jakub Styczyński