# Pęknięty standard ochrony danych – analiza propozycji Rady UE

17 czerwca 2015

Zapowiadana od lat i bardzo potrzebna unijna reforma przepisów o ochronie danych osobowych zyskuje realny kształt. Rada Unii Europejskiej – ostatni organ, na którego stanowisko czekaliśmy – wypracowała tzw. ogólne podejście (general approach) do projektu rozporządzenia. To oznacza początek trilogu, czyli negocjacji między wszystkimi zaangażowanymi instytucjami: Radą, Komisją i Parlamentem Europejskim, a jednocześnie początek ostatniej politycznej batalii. Mimo silnej presji, by prace nad projektem zakończyć jeszcze w tym roku kalendarzowym (Komisja Europejska włączyła harmonizację przepisów o ochronie danych do flagowego projektu stworzenia tzw. jednolitego rynku cyfrowego), należy zakładać, że łatwo nie będzie. Stanowisko Rady UE w kilku fundamentalnych kwestiach mocno odbiega od standardu, jaki wyznaczyły projekty przyjęte przez Komisję i Parlament Europejski – i to na niekorzyść ochrony danych osobowych.

Fundacja Panoptykon śledziła proces prac nad ogólnym rozporządzeniem o ochronie danych osobowych od samego początku, czyli 2012 roku. Ostatnie 20 miesięcy przebiegało pod znakiem ostrych tarć w Radzie UE, a konkretnie w grupie roboczej DAPIX, złożonej z przedstawicieli odpowiednich ministerstw i krajowych organów odpowiedzialnych za ochronę danych. W Polsce prace na tym etapie koordynowało Ministerstwo Administracji i Cyfryzacji, które bardzo poważnie potraktowało konsultacje społeczne. Przez cały okres kształtowania stanowisk w Radzie UE MAiC organizowało regularne spotkania ekspertów reprezentujących wszystkie strony społeczne – biznes, akademię i organizacje pozarządowe. Na podstawie zebranych opinii Ministerstwo wypracowywało polskie stanowisko

przedstawione na forum UE, w dużej mierze dobrze wyważone i godzące różne interesy.

Jaki jest ostateczny efekt? 200 stron i 91 artykułów nierównego, politycznego kompromisu. Z jednej strony ogólne podejście wypracowane w Radzie UE wzmacnia pozycję organów odpowiedzialnych za ochronę danych osobowych (takich jak polski GIODO), przewiduje wysokie sankcje administracyjne, zapewnia stosowanie nowego prawa wobec firm zagranicznych (bez względu na ich siedzibę czy miejsce przetwarzania danych) oraz dobrze zabezpiecza pewne prawa osób, których dane są przetwarzane (np. prawo do informacji, prawo do przeniesienia oraz usunięcia danych). Z drugiej strony w kwestiach dość fundamentalnych pojawiły się niebezpieczne pęknięcia i wyłączenia, które mogą podważyć sens całej reformy.

Oto najpoważniejsze problemy w opinii Fundacji Panoptykon:

1. Ograniczenie stosowania nowego prawa wobec organów państwowych i UE.

Dane osobowe w ryzykowny i nieproporcjonalny sposób przetwarzają nie tylko prywatne firmy – ten problem w równej mierze dotyczy organów państwowych i instytucji europejskich. Mimo to Rada UE proponuje bardzo szerokie wyłączenia, zgodnie z którymi instytucje unijne w ogóle nie będą objęte nowym standardem (art. 2), a państwa zachowają pełną swobodę wszędzie tam, gdzie w grę wchodzi bezpieczeństwo narodowe, obronność, bezpieczeństwo publiczne, interes ekonomiczny lub fiskalny, zdrowie publiczne, opieka społeczna czy „inny ważny interes publiczny” (art. 21). Mając to na uwadze, trudno powiedzieć, co tak naprawdę nowe rozporządzenie ma regulować w sferze relacji obywatel–państwo.

2. Nieprecyzyjna definicja zgody na przetwarzanie danych osobowych.

Jedną z kilku podstaw możliwości przetwarzania danych osobowych jest zgoda osoby, której to dotyczy. Inne to m.in.

niezbędność do realizacji umowy i obowiązek prawny. Administratorzy danych nie powinni sięgać po zgodę, o ile przetwarzanie danych nie jest w pełni dobrowolne, ponieważ w takich sytuacjach mogą skorzystać z innych podstaw prawnych. W tym kontekście ważne jest, by sposób wyrażenia zgody nie pozostawiał żadnych wątpliwości co do intencji danej osoby i by zagwarantowano jej pełną autonomię. Niestety, propozycja Rady UE dopuszcza zgodę niewyrażoną wprost (explicit); która wynika – czy też może zostać wyinterpretowana – z innego zachowania (np. wejścia na stronę internetową lub rozpoczęcia korzystania z danej usługi – por. art. 4). Takie podejście otwiera drogę do nadużywania konstrukcji zgody i zaciemniania sposobu, w jaki dane są zbierane, a następnie wykorzystywane.

3. Możliwość wykorzystywania zebranych danych osobowych w innym celu niż pierwotnie zakładany.

Zasada ograniczenia celu, dla którego przetwarzane dane zostały pierwotnie zebrane, ma fundamentalne znaczenie dla ochrony praw osoby, której dane dotyczą. Zgadzając się na przetwarzanie danych w określonym celu (np. badawczym) lub decydując na przekazanie danych w ramach konkretnej umowy (np. kredytu), mamy prawo oczekiwać, że nie zostaną one następnie – już bez naszej zgody – wykorzystane na potrzeby profilowanej reklamy czy przekazane innej firmie w ramach umowy o współpracy. Propozycja Rady UE stoi w sprzeczności z tą zasadą i przewiduje możliwość zmiany celu przetwarzania danych w oparciu o tzw. uzasadniony interes administratora lub „strony trzeciej” (np. innej firmy, z którą administrator współpracuje – por. art. 6 ust 4). Możliwe ma być również, w zasadzie bez ograniczeń, dalsze przetwarzanie danych w celach naukowych i statystycznych, przy czym projekt nie definiuje, jak rozumieć te nieprecyzyjne określenia (czy np. badania prowadzone przez firmę można uznać za cel naukowy).

4. Możliwość zbierania większej ilości danych, niż to konieczne.

Inną fundamentalną zasadą w ochronie danych osobowych jest reguła ograniczenia zbierania danych do niezbędnego minimum. Ani prywatne, ani publiczne podmioty nie powinny pozyskiwać danych „na wszelki wypadek", czyli zbierać informacji, których podstawa i cel przetwarzania danych nie uzasadnia (np. bank nie powinien pytać klienta o stan zdrowia, a ubezpieczyciel – o stan rachunku oszczędnościowego). Propozycja Rady UE podważa tę zasadę, ponieważ w miejsce twardego zakazu przetwarzania danych, które nie są niezbędne, wprowadza pojęcie „nienadmiarowego przetwarzania danych" (non-excessive data processing) – a to istotna różnica i niebezpieczne otwarcie na zbieranie wszystkiego, co dany podmiot uzna za uzasadnione.

5. Transfer danych poza granice UE niemal bez ograniczeń.

Jedną z newralgicznych kwestii, którą konsekwentnie podnosił w grupie DAPIX polski rząd, jest możliwość transferu danych poza granice UE, szczególnie w ramach spółek należących do międzynarodowych korporacji oraz na linii prywatne firmy – organy państwa (np. USA). Istniejące reguły są daleko niewystarczające, jednak propozycja Rady UE bynajmniej nie rozwiązuje tego problemu. Przewiduje dość swobodne zasady dla międzynarodowych korporacji (oparte na tzw. binding corporate rules, kodeksach postępowania i prywatnych mechanizmach certyfikacji) oraz, jakby tego było mało, szerokie wyłączenia np. dla firm, które wykażą „uzasadniony interes" w transferze danych poza granice UE (por. art. 44).

6. Swobodne przetwarzanie danych wrażliwych, jeśli zostały upublicznione.

Kolejny niebezpieczny wyłom w standardzie ochrony prywatności dotyczy danych wrażliwych, takich jak pochodzenie etniczne, stan zdrowia czy orientacja seksualna. Wynika on z propozycji Rady UE, by przetwarzanie danych wrażliwych było możliwe w zasadzie bez ograniczeń, jeśli osoba, której dane dotyczą, sama je upubliczniła (por. art. 9). A przecież fakt, że zdecydowaliśmy się na ujawnienie swojego stanu zdrowia czy

orientacji seksualnej w serwisie społecznościowym, wcale nie oznacza, że dopuszczamy czy zgadzamy się na wykorzystanie tego typu informacji w kierowanej do nas reklamie, w procesie rekrutacji do pracy czy przy rozpatrywaniu wniosku o kredyt.

7. Profilowanie jako standardowa operacja na danych.

Organizacje obywatelskie, w tym Fundacja Panoptykon, od początku prac nad nowym rozporządzeniem zwracały uwagę na szczególne ryzyka związane z profilowaniem, czyli takim przetwarzaniem danych, które opiera się na analizie korelacji statystycznych i prowadzi do kategoryzowania ludzi ze względu na określone cechy (np. poziom dochodów, płeć, wiek, upodobania konsumenckie). Parlament Europejski zaproponował daleko idącą regulację, w tym gwarancje pełnej przejrzystości zbierania danych, ich przypisywania do konkretnych kategorii i podejmowania na tej podstawie decyzji. W propozycji Rady UE profilowanie co do zasady traktowane jest jak każda inna – neutralna i niegenerująca szczególnych ryzyk – operacja na danych osobowych. Takie podejście sankcjonuje niebezpieczny trend, zgodnie z którym predykcyjne profilowanie klientów przez firmy czy kandydatów do pracy przez rekrutujących staje się rynkowym standardem.

Autorstwo: Katarzyna Szymielewicz
Współpraca merytoryczna: Jędrzej Niklas
Źródło: