FUNDACJA PANOPTYKON

Robocze uwagi Fundacji Panoptykon[1]
do projektu ustawy o ochronie danych osobowych w wersji z 8 lutego

Spis treści:

1. Wyłączenia stosowania niektórych uprawnień jednostki dla MŚP

Ministerstwo Cyfryzacji proponuje, by firmy zatrudniające mniej niż 250 osób, nie przetwarzające danych wrażliwych oraz nieudostępniające danych innym podmiotom – nie były zobowiązane do realizacji obowiązków wynikających z art. 13 ust. 2 (z wyjątkiem litery c) oraz art. 15 ust. 3-4, art. 19 i art. 34.

Opinia Panoptykonu

Naszym zdaniem klucz wyłączenia (250 pracowników) jest nieadekwatny i nieproporcjonalny (szerzej: lit. a), a zaproponowane wyłączenia nadmiernie ograniczają prawa podmiotów danych (szerzej: lit. b i c).

a. Nieadekwatny i nieproporcjonalny klucz wyłączenia (250 pracowników) uprawnień jednostki

Zgodnie z danymi Polskiej Agencji Rozwoju Przedsiębiorczości sektor MSP (miko, małe i średnie firmy) stanowi 99,8% przedsiębiorstw w Polsce.

Potrzeba ograniczenia obowiązków spoczywających na firmach (zwłaszcza ograniczenia zakresu informacji, jakie MŚP powinny przekazywać podmiotom danych), jest uzasadniana interesem ekonomicznym tego sektora, w szczególności dodatkowymi kosztami, jakie będą ponosić przedsiębiorcy pozyskujący dane osobowe przez telefon. Ponieważ katalog obowiązkowych informacji na gruncie RODO jest bardziej rozbudowany, wydłuży się czas potrzebny na ich przekazanie, co niesie ze sobą ryzyko zniechęcenia potencjalnych klientów i utrudni pracę call-center. Takie uzasadnienie pomija fakt, że nie wszystkie małe i średnie przedsiębiorstwa pozyskują dane przez telefon. A skoro tak, proponowane wyłączenie nie jest adekwatne do celu, jaki stawia sobie rząd, szukając sposobu na odciążenie małych i średnich przedsiębiorstw.

[1] Uwagi przygotowane przez Katarzynę Szymielewicz i Wojciecha Klickiego

Bardziej uzasadnionym rozwiązaniem byłoby ograniczenie obowiązku informacyjnego jedynie w sytuacjach, w których umowa jest zawierana przez telefon. Przy czym nawet taką propozycję trudno obronić na gruncie zasady proporcjonalności, której zachowania - w przypadku ograniczania praw jednostki - wymaga RODO i polska konstytucja. Aby osiągnąć postulowany cel, wystarczyłoby doprecyzowanie, że w przypadku pozyskiwania danych osobowych przez telefon administrator nie musi podawać informacji, o których mowa w art. 13 ust 2 RODO, jeśli jest w stanie je przekazać w innej formie zanim umowa zostanie ostatecznie zawarta (np. w polityce prywatności opublikowanej na stronie internetowej lub w umowie, która po bezpośrednio rozmowie telefonicznej zostanie wysłana do klienta).

W pracach nad RODO europejski ustawodawca rozważał wprowadzenie wyjątków dla małych i średnich przedsiębiorstw, jednak w żadnym momencie nie brano pod uwagę ograniczenia obowiązków informacyjnych. W toku prac nad rozporządzeniem ustawodawca unijny doszedł do wniosku, że liczba zatrudnianych pracowników nie jest odpowiednią podstawą dla projektowania wyjątków od ogólnych reguł ochrony danych osobowych, ponieważ w żaden sposób nie przekłada się na ilość przetwarzanych przez przedsiębiorstwo danych ani na ryzyko, które taka działalność generuje. W uzasadnieniu proponowanego ograniczenia obowiązków z art. 13 ust. 2 RODO rząd musiałby zatem wskazać, jakie konkretnie obciążenia wiążą się z realizacją tych obowiązków przez przedsiębiorców zatrudniających poniżej 250 pracowników oraz z czego wynika przekonanie, że wszystkie małe i średnie przedsiębiorstwa (bez względu na ilość przetwarzanych danych i związane z tym ryzyko) należy potraktować w ten sam sposób.

Z przytoczonych powodów wyłączenie obowiązków informacyjnych wynikających z art. 13 ust 2 RODO dla szerokiej kategorii przedsiębiorców narusza zasadę proporcjonalności, a tym samym jest niezgodne z art. 23 RODO. W przypadku rozbieżności między RODO a prawem krajowym, pierwszeństwo ma prawo europejskie. A zatem, w sytuacji, w której polscy przedsiębiorcy będą się stosować do przepisów ustawy o ochronie danych osobowych, która - w zakresie przewidzianych wyłączeń - jest niezgodna z RODO, narażają się na poważne ryzyko prawne. Mimo przeświadczenia, że działają zgodnie z polskim prawem, mogą się spotkać z sankcjami (w tym karami finansowymi) za naruszenie bezpośrednio obowiązującego rozporządzenia.

b. **Ograniczenie obowiązków informacyjnych (art. 13 ust. 2)**

Zasada przejrzystości to jeden z filarów RODO i warunek legalności przetwarzania danych osobowych. Zgodnie z tą zasadą, wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Jej uszczegółowieniem jest art. 13, wskazujący, które informacje i komunikaty powinny być przekazane przez administratora już w momencie zbierania danych osobowych. Za tą konstrukcją prawną stoi następująca logika: podmiot danych powinien być w stanie ocenić ryzyko związane z przekazaniem swoich danych administratorowi, zanim to zrobi. Dlatego kluczowe informacje dla dokonania takiej oceny ryzyka powinny zostać przekazane tak wcześnie, jak to możliwe (najpóźniej w momencie przekazania danych).

Dlatego podmiot danych powinien - przed podjęciem decyzji o przekazaniu danych - zostać poinformowany o **kluczowych czynnikach ryzyka**, do których niewątpliwie należą:

- okres, przez który dane osobowe będą przechowywane (im dłuższy lub im bardziej niedookreślony, tym potencjalnie większe ryzyko dla podmiotu danych)
- fakt zautomatyzowanego podejmowania decyzji w oparciu o przetwarzane dane osobowe.

Świadomość tych czynników może być przesądzająca w momencie podawania danych osobowych. Szczególnie, że na gruncie RODO zautomatyzowane podejmowanie decyzji jest - nie bez powodu - uważane za czynnik zwiększający ryzyko związane z przetwarzaniem danych.

Nieco inny sens, z perspektywy osoby, której dane dotyczą, ma informacja o tym: czy podanie danych osobowych jest wymogiem ustawowym lub umownym; czy jest ona zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych; oraz o możliwości cofnięcia zgody w dowolnym momencie. W tych przypadkach zasadność przekazania informacji najpóźniej w momencie przekazania danych wiąże się z ich perswazyjnym charakterem i bezpośrednim wpływem na podejmowaną przez podmiot danych decyzję.

Ma to szczególne znaczenie w sytuacji, w której niepodanie danych niezbędnych do zawarcia umowy albo wymaganych przepisami prawa może mieć dla osoby, która podejmuje taką decyzję, negatywne konsekwencje (np. odrzucenie wniosku o kredyt, odrzucenie zgłoszenia w ramach rekrutacji, kontrolę skarbową). Wyjaśnienie takich konsekwencji, jak również uświadomienie osobie, której dane dotyczą, istnienia prawnego obowiązku albo zależności między możliwością zrealizowania umowy i podaniem danych, powinno mieć raczej pozytywny wpływ na jej decyzję (a więc leży w interesie administratora).

Jeszcze inny cel ma poinformowanie o uprawnieniach, które podmiot danych może realizować dopiero po przekazaniu danych osobowych, tj. o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, o prawie do przenoszenia danych, a także o prawie wniesienia skargi do organu nadzorczego. Świadomość tych uprawnień jest logicznym warunkiem ich realizacji, a więc ważne jest, by wiedza na ten temat była skutecznie przekazywana.

Europejski ustawodawca uznał, że najmniej kosztownym (w wymiarze społecznym) sposobem na uświadomienie osobom, których dane są przetwarzane, przysługujących im praw, jest uwzględnienie tej informacji w komunikacji, która i tak się odbywa na linii podmiot danych - administrator. W tym kontekście kluczowa jest jakość przekazanej informacji, a nie moment jej przekazania. Jeśli stanowi to obiektywną trudność dla administratora (np. ze względu na wybrany kanał czy formę komunikacji) w momencie zbierania danych osobowych, można dopuścić ich przekazanie w późniejszym momencie lub odesłanie podmiotu danych do informacji opublikowanych w polityce prywatności (dostępnej na stronie internetowej).

Propozycja Panoptykonu

Zamiast blankietowego wyłączenia art. 13 ust 2 proponujemy taryfę ulgową dla MŚP, polegającą na tym, że nie wszystkie informacje wymagane przez RODO muszą być podane w momencie pozyskania danych osobowych od klienta.

W szczególności, informacje o prawie do żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania mogą być udostępniane na stronie internetowej administratora (w ramach polityki prywatności). Przy czym te informacje powinny być zawarte również w treści umowy zawartej z podmiotem danych. Informacja o prawie skargi do organu nadzorczego również może być udostępniona w polityce prywatności.

Natomiast następujące informacje powinny być podane w momencie przekazywania danych osobowych:

- o okresie, przez który dane osobowe będą przechowywane
- o zautomatyzowanym podejmowaniu decyzji (w tym o tym, jakie są zasady ich podejmowania, oraz jakie znaczenie konsekwencje takie przetwarzanie ma dla osoby, której dane dotyczą)
- o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym (i jakie są ewentualne konsekwencje niepodania danych).

c. Ograniczenie innych obowiązków (art. 15 ust. 3-4, art. 19 i art. 34 RODO)

[artykuł 15 ust. 3-4]

Zwolnienie MŚP z obowiązku dostarczania kopii danych osobowych nie będzie stanowić znacznego zmniejszenia obciążenia dla przedsiębiorców, ponieważ wciąż będą oni zobowiązani umożliwić dostęp do danych, co wiąże się z koniecznością ich przygotowania. Dodatkowo, zgodnie z art. 12 RODO, możliwe jest pobranie opłaty lub odmowa żądania, jeśli jest ono ewidentnie nieuzasadnione i nadmierne lub ma charakter ustawiczny.

Natomiast z perspektywy podmiotów danych możliwość uzyskania kopii dotyczących go danych może być niezwykle cenna w sytuacjach przetwarzania dużych ilości danych, którymi podmiot danych nie dysponuje w żadnej innej formie (np. ze względu na ich techniczny charakter). Dodatkowo, w niektórych sytuacjach może dochodzić do sytuacji, że podmiot danych - chcąc samodzielnie dysponować zbiorem danych na swój temat - zamiast skorzystać z uprawnienia z art. 15 ust. 3, skorzysta z uprawnienia do przeniesienia danych (art. 20), którego realizacja po stronie MŚP wymaga większego nakładu pracy, niż przygotowanie kopii danych.

[art. 19]

RODO przyznaje jednostkom uprawnienia do sprostowania, usunięcia danych osobowych (tzw. prawo do bycia zapomnianym) i prawo do ograniczenia przetwarzania np. w sytuacji zakwestionowania prawidłowości danych lub niezgodności przetwarzania z prawem.

Wyłączenie stosowania przez MŚP obowiązku, o którym mowa w art. 19 w praktyce podważa skuteczność uprawnień wymienionych w art. 16-18. Jednocześnie art. 19 RODO nie wiąże się z nadmiernymi obciążeniami dla MŚP, ponieważ administrator zwolniony jest z przekazywania informacji wówczas, gdy jest to niemożliwe lub wymaga niewspółmiernie dużego wysiłku.

Propozycja stanowi też obniżenie standardu wynikającego z ustawy o ochronie danych osobowych z 1997 r., zgodnie z którą administrator jest zobowiązany poinformować innych administratorów o dokonanym uaktualnieniu lub sprostowaniu danych (art. 35 ust. 3).

Propozycja Panoptykonu

Zdajemy sobie sprawę, że art. 35 ust. 3 obowiązującej ustawy o ochronie danych ma węższy charakter - ze względu na to, że RODO zobowiązuje do przekazania informacji nie tylko innym administratorom, ale "każdemu odbiorcy, któremu ujawniono dane", co może rodzić realne problemy. Jednak nic nie stoi na przeszkodzie, by ograniczyć obowiązki spoczywające na MŚP poprzez zawężenie obowiązków wynikających z art. 19 RODO i zobowiązanie MŚP do przekazywania informacji o skorzystaniu z uprawnień, o których mowa w art. 16-18 RODO wyłącznie do innych administratorów.

[art. 34]

Dzięki uzyskaniu wiedzy o naruszeniu, osoba, której dane dotyczą ma możliwość szybszej reakcji na zaistniałą sytuację, np. poprzez zmianę haseł dostępu do określonej usługi (np. poczty elektronicznej).

Jednocześnie art. 34 dotyczy jedynie wycieku wiążącego się z wysokim ryzykiem naruszenia praw osób, które dane dotyczą. Oznacza to, że MŚP nie będzie musiał informować o **każdym** wycieku. Zwolnić się od tego obowiązku może wówczas w sytuacji wdrożenia odpowiednich technicznych środków ochrony (np. szyfrowanie) uniemożliwiających osobom nieuprawnionym dostęp do danych osobowych lub gdyby wymagałoby to niewspółmiernie dużego wysiłku.

Krytycznej oceny tego wyłączenia nie zmienia fakt obowiązywania art. 33 RODO, czyli obowiązku poinformowania o wycieku Prezesa Urzędu Ochrony Danych Osobowych oraz okoliczność, że - jeśli PUODO rozpocznie postępowanie - za jego pośrednictwem o wycieku dowie się także podmiot danych. Intencją unijnego prawodawcy było bowiem umożliwienie podmiotom danych szybkiej interwencji (np. w postaci zmiany hasła) - proponowane wyłączenie uniemożliwi takie działanie.

2. **Prezesa Urzędu Ochrony Danych Osobowych – zagadnienia ustrojowe**

Ministerstwo Cyfryzacji proponuje, że Prezes Urzędu Ochrony Danych Osobowych będzie powoływany przez Sejm za zgodą Senatu. Względem pierwszej wersji projektu oznacza to rezygnację z przyznania Prezesowi Rady Ministrów wyłącznej kompetencji do wyznaczania kandydata na to stanowisko.

Jednocześnie zgodnie z projektem PUODO może mieć **zastępców** powoływanych na wniosek ministra właściwego do spraw informatyzacji (dwóch zastępców) i wniosek ministra właściwego do spraw wewnętrznych (jeden zastępca, wniosek w jego sprawie musi być zaopiniowany przez Ministra Sprawiedliwości, Ministra Obrony Narodowej i Ministra Finansów). Odwołanie zastępców także następuje na wniosek wskazanych ministrów. W poprzedniej wersji projektu mieliby być oni powoływani przez Prezesa Rady Ministrów.

Opinia Panoptykonu

Pozytywnie oceniamy decyzję w sprawie trybu wyboru PUODO. Ograniczenie wpływu Premiera na obsadę stanowiska PUODO jest szczególnie istotna ze względu na fakt, że organ będzie także kontrolować przetwarzanie danych osobowych w administracji rządowej. Wybór przez Sejm i Senat daje osobie pełniącej urząd najmocniejszy – po wyborach powszechnych – mandat demokratyczny.

Pozytywnie oceniamy także przyznanie PUODO (kosztem Premiera) możliwości powołania zastępców. Jednocześnie krytycznie oceniamy wpływ ministerstwa właściwego ds. informatyzacji i MSWiA na obsadę tych stanowisk: zgodnie z projektem PUODO będzie mógł bowiem na to stanowisko powołać (a następnie odwołać) wyłącznie osoby wskazane przez odpowiednich ministrów. Naszym zdaniem to rozwiązanie może stać w sprzeczności z motywem 121 RODO, zgodnie z którym „organ nadzorczy powinien dysponować własnym personelem, który jest dobierany przez ten organ nadzorczy".

Propozycja Panoptykonu

Naszym zdaniem zastępcy PUODO powinni być powoływani analogicznie, jak zastępcy Rzecznika Praw Obywatelskich – a więc wybór osoby powoływanej na to stanowisko powinien być autonomiczną decyzją Prezesa.

3. **<u>Organizacje pozarządowe w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych oraz postępowaniach sądowych</u>**

<u>Ministerstwo Cyfryzacji proponuje</u> (art. 55 projektu), by w sprawach związanych z ochroną danych osobowych pełnomocnikiem mógł być przedstawiciel organizacji, do której zadań statutowych należą sprawy związane z ochroną danych osobowych. Poza tym projekt nie zawiera innych przepisów, których celem byłoby wdrożenie art. 80 RODO.

<u>Opinia Panoptykonu</u>

Zapewnienie możliwie szerokiego udziału organizacji społecznych w postępowaniu związanym ze stosowaniem RODO ma fundamentalne znaczenie z racji na poziom skomplikowania materii, a także wagę właściwej implementacji i późniejszego stosowania rozporządzenia (oraz przepisów krajowych) dla praw podstawowych.

Unijny prawodawca dostrzegł konieczność umożliwienia organizacjom społecznym udziału w postępowaniach dotyczących ochrony danych osobowych w charakterze **pełnomocnika**. Tymczasem projekt ustawy zawęża tę możliwość do reprezentowania podmiotu danych wyłącznie do postępowania przed PUODO. Obowiązujące przepisy ustawy - Prawo o postępowaniu przed sądami administracyjnymi umożliwiają bowiem organizacji społecznej udział w postępowaniu przed sądem administracyjnym (a więc w postępowaniu ze skargi na decyzję PUODO), ale jedynie w charakterze uczestnika na prawach strony (por. art. 33 ppsa).

<u>Propozycja Panoptykonu</u>

W naszej ocenie racjonalnym rozwiązaniem byłoby umożliwienie organizacjom - na kształt propozycji zawartej w art. 55 projektu - reprezentowanie podmiotu danych przez organizację społeczną również na etapie postępowania sądowoadministracyjnego.

4. **<u>Kodeksy postępowań</u>**

<u>Ministerstwo Cyfryzacji proponuje</u>, by kodeksy sporządzało się po przeprowadzeniu konsultacji z zainteresowanymi podmiotami, w tym w szczególności, jeżeli to możliwe, z osobami, których dane dotyczą. Informacje o przeprowadzonych konsultacjach i ich wyniku przekazuje się PUODO, który może - w przypadku uznania konsultacji za niewystarczające - wezwać podmiot do ich ponownego przeprowadzenia. Jednocześnie projekt przesądza, że stroną postępowania przed PUODO w sprawie zatwierdzenia kodeksu jest wyłącznie wnioskodawca (wyłącza się art. 31 kpa).

<u>Opinia Panoptykonu</u>

Popieramy zwiększoną względem poprzedniej wersji projektu możliwość udziału osób zainteresowanych w pracach nad projektem kodeksu. Stanowi to dostrzeżenie rangi kodeksów dla praw i wolności. Wartość ta przyświecała także unijnemu prawodawcy, który w motywie 99 RODO sformułował postulat konieczności umożliwienia włączenia się partnerów społecznych i podmiotów, których dane dotyczą do prac nad kodeksem.

Jednocześnie obawiamy się, że zaproponowany przepis może budzić wątpliwości interpretacyjne oraz praktyczne. Po pierwsze autorzy projektów kodeksów mogą mieć trudności ze zdefiniowaniem, kim są zainteresowane podmioty, a następnie - z dotarciem do nich. Będzie to miało kluczowe znaczenie w decyzji PUODO, czy konsultacje były wystarczające.

Z kolei z perspektywy podmiotów potencjalnie zainteresowanych wzięciem udziału w pracach nad projektem kodeksu, monitorowanie informacji na temat potencjalnych konsultacji projektów, może okazać się niezwykle uciążliwe lub wręcz niemożliwe.

Propozycja Panoptykonu

Naszym zdaniem proces konsultacji kodeksów usprawniłby obowiązek publikacji ich projektów na stronie PUODO wraz z informacją o czasie trwających konsultacji (np. 30 dni). Oczywiście taka publikacja nie będzie oznaczać zwolnienia autorów projektu kodeksu od dotarcia - w miarę możliwości - do osób, których dane dotyczą, jednak ułatwi ona dotarcie do podmiotów potencjalnie zainteresowanych wzięciem udziału w konsultacjach.