



VII.501.315.2014.AG

**Pan
Joachim Brudziński
Minister Spraw Wewnętrznych
i Administracji**

Szanowny Panie Ministrze

W odpowiedzi na pismo z dnia 20 kwietnia 2018 r. (DP-WL-0231-46/2016/KKan), dotyczące przedstawionego w dniu 19 kwietnia 2018 r. na stronach Rządowego Centrum Legislacji **projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości** (UC116, dalej jako: projekt ustawy), działając na podstawie art. 16 ust. 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2017 r. poz. 958), Rzecznik Praw Obywatelskich przedstawia następujące uwagi.

W ostatnich miesiącach Rzecznik kilkakrotnie apelował do Ministra Spraw Wewnętrznych i Administracji o jak najszybsze przedstawienie projektu, który w założeniu ma dokonywać wdrożenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L z 4.5.2016 r., s. 89, dalej jako: dyrektywa 2016/680). Podkreślałem, jakie znaczenie ma pozostawienie wystarczająco długiego terminu na konsultacje i uzgodnienia zaproponowanych przepisów w związku z samą treścią postanowień dyrektywy 2016/680 i jej znaczeniem dla ochrony praw i wolności człowieka. **Wyznaczenie 10-dniowego terminu na przedstawienie uwag**

do projektu nie tylko nie pozwala na pełne ich opracowanie, ale także jest sprzeczne z Regulaminem pracy Rady Ministrów (por. §40 ust. 3 Regulaminu pracy Rady Ministrów – uchwała nr 190 Rady Ministrów z dnia 29 października 2013 r. *Regulamin pracy Rady Ministrów*; M.P. z 2016 r., poz. 1006 ze zm.). Wyznaczenie terminu do zajęcia stanowiska w przypadku projektu aktu normatywnego krótszego niż 14 dni od udostępnienia projektu wymaga szczegółowego uzasadnienia. W tym przypadku MSWiA wskazuje na konieczność wdrożenia dyrektywy 2016/680, jednak podkreślić należy i przypomnieć, że dyrektywa 2016/680 przyjęta została 27 kwietnia 2016 r., weszła w życie 5 maja 2016 r., a zatem **projektodawca miał prawie dwa lata na przygotowanie projektu**. Przedstawienie projektu w ostatnim możliwym terminie należy ocenić zatem krytycznie.

W związku z powyższym, Rzecznik przedstawia następujące uwagi, które jednak nie mogą być traktowane w sposób wyczerpujący.

1. Zakres stosowania ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Pozytywnie należy ocenić podejście zaproponowane w projekcie ustawy, polegające na określeniu zakresu podmiotowego stosowania ustawy poprzez cele, dla których następuje przetwarzanie danych osobowych (art. 1 projektu ustawy). Bez wątplenia ułatwi to dokonanie rozróżnienia między zakresem stosowania rozporządzenia ogólnego o ochronie danych osobowych, nowej ustawy o ochronie danych osobowych¹ i omawianej ustawy, której dotyczy przedstawiony projekt. Pewnym ułatwieniem będzie również zaproponowane określenie w przepisach zmieniających - w odniesieniu do poszczególnych ustaw dotyczących konkretnych służb - tych konkretnych sytuacji, w których przedstawiona ustawa będzie stosowana (por. np. dodawany art. 20 ust. 1a i n. w ustawie z dnia 6 kwietnia 1990 r. o Policji; Dz. U. z 2017 r. poz. 2067 ze zm.).

Jednakże - co już podkreślałem we wcześniejszych pismach - **nie mogę pozytywnie ocenić propozycji zawartej w art. 1 ust. 2 pkt 7 projektu ustawy, polegającej na wyłączeniu z zakresu jej stosowania danych osobowych przetwarzanych w ramach**

¹ Projekt ustawy o ochronie danych osobowych, druk sejmowy nr 2410.

realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

Nie wszystkie bowiem zadania ustawowe realizowane przez te służby mieszczą się w zakresie pojęcia „bezpieczeństwo narodowe”, co uzasadniałoby wyłączenie dopuszczone na mocy art. 2 ust. 3 pkt a dyrektywy 2016/680. Trzeba pamiętać, że z punktu widzenia prawa Unii Europejskiej pojęcie „bezpieczeństwo narodowe” nie może być utożsamiane z pojęciem „bezpieczeństwa wewnętrznego”, o czym świadczą przepisy samego Traktatu o Unii Europejskiej (TUE) i Traktatu o funkcjonowaniu Unii Europejskiej (TFUE; por. art. 4 ust. 2 TUE i art. 73 TFUE odnoszący się do „bezpieczeństwa narodowego” oraz chociażby art. 71 TFUE i art. 73 TFUE dotyczące „bezpieczeństwa wewnętrznego”). Również - przykładowo - zwalczanie terroryzmu nie jest uznawane w UE za domenę wyłączoną z zakresu prawa UE, o czym świadczy chociażby art. 83 ust. 1 TFUE. Dyrektywa 2016/680 zezwala na pozostawienie poza zakresem jej stosowania czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym, a w ogóle bezpieczeństwem (por. też motyw 14 preambuły do dyrektywy 2016/680) .

Poza przywoływanymi przeze mnie już we wcześniejszych pismach wątpliwościami dotyczącymi prawa do wyłączenia całej działalności Agencji Bezpieczeństwa Wewnętrznego², tym razem pragnę dodatkowo zwrócić uwagę na wyłączenie dotyczące Centralnego Biura Antykorupcyjnego. Zgodnie z art. 1 ust. 1 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2017 r., poz. 1993 ze zm.), CBA jest służbą specjalną do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa. **Działalność CBA nie ma zatem bezpośredniego związku z bezpieczeństwem narodowym.** Dodatkowo, w obecnym stanie prawnym, w art. 22a i n. ustawy o CBA uregulowane są zasady ochrony danych osobowych, z odwołaniem do obowiązującej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.). Przedstawiony projekt ustawy nie

² Zob. chociażby pismo z 28 marca 2018 r., VII.501.2015.314.AG. Szerzej na temat rozgraniczenia pojęć pod kątem stosowania dyrektywy 2016/680 i rozporządzenia ogólnego o ochronie danych osobowych zob. J. Kurek, Justyna Kurek *Zakres stosowania ogólnego rozporządzenia o ochronie danych osobowych i dyrektywy 2016/680/UE – wyzwania związane z wyodrębnieniem działań państwa w obszarze bezpieczeństwa narodowego i bezpieczeństwa publicznego*, „Europejski Przegląd Sądowy” 2016 nr 5, s. 43-48.

przewiduje zmian w ustawie o CBA. Tym samym, po pierwsze, należy zwrócić uwagę, że w ustawie o CBA pozostanie odesłanie do ustawy o ochronie danych osobowych z 1997 r., która za chwilę przestanie obowiązywać, a po drugie - za chwilę nie będzie żadnego aktu o charakterze ogólnym, określającego prawa osób, których dane są przetwarzane i zasady przetwarzania danych przez CBA. Trzeba bowiem pamiętać, że analogiczne wyłączenie dotyczące „bezpieczeństwa narodowego” istnieje na gruncie rozporządzenia ogólnego o ochronie danych³.

Tym samym, nie można zgodzić się z proponowaną treścią art. 1 ust. 2 pkt 7 projektu ustawy. Zaproponowany przepis pozostawi poza obowiązkiem stosowania przepisów o ochronie danych osobowych co najmniej 5 wymienionych w nim służb specjalnych. **Takie wyłączenie może oznaczać - przynajmniej w części - nie tylko sprzeczność z postanowieniami dyrektywy 2016/680, ale przede wszystkim z art. 51 Konstytucji RP.**

2. Prezes Urzędu Ochrony Danych Osobowych jako niezależny organ nadzorczy, wykonujący zadania wynikające z dyrektywy 2016/680

Z dużym zadowoleniem przyjąłem do wiadomości, że w projekcie ustawy o ochronie danych osobowych skierowanym do Sejmu (druk sejmowy nr 2410) uwzględniono moje uwagi, dotyczące niezależności przyszłego organu ochrony danych osobowych. Pozytywnie oceniam również decyzję, podjętą zgodnie z art. 41 ust. 3 dyrektywy 2016/680, wskazującą, że Prezes Urzędu Ochrony Danych Osobowych (dalej jako: PUODO) będzie organem nadzorczym zarówno na gruncie rozporządzenia ogólnego o ochronie danych, jak i dyrektywy 2016/680.

Jednocześnie zaniepokojenie budzą informacje o problemach związanych z budżetem przyszłego organu i brakiem przygotowania do stosowania nowych przepisów od maja 2018 roku⁴. Kwestie te powinny zostać rozstrzygnięte jak najszybciej, by możliwe było sprawne

³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (rozporządzenie ogólne o ochronie danych), Dz. Urz. L 119, 4.5.2016, s. 1.

⁴ Zob. m.in. przebieg dyskusji podczas posiedzenia sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii z dnia 13 kwietnia 2018 r., <http://www.sejm.gov.pl/Sejm8.nsf/biuletyn.xsp?sknr=CNT-89> (pobrano 22 kwietnia 2018 r.).

wykonywanie nowych obowiązków od początku obowiązywania przepisów ustawy o ochronie danych osobowych oraz ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości.

Dodatkowo, pragnę zwrócić uprzejmie uwagę na fakt, że w rozdziale 2 projektu, regulującym nadzór nad przetwarzaniem danych osobowych uwagę zwracają wyłączenia zawarte w art. 7. Nie jest jasne, dlaczego do prowadzenia kontroli nie mają mieć zastosowania wymienione przepisy rozdziału 9 ustawy o ochronie danych osobowych, a mianowicie art. 80 ust. 1 pkt 2 (wyłączenie kontrolującego, gdy zachodzą wątpliwości co do jego bezstronności), art. 85 ust. 4 (przekazanie potwierdzenia wezwania na piśmie przez PUODO oraz art. 86 (przesłuchanie pracownika kontrolowanego w charakterze świadka).

Zastrzeżenia budzi również wskazanie w art. 7 projektu ustawy, że kontrola przetwarzania danych osobowych może być przeprowadzana przez Prezesa Urzędu w celu wykonywania zadań określonych w art. 6 ust. 1 pkt 1 i 5-7. Tym samym wyłącza się bowiem możliwość przeprowadzenia kontroli w przypadku, gdy taka potrzeba wyniknie w wyniku rozpatrywania zażalenia, o którym mowa w art. 50 (zob. art. 6 ust. 1 pkt 4 projektu ustawy).

W mojej ocenie poza dopuszczalny zakres wynikający z dyrektywy 2016/680 wykracza też art. 9 ust. 3 projektu ustawy, zgodnie z którym decyzje Prezesa Urzędu nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Co prawda, administrator lub podmiot przetwarzający dane osobowe będzie zobowiązany do niezwłocznego przywrócenia zgodnego z prawem sposobu ich przetwarzania, jednak należy pamiętać o tym, że dane te mogą już być zebrane wbrew przepisom prawa. Nie ma zatem możliwości przywrócenia zgodnego z prawem ich przetwarzania, jeżeli znalazły się one już w posiadaniu administratora.

Warto w tym miejscu przypomnieć stanowisko Rzecznika Praw Obywatelskich w sprawie art. 168a kodeksu postępowania karnego - dopuszczania przed sądem dowodów zdobytych z naruszeniem przepisów⁵.

⁵ Co prawda, wniosek RPO w tej sprawie został wycofany z Trybunału Konstytucyjnego, jednak przyczyną były kwestie formalne, a nie merytoryczne. Aktualność argumentacji nie zmieniła się. Zob. stanowisko RPO <https://www.rpo.gov.pl/pl/content/rpo-wycofal-z-trybunalu-konstytucyjnego-wniosek-ws-%E2%80%9Eowocow-zatrutego-drzewa%E2%80%9D>

3. Nadzór nad sądami i prokuraturą

Projekt ustawy wyłącza nadzór Prezesa Urzędu Ochrony Danych Osobowych nad prokuraturą i sądami. W art. 1 ust. 1 pkt 3) projektu wskazano, że ustawa w ogóle nie będzie dotyczyć sposobu prowadzenia nadzoru nad sądami i prokuraturą, a następnie w art. 5 ust. 2 wyłącza się nadzór Prezesa Urzędu nad danymi przetwarzanymi w celach określonych w ustawie przez prokuraturę i sądy.

Przed wszystkim należy zauważyć, że istotnie - dyrektywa 2016/680 w art. 45 ust. 2 zobowiązuje państwa członkowskie do zapewnienia, by żaden organ nadzorczy nie był właściwy do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku sprawowania przez nie wymiaru sprawiedliwości. Jednocześnie jednak przepis ten umożliwia państwu (ale nie zobowiązuje) wyłączenie spod zakresu właściwości organu nadzorczego operacji nadzorowania dokonywanych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości. Jak wynika z motywu 80 preambuły do dyrektywy 2016/680, prawodawcy unijnemu chodzi w tym przypadku np. o prokuraturę. Wyłączenie zaproponowane w projekcie ustawy nasuwa kilka wątpliwości.

Po pierwsze, na gruncie prawa polskiego nie zawsze działania prokuratury wiążą się z niezależnością⁶. Można zatem mieć wątpliwości, czy na pewno prokuratury dotyczyć będzie art. 45 ust. 2 dyrektywy 2016/680. Po drugie zaś, w motywie 80 dyrektywy wyraźnie potwierdza się oczywistą tezę, iż zgodnie z art. 8 ust. 3 Karty Praw Podstawowych Unii Europejskiej (KPP UE) **przestrzeganie przepisów dyrektywy przez sądy i inne niezależne organy wymiaru sprawiedliwości zawsze podlega niezależnej kontroli zgodnie z art. 8 ust. 3 KPP UE**. Tymczasem w projekcie ustawy takiej niezależnej kontroli nie przewidziano. Należy zauważyć, że analogiczne wyłączenie w odniesieniu do sądów (już nie prokuratury) zawiera rozporządzenie ogólne o ochronie danych (art. 55 ust. 3). W związku z tym, w projekcie ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679⁷ słusznie przewidziano nowelizację

⁶ Por. art. 7 i zastrzeżenia w art. 8 i 9 ustawy z dnia 28 stycznia 2016 r. - Prawo o prokuraturze; Dz. U. 2017 poz. 1767 ze zm.

⁷ Ustawa o nr UC100 w wykazie prac legislacyjnych, wersja z 28 marca 2018 r.

ustawy z dnia 27 lipca 2001 r. - Prawo o ustroju sądów powszechnych (Dz. U. z 2018 r., poz. 23 ze zm.; por. dodawany art. 175dd) wskazując, kto sprawuje nadzór nad przetwarzaniem danych osobowych przez sądy na gruncie rozporządzenia ogólnego o ochronie danych. Wydaje się, że analogiczne przepisy - odnoszące się do zakresu stosowania dyrektywy 2016/680 - w związku z treścią art. 8 ust. 3 KPP UE muszą zostać zaproponowane również w omawianej ustawie, co najmniej w odniesieniu do prokuratury.

4. Definicja danych osobowych

Zgodnie z art. 3 ust. 1 projektu ustawy, za dane osobowe uważa się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, przetwarzane w celach, o których mowa w art. 1 ust. 1 pkt 1. Jak się wydaje, zamiarem projektodawcy w odniesieniu do dodania celu w definicji danych osobowych ma być odróżnienie tego pojęcia od pojęcia na gruncie rozporządzenia ogólnego o ochronie danych osobowych. Trzeba jednak zwrócić uwagę, że ta technika legislacyjna stosowana jest w dalszej części niekonsekwentnie, bo np. w art. 14 ust. 2 projektu ustawy powtarza się, że „dane osobowe mogą być przetwarzane wyłącznie w celach, o których mowa w art. 1 ust. 1 pkt 1”.

Pewne wątpliwości może budzić dodanie w art. 3 ust. 3 znanego z dzisiaj obowiązującej ustawy z 1997 r. o ochronie danych osobowych zastrzeżenia, określającego kiedy informacji nie uważa się za umożliwiającą określenia tożsamości osoby. Chociaż w samej części normatywnej dyrektywy 2016/680 takiego zastrzeżenia nie ma, tym niemniej może ono wynikać z motywu 21 preambuły dyrektywy. Trzeba jedynie pamiętać o tym, by przepis ten stosowany był spójnie z definicją danych osobowych na gruncie rozporządzenia ogólnego o ochronie danych⁸.

5. Zasady przetwarzania danych osobowych

W art. 17 projektu ustawy wskazano, że w przypadku, gdy przepisy nie określają terminu, to administrator dokonuje weryfikacji danych osobowych nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania i aktualizacji danych. Warto przy tym zwrócić uwagę,

⁸ Zob. też motyw 26 do rozporządzenia ogólnego o ochronie danych.

że w przepisach zmieniających zaproponowano takie zmiany, które wydłużają termin weryfikacji z obecnie obowiązujących 5 lat na 10 lat (wymienione dalej w części opinii, dotyczącej przepisów zmieniających). Tym samym, jak widać, zdaniem projektodawcy wystarczające jest, aby weryfikacja danych miała miejsce tylko co 10 lat, chociaż nie wiadomo, jakie przesłanki to uzasadniają. Co prawda art. 5 dyrektywy 2016/680 w tym względzie jest bardzo ogólnie sformułowany i pozwala na duży margines uznania państwa członkowskiego, jednak **propozycja 10 lat wymagałaby przedstawienia przekonującego wyjaśnienia chociażby w uzasadnieniu do projektu ustawy. Nie są bowiem znane przyczyny, dla których akurat 10, a nie 5 lat, jest okresem właściwym do weryfikacji danych.** Trzeba też przypomnieć, że Trybunał Sprawiedliwości UE oceniając zgodność przepisów prawa UE, czy też prawa krajowego, w zakresie zastosowania prawa UE z Kartą Praw Podstawowych UE nie akceptuje zasadniczo rozwiązań tego typu, które nie posiadają żadnego uzasadnienia⁹.

W art. 20 i 21 projektu ustawy proponuje się przepisy, które mają zapewne na celu wdrożenie art. 6 i 7 dyrektywy 2016/680. Trzeba jednak wyraźnie podkreślić, że samo nałożenie obowiązku na administratora dokonania rozróżnień, o których mowa w przepisach, bez powiązania go np. z okresem przechowywania danych, terminami weryfikacji danych, czy uprawnieniami podmiotu danych nie spełnia celu dyrektywy. W takim kształcie przepisy te nie będą realizowały bowiem żadnego praktycznego celu czy miały jakiegokolwiek zastosowania. Warto przy tym zwrócić uwagę na opinię Grupy roboczej art. 29, która w swoim stanowisku z 29 listopada 2017 r. również podniosła tę kwestię¹⁰.

Przy tej okazji warto zauważyć, że sformułowanie użyte w art. 20 projektu („Przy przetwarzaniu danych osobowych, o ile rozróżnienie to jest niemożliwe lub dalece utrudnione, administrator zapewnia podział...”) jest najprawdopodobniej błędne - zabrakło bowiem słowa „nie” (powinno być: „nie jest niemożliwe...”).

6. Prawa osoby, której dane dotyczą

⁹ Zob. wyrok TSUE w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland* (ECLI:EU:C:2014:238), w sprawie C-203/15 *Tele2 Sverige AB* (ECLI:EU:C:2016:970) czy też opinię 1/15 w sprawie zawarcia umowy UE z Kanadą dotyczącej przekazywania tzw. danych PNR (ECLI:EU:C:2016:656).

¹⁰ Article 29 Data Protection Working Part, WP 258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), adopted on 29 November 2017

W rozdziale 4 projektu ustawy proponuje się uregulowanie praw osób, której dane dotyczą. Obok przepisów, które zasadniczo oddają treść dyrektywy 2016/680, projektodawca dodaje również takie rozwiązania, które mogą wypaczyć sens i istotę tych postanowień.

Przykładowo, w art. 24 ust. 1 projektu ustawy znalazło się zastrzeżenie - w mojej ocenie zbędne - wskazujące, że prawo do uzyskania informacji od administratora o przetwarzaniu danych osobowych konkretnej osoby przysługuje „z zastrzeżeniem przepisów ustawy o ochronie informacji niejawnych”.

Za szczególnie zbędny i niezgodny z dyrektywą uważam art. 24 ust. 4 projektu ustawy, który uzależnia przekazanie informacji osobie, której dane dotyczą od niezbydności do ochrony jej żywotnych interesów lub innej osoby. Takiego dodatkowego wymogu, od którego uzależniona jest realizacja prawa do informacji dyrektywa 2016/680 również nie przewiduje. Dodatkowo, brzmienie art. 24 ust. 4 projektu ustawy wydaje się być sprzeczne z uzasadnieniem zawartym na s. 17, gdzie mowa jest o wprowadzeniu tego wymogu przy uzupełnieniu, aktualizacji, sprostowaniu lub usunięciu danych osobowych, a nie realizacji praw informacyjnych.

Ponadto, w art. 13 ust. 1 lit. d dyrektywy 2016/680 mowa jest o konieczności poinformowania osoby, której dane dotyczą, o prawie do wniesienia skargi do organu nadzorczego. Tymczasem w projekcie ustawy, w art. 24 ust. 5 pkt 2, mowa jest o pouczeniu dotyczącym wniesienia zażalenia, o którym mowa w art. 50. Zażalenie nie może jednak być tożsame ze skargą - zażalenie bowiem nie prowadzi do wszczęcia postępowania, o którym mowa w art. 7 projektu, a w szczególności nie kończy się decyzją PUODO i ewentualną skargą do sądu administracyjnego (art. 9 i 10 projektu). Tym samym, **nie jest zrealizowane w ogóle w projekcie ustawy prawo do wniesienia skutecznej skargi na działania administratora.** Prawo przyznane w projekcie ustawy wydaje się być wyłącznie iluzoryczne.

W art. 25 ust. 1 pkt 8 projektu ustawy mowa jest o kategoriach odbiorców danych, podczas gdy w dyrektywie 2016/680 wskazuje się wyraźnie na „odbiorców i kategorie odbiorców danych” (art. 14 lit. c dyrektywy 2016/680).

W art. 26 ust. 1 pkt 2 projektu ustawy przewidziano możliwość żądania usunięcia danych osobowych z jawnych zbiorów danych osobowych - również ta kwestia wymaga wyjaśnienia, bowiem dyrektywa 2016/680 takiego ograniczenia tylko do zbiorów jawnych nie przewiduje.

W projekcie ustawy w art. 25 ust. 1 projektu ustawy w ogóle nie przewidziano realizacji art. 14 lit g dyrektywy 2016/680 - **nie zagwarantowano tym samym w ogóle istoty prawa dostępu, czyli informacji o tym, jakie dane osobowe są przetwarzane i wszelkich dostępnych informacji o ich pochodzeniu.**

W art. 28 ust. 1 projektu ustawy, projektodawca odwołuje się m.in. do wniosku, o którym mowa w art. 24 ust. 3 projektu ustawy, jednak w art. 24 ust. 3 projektu ustawy nie ma mowy o żadnym wniosku. Wydaje się, że chodziło o art. 24 ust. 1 projektu ustawy. Przepis ten wymaga również dalszej dyskusji, bowiem w obecnym kształcie wyłącza kompetencje Prezesa Urzędu do weryfikacji zasadności zastosowania przez administratora przesłanek, o których mowa w art. 28 ust. 1 pkt 2 projektu ustawy w odniesieniu do informacji niejawnych. Takie wyłączenie nie jest przewidziane na gruncie przepisów dyrektywy 2016/680.

Wreszcie, przepisy projektu ustawy w ogóle nie odnoszą się do wymogu nałożonego przez dyrektywę 2016/680, by komunikacja z osobą, której dane dotyczą, odbywała się w zwięzłej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka, z wykorzystaniem wszelkich stosownych sposobów, w tym elektronicznych. Dyrektywa jasno wskazuje też, że administrator ma obowiązek udzielić informacji w takiej samej formie, w jakiej wniesiono żądanie (por. art. 12 ust. 1 dyrektywy 2016/680). Wymogi te są analogiczne do tych, jakie na podmioty prywatne nakłada rozporządzenie ogólne, a zatem wymagania te powinny znaleźć swoje odzwierciedlenie w omawianej ustawie.

7. Środki ochrony prawnej i odpowiedzialność prawna

Zgodnie z art. 52 dyrektywy 2016/680, jednym z podstawowych środków ochrony prawnej jest **możliwość wniesienia skargi do organu nadzorczego w sytuacji, gdy osoba, której dane dotyczą sądzi, że przetwarzanie narusza przepisy przyjęte na podstawie dyrektywy.** Analizując projekt ustawy można mieć zasadnicze wątpliwości, czy

prawo to zostało w projekcie zrealizowane. Trzeba bowiem zauważyć, że żaden z przepisów w rozdziale 2 projektu ustawy nie wskazuje wprost na możliwość wniesienia skargi (w art. 9 mowa jest tylko, że PUODO działa z urzędu lub na wniosek osoby zainteresowanej). W szczególności jednak, w rozdziale 7 projektu ustawy nie przewidziano żadnej regulacji dotyczącej procedury wniesienia skargi. Można oczywiście argumentować, że prawo do wniesienia skargi wynika z ogólnych przepisów kodeksu postępowania administracyjnego (kpa), jednak ze względów pewności prawnej bez wątpienia wskazanie o przysługującej skardze powinno znaleźć się w ustawie.

Za taką skargę nie można bowiem uznać zażalenia, o którym mowa w art. 50 ustawy. Zażalenie wnosi się, zgodnie z art. 141 kpa, na wydane w toku postępowania postanowienie, gdy kodeks tak stanowi, w terminie siedmiu dni od dnia doręczenia postanowienia stronie, a gdy postanowienie zostało ogłoszone ustnie - od dnia jego ogłoszenia stronie. Można mieć wątpliwości czy wprowadzając w art. 50 projektu ustawy instytucję zażalenia, projektodawca miał na myśli zażalenie, o którym mowa w kpa. Jeśli tak, to bez wątpienia nie jest to realizacja prawa do skargi o którym mowa w dyrektywie.

Z kolei w art. 52 projektu ustawy mowa jest o prawie do wniesienia skargi do sądu administracyjnego na decyzje PUODO, co oznacza, że do PUODO można wnieść skargę. Jeżeli zatem prawo do skargi miałyby wynikać z art. 9 ust. 1 projektu ustawy, to należy zaznaczyć, że postępowanie przed PUODO powinno zostać uregulowane analogicznie do tego, które będzie miało miejsce w związku z rozporządzeniem ogólnym o ochronie danych. Należy rozważyć chociażby konieczność odejścia od dwuinstancyjności postępowania administracyjnego tak, jak ma to miejsce na gruncie projektu ustawy o ochronie danych osobowych (druk nr 2410).

Niejasny również, zwłaszcza w kontekście art. 9 i 10 projektu ustawy, jest proponowany art. 51 ustawy. Jak się wydaje, wprowadza on swoistą dwuinstancyjność postępowania w odniesieniu do tych spraw, których dotyczy art. 24 projektu ustawy. Ustawodawca przewidział wyłącznie opiniowanie takiego wniosku o ponowne rozpatrzenie sprawy przez Prezesa Urzędu, natomiast nie wprowadza żadnego rozstrzygnięcia o charakterze władczym.

W projekcie ustawy **zabrakło również wdrożenia art. 54 dyrektywy 2016/680**, a zatem możliwości wniesienia sprawy do sądu, niezależnie od postępowania

administracyjnego i sądownoadministracyjnego. Taka możliwość - analogicznie - została przewidziana w ustawie o ochronie danych osobowych w odniesieniu do rozporządzenia ogólnego o ochronie danych osobowych.

8. Przepisy zmieniające

Zastrzeżenia Rzecznika Praw Obywatelskich muszą budzić te wszystkie zmiany w ustawach, które przewidują przyznanie prawa do pozyskiwania informacji przez służby, bez konieczności składania wniosku o dostęp, za pomocą urządzeń telekomunikacyjnych. Stanowisko w tej sprawie przedstawiałem już wielokrotnie, pragnę zatem jedynie przypomnieć, że zbyt duża i niekontrolowana możliwość sięgania po dane obywateli narusza ich prawo do prywatności i zaufanie do państwa. We wniosku do Trybunału Konstytucyjnego w sprawie tzw. ustawy inwigilacyjnej wskazałem na zagrożenia dla prywatności obywateli, ale także na wymagania związane chociażby z koniecznością odnotowywania (w systemie informatycznym), kto i kiedy sięgał i w jakim celu po dane. Umożliwienie służbom swobodnego dostępu do danych obywateli, wymaga zawsze silnych argumentów, pozwalających na stwierdzenie, że ochrona prywatności może ulec uszczupleniu na rzecz realizacji innych celów. Kluczowy wymóg dopuszczalności wprowadzenia ograniczenia prawa do prywatności i dopuszczalności zbierania danych o obywatelach przez władze państwowe, zarówno w odniesieniu do art. 47, jak i 51 ust. 2 Konstytucji RP, a także art. 8 Europejskiej Konwencji Praw Człowieka (EKPCz) oraz art. 7 w związku z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej odwołuje się do pojęcia „niezbędność”. Wiąże się to z dążeniem do ograniczenia pozyskiwania przez władzę publiczną „niekoniecznych, lecz wygodnych” informacji o jednostce. Ani zatem względy celowości ani „wygody” organów władzy publicznej nie mogą *per se* uzasadnić naruszenia autonomii informacyjnej jednostki (wyrok Trybunału Konstytucyjnego z 20 listopada 2002 r. w sprawie o sygn. akt K 41/02)

Za zbyt ogólne należy uznać również te przepisy, które przewidują uprawnienia służb do przetwarzania danych osobowych „przez okres niezbędny do wykonywania ustawowych zadań” w związku z jednoczesnym wydłużeniem okresu weryfikacji danych do 10 lat (por. przykładowo zmieniany art. 10a ust. 14 ustawy o Straży Granicznej,

art. 11t ust. 7b ustawy o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, dodawany art. 10a ust. 6 ustawy o strażach gminnych, art. 29 ust. 10 ustawy o Żandarmerii Wojskowej), albo usunięciem przepisu o konieczności weryfikacji po zakończeniu sprawy, w ramach której dane były przetwarzane (por. dodawany art. 20 ust. 1k ustawy o Policji z obecnie obowiązującym art. 20 ust. 17 ustawy o Policji albo zmieniany art. 4 ust. 4 ustawy o Straży Marszałkowskiej).

Należy także podkreślić, że **niejasne i budzące poważne zastrzeżenia są te wszystkie przepisy zmieniające, które wyłączają stosowanie art. 12-22 oraz art. 34 rozporządzenia ogólnego w sytuacji, gdy dane przetwarzane są przez służby w celu innym niż wynikający z dyrektywy 2016/680** (zob. przykładowo zmieniany art. 10a ust. 16 ustawy o Straży Granicznej, art. 11t ust. 9 ustawy o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, art. 29 ust. 12 ustawy o Żandarmerii Wojskowej, art. 11 ust. 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym czy też art. 35 ust. 5 ustawy o Krajowej Administracji Skarbowej, a wreszcie art. 4 ust. 2b oraz art. 19a ust. 2 ustawy o Straży Marszałkowskiej).

Pragnę podkreślić, że propozycja wprowadzenia podobnych wyłączeń dotyczących małych przedsiębiorców w projekcie ustawy o ochronie danych osobowych w jej poprzednich wersjach wzbudziła poważne kontrowersje, które doprowadziły do rezygnacji (na obecnym etapie) z takiej propozycji. **Ani projekt opiniowanej ustawy ani najnowsza wersja uzasadnienia do projektu ustawy nie wyjaśnia zasadności przyjmowania proponowanych ograniczeń.** Tym samym nie jest jasne, czy cel i zakres wprowadzonych ograniczeń będą mogły być uznane za „niezbędne w demokratycznym państwie prawnym” i czy takie ograniczenie prawa do prywatności będzie mogło być uznane za zgodne z art. 47 i art. 51 w związku z art. 31 ust. 3 Konstytucji RP. Naruszenia konstytucyjnego prawa do ochrony danych osobowych można upatrywać również w ograniczeniu praw przysługujących jednostce, w ramach wykraczających poza dopuszczalny zakres. **Wprowadzenie rozwiązań wyłączających stosowanie art. 12-20 i art. 34 wymagałoby zatem nie tylko szczegółowej oceny pod kątem realizacji gwarancji wymaganych przez rozporządzenie ogólne o ochronie danych osobowych, ale także pod kątem realizacji przesłanek wskazanych w powołanych wyżej przepisach Konstytucji RP.** Pragnę przy

tym dodać, że również w opinii Grupy roboczej art. 29 wyraźnie podkreśla się, że dyrektywa nie zezwala na blankietowe ograniczenie praw jednostki¹¹.

9. Uwagi końcowe

Na koniec pragnę podkreślić, że do projektu ustawy nie dołączono tabeli zbieżności, która ułatwiłaby ocenę, czy w istocie dyrektywa 2016/680 jest prawidłowo wdrożona do polskiego porządku prawnego. Należy bowiem pamiętać, że część jej przepisów znajduje swoje odzwierciedlenie w przepisach projektu ustawy o ochronie danych osobowych (np. dotyczące zadań Prezesa Urzędu). Z punktu widzenia przejrzystości i pewności prawa, dokładne wskazanie przez projektodawcę sposobu wdrożenia poszczególnych przepisów w tabeli zbieżności, ale także w prawidłowo opracowanym uzasadnieniu, w którym wyjaśnione zostałyby faktyczne przesłanki niektórych rozwiązań, a nie jedynie ponownie przytoczone przepisy, przyczyniłoby się do lepszego zrozumienia przez obywateli tego skomplikowanego stanu prawnego, jaki będzie miał miejsce po wejściu w życie ustawy o ochronie danych osobowych, ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, a także rozpoczęciem stosowania rozporządzenia ogólnego o ochronie danych osobowych.

Również uzasadnienie nie spełnia podstawowego wymogu, jakim jest wyjaśnienie przyczyn stojących z konkretnymi rozwiązaniami. W większości przypadków projektodawca ograniczył się do skrótowego przywołania po raz kolejny treści przepisów, nie przedstawiając żadnej dodatkowej argumentacji.

Podsumowując pragnę stwierdzić, że **z punktu widzenia ochrony praw jednostki przedstawiony projekt nie może zostać oceniony całkowicie pozytywnie**. Wiele z uwag, które można byłoby zgłosić związanych jest z niedoskonałością samej dyrektywy 2016/680. W tej kwestii ocena pozostawiona jest jednak Trybunałowi Sprawiedliwości UE, który z pewnością w przyszłości będzie miał niejedną okazję do wypowiedzi orzeczniczej na ten temat. Jednak szereg uwag dotyczy również przyjętych w projekcie ustawy rozwiązań. **Szczególnej rozwagi wymagają te moje uwagi, które dotyczą systemu środków**

¹¹ Zob. przywoływany wcześniej dokument, WP 258, s. 24.

ochrony prawnej, czy też praw osoby, której dane dotyczą. Wprowadzanie ograniczeń albo blankietowych wyłączeń od reguł ogólnych, wyłączanie określonych służb z reżimu przepisów o ochronie danych osobowych, czy też rozszerzanie uprawnień innych służb stoi w sprzeczności z podstawowym celem dyrektywy, jakim jest ochrona praw podstawowych i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, o którym mowa w art. 16 TFUE i w art. 8 KPP UE.

Niniejsze uwagi Rzecznik Praw Obywatelskich przedstawia Panu Ministrowi i poddaje je pod rozwagę. Będę wdzięczny za poinformowanie Rzecznika o sposobie ich wykorzystania w pracach legislacyjnych.

Z poważaniem

Stanisław Trociuk

Do wiadomości:

- 1) **Pan Marek Zagórski**
Minister Cyfryzacji

- 2) **Pani Edyta Bielak-Jomaa**
Generalny Inspektor Ochrony Danych Osobowych