

Zdażyć przed majem 2018 r.

Wiosną tego roku powinniśmy poznać ostateczny projekt aktu prawnego, który zastąpi obowiązujące przepisy w zakresie ochrony danych osobowych. Obecnie obowiązujące prawo nie gwarantuje bowiem ich bezpieczeństwa.

Jerzy MAJKA

– Obowiązująca ustawa, poprzez swoją nieaktualność i nieadekwatność, nie zapewnia gwarancji poszanowania prywatności nas wszystkich – podkreślił **dr Maciej Kawecki**, doradca w Gabinetie Politycznym Ministra Cyfryzacji, odpowiedzialny za reformę polskiego systemu ochrony danych osobowych.

Uchwalenie zupełnie nowych regulacji w tym zakresie konieczne jest również, a raczej przede wszystkim, z uwagi na obowiązujące od maja przyszłego roku ogólne rozporządzenia o ochronie danych (GDPR). – Ustawodawca unijny ograniczył w tym zakresie swobodę państw członkowskich do przyjęcia własnych regulacji, wyłącznie do zapewnienia skutecznego stosowania rozporządzenia w swoich wewnętrznych porządkach prawnych – przypomniał przedstawiciel resortu cyfryzacji.

Aby skutecznie przygotować polski system prawny do efektywnego stosowania nowej unijnej regulacji, nie wystarczy uchylene obowiązującej ustawy o ochronie danych osobowych i stworzenie nowego aktu prawnego, kompleksowego wobec rozporządzenia GDPR. Przepisy odnoszące się do problematyki ochrony danych osobowych znajdują się bowiem w setkach najprzeróżniejszych aktów prawnych, poczynając od kodeksu postępowania administracyjnego, a kończąc na ustawach regulujących funkcjonowanie poszczególnych segmentów rynku.

Kompleksowa reforma systemu ochrony danych osobowych wymaga zatem współdziałania całego

urzędu. – Każdy z resortów odpowiedzialny jest za przegląd swojego ustawodawstwa sektorowego z punktu widzenia możliwych zmian i przekazanie propozycji przepisów do Ministerstwa Cyfryzacji – zadeklarował Maciej Kawecki. Stosowne zawiadomienie powinny złożyć również te ministerstwa, które chciałyby skorzystać ze zwolnień przewidzianych w unijnym rozporządzeniu.

Bez silnego GIODO nie ma skutecznej ochrony prywatności

Jednym z istotniejszych kierunków podjętych prac legislacyjnych jest głębokie odformalizowanie całego procesu. – Celem działań podejmowanych przez ustawodawcę krajowego nie może być ochrona dotychczasowego systemu instytucjonalnego i prawnego w zakresie ochrony danych osobowych, ale stricte ochrona danych osobowych poprzez zapewnienie systemu realizującego efektywną ich ochronę – wskazał przedstawiciel resortu cyfryzacji. Wyraził równocześnie pogląd, iż odformalizowanie postępowań związanych z ochroną danych osobowych pozwoli na lepsze wypełnienie zasadniczego celu rozporządzenia GDPR, jakim jest skuteczniejsze zabezpieczenie prywatności.

Podstawową instancją stojącą na straży danych osobowych powinien zostać oczywiście GIODO. – Bez sprawnie działającego organu egzekwującego ochronę naszych danych osobowych, stosowanie ogólnego rozporządzenia o ochronie danych będzie tylko na papierze, na czym stracą wszyscy: zarówno osoby, których prawa powinny być chronione, jak i przedsiębiorcy – stwierdził koordynator reformy systemu ochrony danych. Zwiększeniu skuteczności działań inspektora miałyby posłużyć:

- ▶ utworzenie Rady ds. Ochrony Danych – członkowie tego organu powinni być wybierani kadencyjnie, a kryteria ich wyłaniania powinna jednoznacznie określać ustawa;
- ▶ wprowadzenie zasady, w myśl której kandydat na GIODO powinien dysponować wieloletnim doświadczeniem zawodowym w zakresie danych osobowych;

Odformalizowanie postępowań związanych z ochroną danych osobowych pozwoli na lepsze wypełnienie zasadniczego celu rozporządzenia GDPR, jakim jest skuteczniejsze zabezpieczenie prywatności.

- ▶ umożliwienie GIODO samodzielnego kształtowania własnego statutu, co stanowiłoby wyjątek od powszechnej praktyki. – Rozwiązanie takie zapewni możliwość szybkiego reagowania na potrzebę wyodrębniania nowych jednostek wewnątrz organu, czerpiąc doświadczenia ze stosowania nowego dla wszystkich prawa ochrony danych osobowych – ocenił Maciej Kawecki;
 - ▶ zwiększenie liczby zastępców inspektora, którym przypisać powinny poszczególne obszary działalności urzędu.
- Organ, którego istotą w świetle obowiązującego prawa jest wspieranie obywateli w ochronie ich prawa podstawowego, jakim jest ochrona danych osobowych, nie jest więc w stanie reagować na wszelkie informacje związane z incydentami jej naruszenia. Nie jest też w stanie wspierać obywateli poprzez podwyższanie świadomości na temat ochrony ich prywatności, również we wszelkich indywidualnych sprawach kierowanych do organu mniej formalnymi kanałami – podkreślił przedstawiciel resortu cyfryzacji, wskazując przykład zlikwidowania w ubiegłym roku infolinii GIODO, co motywowane było brakami kadrowymi.

Chroniąc dane, nie ograniczamy wolności gospodarczej

Gruntowne zmiany obejmą również obowiązki przedsiębiorców, w tym instytucji finansowych, związane z zapewnieniem bezpieczeństwa gromadzonych danych. Ekspert Ministerstwa Cyfryzacji

podkreślił, że rozporządzenie GDPR odchodzi od sztywnych i sprecyzowanych w ustawach zasad bezpieczeństwa, wprowadzając kryterium ryzyka jako podstawę dla zastosowania określonego rodzaju środków. – *Każdy przetwarzający dane osobowe musi ocenić, czy w danym stanie faktycznym zastosował dostępne i uznane w chwili przetwarzania za stabilne technologicznie środki zapewniające najwyższą ochronę danych osobowych* – zauważył Kawecki. Przedstawiciel rządu zapewnił również, iż reprezentowany przez niego resort będzie dokładać wszelkich starań, by nowe przepisy w zakresie ochrony danych nie powodowały zbytniego obciążenia dla przedsiębiorców i nie ograniczały bezpodstawnie swobody działalności gospodarczej, będącej wszak równoważną wartością konstytucyjną. W toku prac nad przygotowaniem polskiego systemu prawnego na przyjęcie rozporządzenia GDPR zwrócono uwagę m.in. na konieczność zwiększenia ochrony treści będących szeroko rozumianą tajemnicą przedsiębiorstwa (np. know-how, patenty czy kody źródłowe oprogramowania). W obecnym stanie prawnym dokonujący kontroli pracownicy GIODO (jak również wielu innych organów państwowych) nie są z mocy ustawy objęci obowiązkiem zachowania tajemnicy w tym zakresie. A w przypadku ujawnienia danych ważnych dla firmy ta ostatnia może dochodzić ewentualnych roszczeń jedynie w ramach postępowania sądowego wytoczonego z powództwa cywilnego. – *Wprowadzenie takiej tajemnicy wprost do ustawy wydaje się kolejną gwarancją ochrony informacji o nas samych* – stwierdził przedstawiciel rządu.

Z kolei Generalny Inspektor Danych Osobowych **dr Edyta Bielak-Jomaa** zwraca uwagę na fakt, iż rozwiązania GDPR mają priorytet nad przepisami rangi krajowej, na-



Dag Tyndale

wet jeżeli te ostatnie wydawane są na podstawie stosownych unijnych dyrektyw. W przypadku sektora bankowego chodzi tu w szczególności o dyrektywę PSD2, która zobowiązuje banki do otwarcia swych zasobów dla podmiotów konkurencyjnych. Zdaniem GIODO, ustawodawca już na etapie prac nad implementacją dyrektywy powinien uwzględnić regulacje w zakresie danych osobowych, a zatem również GDPR, które oficjalnie weszło w życie w maju ub.r., a jedynie jego stosowanie odroczone zostało o dwa lata.

IOD, czyli pierwsza instancja

Wśród licznych obszarów, które pozostały do uregulowania w nowym modelu ochrony danych osobowych szczególne znaczenie odgrywa kwestia kompetencji inspektorów danych osobowych (IOD). Stanowią oni będą niejako pierwszą instancję systemu gwarantującego ochronę bezpieczeństwa gromadzonych danych. W myśl nowego prawa unijnego mianowanie takiej osoby będzie obligatoryjne w przypadku organów i podmiotów publicznych (z wyjątkiem sądów), podmiotów przetwarzających dane wrażliwe oraz informacje o wyrokach w sprawach karnych, jak też instytucji, których główna działalność „polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę”. Do tej ostatniej kategorii zdaje się zaliczać zdecydowana większość instytucji finansowych.

Nie oznacza to jednak, iż każdy najmniejszy bank spółdzielczy będzie musiał ustanawiać własnego inspektora ochrony danych osobowych. Dr Edyta Bielak-Jomaa podkreśla, iż nowe przepisy uwzględniają możliwość scedowania tego obowiązku placówce zrzeszającej w przypadku podmiotów funkcjonujących w zrzeszeniach. W takim przypadku kluczowe jest jednak, aby czyn-

niki takie, jak zasięg terytorialny funkcjonowania danego zrzeszenia lub liczba jego członków były adekwatne do możliwości inspektora. Dlatego nowe regulacje przewidują możliwość powołania w takich przypadkach zastępców inspektora danych osobowych.

Warto również podkreślić, że wiele instytucji, w tym również banków, dysponuje już osobą o kompetencjach analogicznych do IOD. To efekt przezorności polskiego rządu, który w toku niedawnej nowelizacji przepisów o ochronie danych osobowych wziął pod uwagę kierunek prac prowadzonych w Europarlamencie i wprowadził funkcję administratora bezpieczeństwa informacji (ABI). Stanowisko to ma charakter dobrowolny, jednak – zdaniem GIODO – firmy, które zdecydowały się na ustanowienie ABI znacznie lepiej radzą sobie z przestrzeganiem zasad ochrony danych osobowych aniżeli pozostałe podmioty. Utrzymanie dotychczasowej kadry, która zdążyła już nabyć pewnego doświadczenia na tym odpowiedzialnym stanowisku powinno być zdaniem GIODO jednym z celów przyświecających ustawodawcy.

– *W nowych regulacjach powinien znaleźć się przepis, który stanowiłby, iż administratorzy bezpieczeństwa informacji zarejestrowani przed wejściem w życie nowych regulacji stali się inspektorami ochrony danych* – podkreśla dr Edyta Bielak-Jomaa.

Ochrona danych osobowych polskiego obywatela przed marketingowymi zakusami globalnych koncernów to obowiązek państwa wynikający z ochrony jego strategicznych interesów. Obrona danych typowego Kowalskiego to pierwsza cegiełka w murze obronnym infrastruktury krytycznej III RP. To smutna, choć nieuchronna konieczność, gdy Polska stała się jednym z celów regularnych cyberataków, inspirowanych nie tylko przez świat przestępczy. ■