Do druku nr 3318

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

Warszawa, dnia 14-06-2023

DOL.401.268.2023.WL.NP

SEKRETARIAT Z-CY SZEFA KS
L.dz. DS.175.344.2023
Data wpływu 16.06.2023

Sz. P.
Agnieszka Kaczmarska
Szef Kancelarii Sejmu
ul. Wiejska 4/6/8
00-489 Warszawa

Szanowna Pani,

w odpowiedzi na pismo z 5 czerwca br., znak: SPS-WP.020.156.3.2023, uprzejmie informuję, że Prezes Urzędu Ochrony Danych Osobowych – z punktu widzenia przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) (ogólne rozporządzenie o ochronie danych), dalej: rozporządzenie 2016/679 – w odniesieniu do **prezydenckiego projektu ustawy o zmianie ustawy o Państwowej Komisji do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007-2022 oraz niektórych innych ustaw (druk nr 3318)** wskazuje na poniższe.

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-WP.020.156.3.2023
Data wpływu 18.06.2023

1. Uwagi o charakterze ogólnym

Zgodnie z przedstawionym uzasadnieniem do projektu, celem ustawy jest wprowadzenie zmian m.in. w ustawie o Państwowej Komisji do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007-2022 (dalej: ustawa), zmierzających do zniesienia możliwości stosowania przez Komisję do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007–2022, środków zaradczych, o których mowa w art. 37 ust. 1 ustawy, zmiany trybu odwoławczego od decyzji Komisji z sądów administracyjnych na sądy powszechne, wykluczenia możliwości pełnienia funkcji członka Komisji przez posła lub senatora, zwiększenia niezależności Komisji i transparentności postępowań przed nią oraz ujednolicenia w ramach systemu prawnego ochrony tajemnic zawodowych.

Dla realizacji tak istotnego celu niezbędne będzie przetwarzanie danych osobowych, dlatego też wprowadzane normy prawne stanowiące o ich pozyskiwaniu, udostępnianiu i dalszym wykorzystywaniu, powinny przejść **test zgodności z europejskimi przepisami o ochronie danych osobowych**. Uzasadnionym byłoby zatem dokonanie **oceny skutków** dla ochrony danych osobowych, o której mowa w art. 35 rozporządzenia 2016/679[1], w której Projektodawca (ustawodawca) wykazałby konieczność lub brak niezbędności wprowadzenia określonych rozwiązań tak, by tworzyć regulacje prawne z poszanowaniem ogólnego rozporządzenia 2016/679. **Na powyższe kwestie wskazywał organ w toku opiniowania poselskiego projektu ustawy o Państwowej Komisji do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007-2022** (pismo z 13 grudnia 2022 r. znak: DOL.401.593.2022.WL.NP).

Komisja Państwowa będąca organem administracji publicznej powinna być wyposażona przy realizacji swoich zadań w instrumenty jasno określone w przepisach prawa, odpowiadające stosowaniu przepisów rozporządzenia 2016/679, w tym w kontekście jego art. 24[2] i art. 25. Za określeniem chociażby minimalnych standardów bezpieczeństwa przetwarzania danych w przypadku podmiotów administracji publicznej przemawia charakter realizowanych przez te podmioty zadań publicznych i spoczywająca na nich z tego tytułu odpowiedzialność. Dlatego to Projektodawca, a następnie ustawodawca, wdrażając właściwe przepisy prawa, powinien zadbać o wskazanie co najmniej kryteriów wymaganych dla zapewnienia odpowiednich gwarancji dla praw i wolności osób, których dane osobowe będą przetwarzane w ramach przeprowadzanych działań Komisji, co pozwoli zapewnić należytą ochronę danych osobowych dla realizacji celów wskazanych w przepisach.

Projektodawca zdecydował się uregulować w ustawie kwestie dotyczące ochrony tajemnic prawnie chronionych w przepisach zmienianej ustawy (**zmiana 7, dodanie art. 29a**), co ocenić należy pozytywnie. Niemniej jednak w ustawie brakuje nadal regulacji – na które wskazywał organ w ww. piśmie opiniując projekt ustawy - dotyczących ustalenia okresu retencji danych. Biorąc pod uwagę, że w toku prac Komisji przetwarzane mogą być także dane osób, które nie działały na szkodę interesów Rzeczypospolitej Polskiej, a także osób, które ostatecznie okażą się niewinne, istotne jest ustalenie okresu retencji danych, który uzależniony jest od celu dla jakiego dane osobowe zostały zebrane i mają być przetwarzane. Zaznaczyć należy, że dane osobowe po zakończeniu przetwarzania powinny zostać usunięte, zanonimizowane lub też przekazane podmiotowi uprawnionemu ustawowo do ich przejęcia od administratora. Projektowane rozwiązania powinny to uwzględniać przez wskazanie okresu przechowywania danych oraz wskazania sposobu postępowania po wyznaczonym okresie (art. 5 ust. 1 lit. e

---

[1] Zgodnie z art. 35 ust. 1 rozporządzenia 2016/679 ocena taka jest niezbędna, gdy projektowane procesy przetwarzania danych - w szczególności następujące z użyciem nowych technologii - ze względu na rodzaj przetwarzania, jego charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

[2] Art. 24 ust. 1 rozporządzenia 2016/679: uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;

rozporządzenia 2016/679). Dlatego też warto, aby Projektodawca rozważył wprowadzenie stosownych zmian.

2. Uwagi szczegółowe

Wątpliwości budzi też projektowana **zmiana 5**, która dotyczy **art. 12 ust. 7 ustawy**. Zgodnie z obecną regulacją: Prezes Rady Ministrów określa, w drodze zarządzenia, regulamin działania Komisji. Projektodawca proponuje jednak nowe rozwiązanie, tj.: Komisja, w drodze uchwały, określa regulamin swojego działania (...). Takie regulacje, **jeżeli będą dotyczyły przetwarzania danych osobowych**, powinny jednak być wprowadzane **mocą przepisów ustawowych**, a nie wewnętrznego regulaminu określonego w drodze uchwały, tak aby zagwarantować ochronę podstawowych praw, w tym prawa do ochrony danych osobowych oraz zgodność ze standardami określonymi w rozporządzeniu 2016/679. To przepisy ustawy powinny wskazywać jak następować ma przetwarzanie danych w związku z pracami Komisji. Wymaga tego wzgląd na zasady legalizmu i zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679). Nie może bowiem dochodzić do mającego wpływ na prawa i obowiązki oraz odpowiedzialność z zakresu przetwarzania danych osobowych kształtowania zakresu działań Komisji (celów ustawowych) wewnętrznym regulaminem, o ile brak w tym zakresie regulacji rangi ustawy. Ma to istotne znaczenie dla prawidłowego stosowania przepisów rozporządzenia 20176/679, w tym ww. zasad dotyczących przetwarzania danych osobowych[3], w szczególności zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679).

Zmiana 9 nadaje nowe brzmienie **art. 33 ustawy**, tj.: Posiedzenia Komisji wyznaczone poza rozprawą są jawne, chyba że przewodniczący Komisji zarządzi inaczej (...). Biorąc pod uwagę art. 23 ust. 1 ustawy, który stanowi, że Przewodniczący Komisji zezwala przedstawicielom środków masowego przekazu na dokonywanie za pomocą aparatury utrwaleń obrazu i dźwięku z przebiegu rozprawy oraz transmisję audiowizualną za pośrednictwem sieci Internet – ustawa powinna regulować również kwestie dotyczące bezpieczeństwa przetwarzanych danych w związku z wykorzystaniem ww. systemów. Przyjęcie takiego sposobu organizacji posiedzeń Komisji jest potencjalnie narażone na cyberzagrożenia, wiąże się z ryzykiem niekontrolowanego dostępu do danych, czy też niezgodnego z prawem ich przetwarzania. Projektodawca powinien zwrócić również uwagę na aspekt kategorii/rodzaju danych, jakie podczas posiedzeń Komisji mogą być przetwarzane (głos, wizerunek, dane osobowe szczególnych kategorii, dla których art. 9

---

[3] Zgodnie z art. 5 rozporządzenia 2016/679 zdane osobowe muszą być przetwarzane: zgodnie z prawem, rzetelnie i w sposób przejrzysty – zasada zgodności z prawem, rzetelności i przejrzystości (ust. 1 lit. a); zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami – zasada ograniczeni celu (ust. 1 lit. b); adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – zasada minimalizacji danych (ust. 1 li.t c); prawidłowe i w razie potrzeby uaktualniane – zasada prawidłowości (ust. 1 lit. d); przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane – zasada ograniczenia przechowywania (ust. 1 lit. e); przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych – zasada integralności i poufności (ust. 1 lit. f). Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie – zasada rozliczalności (art. 5 ust. 2).

rozporządzenia 2016/679 przewiduje szczególny reżim przetwarzania). Przy aktualnym brzmieniu przepisu wszystkie dane osobowe, włącznie z danymi szczególnych kategorii i danymi z art. 10 rozporządzenia 2016/679 podlegałyby upublicznieniu, co niewątpliwie w sposób nadmiarowy ingerowałoby w sferę prywatności podmiotów danych.

Należy zwrócić uwagę, że Europejska Rada Ochrony Danych przyjęła 10 lipca 2019 r. *Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo*, które mają na celu wyjaśnienie, w jaki sposób rozporządzenie 2016/679 ma zastosowanie do przetwarzania danych osobowych w przypadku korzystania z urządzeń wideo oraz zapewnienie spójnego stosowania ogólnego rozporządzenia o ochronie danych w tym zakresie. Wskazują one m.in., że dokonując wyboru rozwiązań technicznych administrator powinien brać pod uwagę technologie przyjazne prywatności, które zwiększają bezpieczeństwo. Ponadto podkreślają, że przyjmowane rozwiązania mają ogromny wpływ na procesy związane z ochroną danych osobowych, zatem należy przyjmować rozwiązania zapobiegające nadużyciom oraz, że w każdym przypadku należy analizować wprowadzane rozwiązania pod kątem ich zgodności z zasadami określonymi w art. 5 rozporządzenia 2016/679.

W świetle powyższego, zasadnym wydaje się doprecyzowanie projektu o normy prawne, które będą sprzyjały bezpieczeństwu przetwarzanych danych, tak aby zachować ich integralność i poufność.

Wskazówki organu nadzorczego w niniejszej sprawie mają wyłącznie charakter ekspercki dla Projektodawcy (ustawodawcy), który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych.

Z wyrazami szacunku
Prezes Urzędu Ochrony Danych Osobowych
Jan Nowak
/-podpisano elektronicznie-/