Po konsultacjach nowej ustawy o ochronie danych

14 lutego 2018

Ministerstwo Cyfryzacji opublikowało nową wersję ustawy o ochronie danych osobowych, będącej wdrożeniem RODO. Prowadzone przez kilka miesięcy konsultacje publiczne nie poszły na marne: pod wpływem zgłoszonych uwag Ministerstwo poprawiło tryb powoływania prezesa Urzędu Ochrony Danych Osobowych (wykreślając przepis uzależniający wybór kandydata od decyzji prezesa Rady Ministrów) i przepisy proceduralne (m.in. obowiązek konsultowania branżowych kodeksów postępowań). Niestety, wygląda na to, że ceną za sprawne przyjęcie ustawy przez rząd i przejście do kolejnego etapu prac legislacyjnych będą szerokie wyłączenia dla małych i średnich przedsiębiorstw, na które nalegało Ministerstwo Rozwoju. To poważny wyłom w standardzie, jaki przewiduje RODO. I zarzewie kolejnego sporu z Komisją Europejską.

ORGAN NADZORCZY Z SILNYM, DEMOKRATYCZNYM MANDATEM

Od początku prac nad wdrożeniem RODO jednym z gorętszych tematów był tryb powoływania szefa nowego organu nadzorczego (PUODO). W pierwszej wersji projekt przewidywał powoływanie PUODO przez Sejm za zgodą Senatu, ale na wniosek prezesa Rady Ministrów. W praktyce taka procedura sprowadzałaby parlament do roli notariusza zatwierdzającego polityczną decyzję szefa rządu. Nie byłoby też w niej miejsca na otwartą konkurencję między kandydatami na to stanowisko i ich wizjami sprawowania urzędu. W aktualnej wersji projektu nie ma wzmianki o wniosku prezesa Rady Ministrów, co oznacza, że kandydatów na PUODO (tak jak obecnie kandydatów na GIODO) będą mogły zgłaszać grupy posłów.

Ministerstwo Cyfryzacji, broniąc pierwotnego pomysłu, argumentowało, że wybór piastuna organu władzy zawsze ma

charakter polityczny. A jednak to, czy o wyborze kandydata decyduje jednoosobowo szef rządu, czy – w pluralistycznym systemie – konkurujące grupy posłów, czyni różnicę. Ostatecznie nowy organ ma kontrolować także działania rządu (np. przetwarzanie danych w ramach rozmaitych publicznych baz danych), a więc potrzebuje gwarancji niezależności od władzy wykonawczej. Wybór przez Sejm i Senat daje osobie pełniącej urząd najmocniejszy – po wyborach powszechnych – mandat demokratyczny. A takiego PUODO niewątpliwie potrzebuje, jeśli ma skutecznie realizować stawiane przez nim zadania.

OBOWIĄZEK KONSULTOWANIA KODEKSÓW POSTĘPOWAŃ

W konsultacjach publicznych postulowaliśmy też zmiany w trybie przyjmowania tzw. kodeksów postępowań, czyli wypracowywanych przez poszczególne branże standardów, które będą miały bezpośredni wpływ na to, w jaki sposób przepisy RODO są stosowane i interpretowane. Te standardy mogą dotyczyć np. treści modelowej klauzuli zgody na przetwarzanie danych, sposobu realizowania prawa do informacji (łącznie z wyjątkami, które dana branża uważa za uzasadnione) czy prawa do przeniesienia danych (w tym wyboru formatu, jaki będzie wykorzystywany, albo kategorii danych, które będą tym prawem objęte). To wszystko sprawy o dużym znaczeniu dla konsumentów, a więc nie powinny być rozstrzygane bez dyskusji z bezpośrednio zainteresowanymi.

W pierwszej wersji przepisy ustawy o ochronie danych osobowych w ogóle nie odnosiły się do obowiązku konsultowania kodeksów z osobami, których praw będą one dotyczyć, ani do roli organizacji społecznych w tym procesie. Panoptykon proponował otwarty dialog izbom, które od miesięcy pracują nad swoimi kodeksami (m.in. Związkowi Banków Polskich i IAB), ale do tej pory żadne drzwi się nie otworzyły. Teraz obowiązek prowadzenia publicznych konsultacji znalazł się w ustawie. Dzięki temu wszyscy będziemy mieli szansę skomentować pomysły biznesu na dobre praktyki w zakresie ochrony danych, zanim staną się one rynkowym standardem, zaakceptowanym przez PUODO.

WYŁĄCZENIA DLA MŚP

Niestety, w innych aspektach obecny projekt ustawy o ochronie danych osobowych jest zdecydowanie gorszy niż ten, który Ministerstwo Cyfryzacji przedstawiło do konsultacji. W toku uzgodnień międzyresortowych, na wniosek Ministerstwa Rozwoju, przyjęto ograniczenie obowiązków, jakie na gruncie RODO mają realizować małe i średnie przedsiębiorstwa, czyli firmy zatrudniające mniej niż 250 pracowników.

Pod wpływem krytyki, również ze strony biznesu, Ministerstwo Cyfryzacji cofnęło się o krok, przywracając w stosunku do MŚP podstawowe obowiązki zawarte w art. 13 ust. 1 RODO, w tym obowiązek informowania o tym, kto i w jakim celu przetwarza dane osobowe. Nadal jednak w projekcie ustawy o ochronie danych osobowych pojawia się szereg trudnych do uzasadnienia wyłączeń. Małe i średnie przedsiębiorstwa (pod warunkiem, że nie będą przetwarzać danych wrażliwych i przekazywać naszych danych innym firmom) nie będą musiały informować swoich klientów o tym:

– czy stosują zautomatyzowane podejmowanie decyzji (w tym na podstawie profilowania); a jeśli tak, jakie są zasady podejmowania tych decyzji oraz znaczenie i przewidywane konsekwencje dla osoby, której dane dotyczą;

– jak długo mają zamiar przetwarzać dane;

– jak podchodzą do kwestii zabezpieczenia danych;

– czy podanie danych osobowych jest wymogiem ustawowym albo jest niezbędne do zawarcia umowy oraz czy jesteśmy zobowiązani do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Bez tych informacji osoba, która decyduje się przekazać dane, nie będzie w stanie ocenić związanego z tą decyzją ryzyka. Świadomość czynników, o których mowa w art. 13 ust. 2 RODO, może zadziałać jak sygnał alarmowy – np. jeśli z przekazanych

informacji wynika, że administrator nie podchodzi odpowiedzialnie do zabezpieczenia danych albo zamierza trzymać dane w nieskończoność. Z perspektywy osoby, której dane dotyczą, ta wiedza ma największą wartość właśnie w momencie podejmowania decyzji, czy przekazać dane.

Zgodnie z projektem małe i średnie przedsiębiorstwa nie będą też musiały w aktywny sposób informować swoich klientów o ich prawie do:

– żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania;

– wniesienia sprzeciwu wobec przetwarzania;

– przenoszenia danych;

– wniesienia skargi do organu nadzorczego.

O ile te informacje są mniej newralgiczne z perspektywy oceny ryzyka, o tyle pełnią ważną funkcję uświadamiającą: żeby móc skorzystać ze swojego prawa, najpierw trzeba się o nim dowiedzieć. Oczywiście, można sobie wyobrazić, że tę rolę przejmą kampanie prowadzone przez PUODO. Jednak o wiele łatwiej i taniej podstawową wiedzę na ten temat mogą przekazać firmy, które tak czy inaczej kontaktują się ze swoimi klientami i przetwarzają ich dane.

Kolejną ofiarą taryfy ulgowej dla MŚP jest obowiązek informowania o naruszeniu bezpieczeństwa danych. Mniejsze firmy, wśród których może się np. znaleźć dostawca poczty elektronicznej czy sklep internetowy, nie będą musiały informować swoich klientów, jeśli dojdzie do wycieku ich danych, mimo że takie zdarzenie oznacza wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą (tylko w takich okolicznościach wymaga tego RODO). Łatwo sobie wyobrazić niebezpieczny wyciek haseł, o którym klienci dowiedzą się (o ile w ogóle) dopiero z mediów, bez szans na szybką reakcję i zabezpieczenie swojego konta przed włamaniem.

Wreszcie: małe i średnie przedsiębiorstwa nie będą musiały informować swoich kontrahentów, którym wcześniej przekazały dane, o tym, że ich klienci te dane usunęli albo sprostowali. Brak takiego obowiązku nie tylko ograniczy skuteczność praw osób, których dane dotyczą (nieprawidłowe lub zbędne dane, które próbowali usunąć, nadal będą krążyć), ale może też zaszkodzić innym administratorom (kontrahenci nie dowiedzą się, że dane, które przetwarzają, są nieaktualne albo niepoprawne).

W POSZUKIWANIU UZASADNIENIA (I DROGI WYJŚCIA)

Po co to wszystko? Możemy tylko spekulować, ponieważ ani Ministerstwo Cyfryzacji, ani Ministerstwo Rozwoju (które zaproponowało inne standardy dla MŚP) nie wyjaśniło, jak został przeprowadzony test proporcjonalności – czyli analiza pokazująca, że korzyści z perspektywy interesu publicznego przewyższają straty i ryzyko po stronie obywateli. Jedynym argumentem, jaki powraca w uzasadnieniach, jest obiektywna trudność przekazania wymaganych informacji, kiedy dane są pozyskiwane przez telefon. Przy czym nie wiadomo, jak ta konkretna trudność ma się do sytuacji dziesiątek tysięcy firm o różnych modelach biznesowych.

Według raportu Polskiej Agencji Rozwoju Przedsiębiorczości za 2017 r. w Polsce działa 3,5 tys. dużych firm, co przekłada się na 0,2% sektora biznesu. Cała reszta to, z prawnego punktu widzenia, małe i średnie przedsiębiorstwa. Nie mamy danych pokazujących, ile z nich spełnia dodatkowe warunki, o których mowa w projekcie ustawy (nie przetwarza danych wrażliwych i nie przekazuje danych stronom trzecim na podstawie innej niż zgoda). Można jednak bezpiecznie założyć, że proponowane wyłączenia objęłyby większość firm przetwarzających dane osobowe, w tym całą rzeszę sklepów internetowych i firm z branży marketingu bezpośredniego.

W swojej masie to one wyznaczają rynkowy standard i mają istotną rolę do odegrania w upowszechnianiu dobrych praktyk. W

tym sektorze nie jest normą zawieranie umów przez telefon – o wiele częściej tym kanałem jest Internet, co pozwala zrealizować obowiązki informacyjne w stosunkowo tani i prosty sposób (wystarczy e-mail albo odpowiednia klauzula na stronie internetowej). Z kolei problem firm, które pozyskują dane przez telefon, można by rozwiązać poprzez węższe wyłączenie, zarezerwowane tylko dla takich sytuacji (ustawa mogłaby dopuszczać np. niezwłoczne przesłanie wymaganych informacji w formie elektronicznej).

Prace nad ustawą o ochronie danych osobowych jeszcze potrwają, a więc szansa na dopracowanie jej słabych elementów nadal istnieje. Zanim projekt trafi na agendę Rady Ministrów, musi przejść przez Komitet do spraw Europejskich, który zapewne zgłosi poważne zastrzeżenia do ograniczenia obowiązków, jakie przewiduje RODO (takie zastrzeżenia już zasygnalizowała Ministerstwu Cyfryzacji Komisja Europejska). Kolejna szansa na poprawki – w tym rządowe autopoprawki – będzie w parlamencie. Wreszcie, gdyby się okazało, że wyłączenia dla MŚP są politycznie nie do ruszenia, zostaje możliwość zaskarżenia polskiej ustawy do Trybunału Sprawiedliwości UE. Przy czym oczekiwanie na wyrok trybunału w Luksemburgu oznacza niepewność co do prawa i niepotrzebne koszty dla Polski, a więc lepiej by było, gdyby tę ustawę udało się naprawić własnymi rękami.

Autorstwo: Katarzyna Szymielewicz
Źródło: Panoptykon.org

BIBLIOGRAFIA

1. http://legislacja.rcl.gov.pl/docs//2/12302950/12457674/12457675/dokument329506.pdf

2. https://panoptykon.org/wiadomosc/premier-podstawia-noge-rodo

3.

https://panoptykon.org/biblio/wystapienie-fundacji-panoptykon-i-polskiej-rady-biznesu-w-sprawie-prac-nad-ustawa-o-ochronie