FUNDACJA PANOPTYKON

Warszawa, 20 marca 2017 r.

5 postulatów dotyczących reformy ochrony danych w Polsce

1. Dobre gwarancje poszanowania prawa do ochrony danych obywateli w przepisach sektorowych

Unijne przepisy ustalają jednolite standardy ochrony danych we wszystkich krajach członkowskich. Jednocześnie przyznają państwom pewien margines swobody w ustalaniu nowych reguł w konkretnych obszarach jak np. ochrona zdrowia, badania czy stosunki pracownik – pracodawca. W praktyce oznaczać to może m.in. ograniczanie niektórych uprawnień obywateli jak np. prawo do informacji o przetwarzaniu danych osobowych w określonych sytuacjach.

Istnieje realne ryzyko, że te ograniczenia w istotny sposób mogą nadwyrężyć system ochrony danych. Polski rząd nie może dopuścić, do sytuacji, w której ochrona danych osobowych w konkretnych obszarach stanie się fikcją. Do takich przypadków zaliczamy chociażby stosowanie technik profilowania czy automatycznego podejmowania decyzji w sektorze bankowym czy ubezpieczeniowym. Innym wrażliwą kwestią będzie ustalenie zakresu danych pracowników wykorzystywanych przez pracodawców czy udzielnie przez dzieci zgody na przetwarzanie danych. Wszystkie powyższe przykłady wiążą się z bardzo konkretnymi problemami społecznymi i sytuacjami, w których obywatele powinni zachować wysokie gwarancje ochrony swoich praw.

Reforma ochrony danych było wielkim wysiłkiem i jednocześnie stanowi ogromną szansę dla zapewnienia obywatelom lepszego standardu ochrony prywatności. Nie możemy tej szansy zmarnować. Dlatego oczekujemy, że polskie władze nie wprowadzą daleko idących wyłączeń a sam proces przyjmowania nowych przepisów będzie przejrzysty oraz prowadzony we współpracy z partnerami społecznymi.

2. Silny i niezależny organ ochrony danych osobowych

Podstawą dobrego i skutecznego systemu ochrony danych osobowych jest organ, który będzie mógł wyegzekwować obowiązujące przepisy prawne. Unijna reforma przyznaje organowi stojącemu na straży ochrony prywatności nowe i silniejsze kompetencje – jak chociażby nakładanie znacznych kar finansowych za naruszenie prawa. O kształcie i zasadach funkcjonowania organu zdecyduje polski prawodawca. Decyzja ta powinna zagwarantować niezależność instytucji oraz być daleka o zawirowań bieżącej polityki. Decydenci muszą pamiętać, że prawo do ochrony danych osobowych i autonomia informacyjna jest prawem gwarantowanym Konstytucją Rzeczypospolitej Polskiej (art. 51). Dlatego też instytucjonalne ramy ochrony tego prawa muszą zapewniać adekwatny standard jego ochrony. Wytyczne w zakresie niezależności organu ochrony danych osobowych zostały określone również w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Np. w wyroku w sprawie Komisja Europejska p. Węgrom, sygn. C-288/12 Trybunał wskazał, że organy nadzorcze

powinny mieć możliwość wykonywania swoich zadań bez jakiegokolwiek wpływu z zewnątrz. Wymóg ten oznacza, że organy nie mogą być związane żadnymi instrukcjami w zakresie wykonywanych przez siebie funkcji oraz że powinny podejmować swoje decyzje bez jakiegokolwiek wpływu politycznego – „ gdyż samo zagrożenie takiego wpływu powinno zostać usunięte".

Naszym zdaniem osoba (lub osoby) stojąca na czele organu zajmującego się ochroną danych osobowych powinny charakteryzować się wysokim poziomem wiedzy merytorycznej i doświadczeniem oraz posiadać silny, demokratyczny mandat w pełnieniu swoich funkcji. Taki mandat gwarantuje przede wszystkim wybór osoby lub osób sprawującą tą funkcję przez parlament RP. Rozwiązanie takie nie jest oczywiście idealne. Jednak dzięki niemu najważniejszy organ władzy w Polsce zachowa wpływ na kształt ochrony praw konstytucyjnych. Procedura wyboru powinna jednak obejmować również weryfikację merytoryczną kompetencji oraz aktywny udział partnerów społecznych.

Niezależność organu przekłada się również na problem kadencji organu ochrony danych i jej ewentualnego skrócenia. Organ nadzoru nie może być dowolnie odwoływany i powoływany np. przez Prezesa Rady Ministrów, jak dzieje się to np. w przypadku prezesa Urzędu Ochrony Konkurencji i Konsumentów czy prezesa Urzędu Komunikacji Elektronicznej. Zgodnie z orzecznictwem TSUE kadencja organu musi być ściśle wyznaczona, a władza polityczna może ją skrócić tylko w przypadku poważnej i obiektywnie weryfikowalnej przyczyny (jak np. popełnienie poważnego przestępstwa) oraz przy zachowaniu odpowiednich gwarancji proceduralnych. Przy czym wymóg ten dotyczy również sytuacji przekształcenia lub zmiany modelu funkcjonowania samego organu.

3. Przejrzysty proces wdrożenia reformy

Dynamiczny rozwoju cyfrowej gospodarki wymaga wprowadzenia wysokiego poziomu ochrony danych osobowych. Niestety dla części biznesu ochrona prywatności staje się niechcianą „barierą regulacją". Prace nad unijną reformą pokazały, że instytucje odpowiedzialne za kształtowanie nowych przepisów są obiektem zmasowanego i nie zawsze przejrzystego lobbingu ze strony biznesu. Wdrożenie nowych regulacji i dostosowanie ich do polskich realiów jest procesem, w którym może pojawić się podobne zjawisko. Dlatego uważamy, że polskie władze powinny w przypadku procesu legislacyjnego dotyczącego reformy ochrony danych zagwarantować bardzo wysoki poziom przejrzystości. Przykładem dobrych praktyk w tym względzie były działania sprawozdawcy projektu rozporządzenia dotyczącego ochrony danych osobowych w Parlamencie Europejskim – Jana Albrechta. Niemiecki europoseł publikował na swojej stronie rejestr wszystkich spotkań z grupami interesów oraz wszystkie dokumenty, listy, rekomendacje powstałe na potrzeby procesu legislacyjnego lub które otrzymał sprawozdawca

Podobnych praktyk oczekujemy od polskich władz publicznych. Uważamy, że resorty pracujące nad dostosowaniem polskiego prawa do norm unijnych powinny opublikować listy spotkań z interesariuszami, precyzyjne plany legislacyjne, stanowiska i inne dokumenty zgłoszone przez różnych partnerów. W całym procesie dostrzegamy również szczególną rolę dla Ministerstwa Cyfryzacji. Powinno ono czuwać nad spójnym wdrożeniem reformy, ale również informować opinię publiczną o projektach innych ministerstw, które związane są z dostosowaniem polskich przepisów do nowego unijnego prawa.

4. Procedura przyjazna obywatelom

Reformy ochrony danych przyznała obywatelom nowe możliwość ochrony ich praw. To silne gwarancje, które jednak by mogły być faktycznie egzekwowane, wymagają odpowiednich narzędzi proceduralnych. Dotyczy to zarówno możliwości składania skarg do organu nadzorczego jak i obrony swoich spraw przed sądami powszechnymi. Obywatel zwracając się do instytucji chroniącej dane powinien oczekiwać, że jego sprawa zostanie załatwiona szybko i sprawie. Stąd procedura przed organem ochrony danych powinna zawierać możliwie krótkie terminy rozpatrzenia skarg, określać w sposób przejrzysty uprawnienia stron.

Unijna reforma uwzględnia również możliwość uzyskania odszkodowania w przypadku naruszenia prawa ochrony danych. Obecny system prawny w Polsce takiej możliwości nie uwzględnia. Wyjątkiem są sprawy z zakresu naruszenia dóbr osobistych, które – choć podobne – nie są tożsame z ochroną danych osobowych. Dlatego też ustawodawca będzie musiał wprowadzić konkretne zmiany w przepisach dotyczących postępowania przed sądami powszechnymi. Uważamy, że sprawy z zakresu ochrony danych osobowych w kwestiach dotyczących odszkodowań powinny rozpatrywać sądy cywilne.

5. Organizacje społeczne jako adwokaci interesu publicznego

Organizacje społeczne mogą odegrać ważną i pozytywną rolę w praktycznym kształtowaniu standardów ochrony danych osobowych. Zgodnie z unijnymi przepisami organizacje będą mogły reprezentować obywateli przed organem ochrony danych i sądami. Bardzo często naruszeń prywatności mogą dopuszczać się duże podmioty posiadające spore zasoby finansowe i profesjonalną obsługę prawną. W takich sytuacjach dochodzić może do faktycznej nierówności stron postępowania i równocześnie negatywnie odbijać się na pozycji obywateli składających skargi. Udział wyspecjalizowanych organizacji społecznych posiadających fachową wiedzę w zakresie ochrony danych osobowych może zmniejszać te nierówność.

Dodatkowo kraje członkowskie mogą przyznać organizacjom kompetencje we wnoszeniu skarg „w interesie publicznym". To ważna funkcja, która powinna znaleźć swoje odzwierciedlenie również w polskim systemie prawnym. Organizacja społeczne mogłyby żądać wszczęcia postępowania przed organem ochrony danych osobowych w sytuacji gdy wykryje potencjalne naruszenia prawa przez konkretne podmioty. Takimi przypadkami mogą być np. polityki prywatności portali internetowych zawierające klauzule rażąco naruszające prawa konsumentów. Przyznanie tych dodatkowych kompetencji organizacjom społecznym mogłoby wzmocnić poziom ochrony danych osobowych oraz pomóc organowi ochrony danych w egzekwowaniu przepisów. Jednocześnie służyłoby podnoszeniu świadomości obywateli w zakresie ochrony prywatności i danych osobowych.