Do druku nr 2267

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

DOL.401.246.2022.WL.MW

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu RP
ul. Wiejska 4/6/8
00-902 Warszawa
ePUAP: /KSRP/SkrytkaESP

Szanowny Panie Ministrze,

w związku z korespondencją z dnia 17 maja 2022 r. (znak: SPS-WP.020.144.5.2022) przekazującą do zaopiniowania poselski projekt ***ustawy o zmianie ustawy o pomocy państwa w spłacie niektórych kredytów mieszkaniowych, udzielaniu premii gwarancyjnych oraz refundacji bankom wypłaconych premii gwarancyjnych*** (nr druku: 2267), dalej: projekt (przedstawiciel wnioskodawców: poseł Paulina Henning-Kloska), organ nadzorczy z punktu widzenia przepisów *rozporządzenia 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 (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[1)]) zwraca uwagę na następujące kwestie.

Wątpliwości budzi **art. 1 projektu ustawy**, który w ustawie z dnia 30 listopada 1995 r. *o pomocy państwa w spłacie niektórych kredytów mieszkaniowych, udzielaniu premii gwarancyjnych oraz refundacji bankom wypłaconych premii gwarancyjnych* (Dz. U. z 2021 r. poz. 1286, 1981 i 2270) po art. 12a **dodaje art. 12b-12d**. W projektowanym **art. 12b ust. 3** projektodawca wskazuje, że *„Kredytobiorca składa wniosek o zawieszenie spłaty kredytu na trwałym nośniku, odpowiednio w rozumieniu art. 5 pkt 17 ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim albo art. 4 pkt 22 ustawy z dnia 23 marca 2017 r. o kredycie hipotecznym oraz o nadzorze nad pośrednikami kredytu hipotecznego i agentami”*. Zauważyć należy, że definicja

[1)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35.

„trwałego nośnika" w rozumieniu art. 5 pkt 17 ustawy z dnia 12 maja 2011 r. *o kredycie konsumenckim* albo art. 4 pkt 22 ustawy z dnia 23 marca 2017 r. *o kredycie hipotecznym oraz o nadzorze nad pośrednikami kredytu hipotecznego i agentami* dotyczy informacji przekazywanych konsumentowi a nie przez konsumenta (kredytobiorcę), jak to zostało wskazane w projektowanym art. 12b ust. 3. Natomiast w ust. 7 tego przepisu jest mowa o kredytodawcy, który potwierdza na trwałym nośniku otrzymanie wniosku. Uzasadnionym byłoby zatem, aby na potrzeby projektowanego rozwiązania narzędzie, jakim jest „trwały nośnik" (służące także przetwarzaniu informacji będących danymi osobowymi) zostało wyczerpująco zdefiniowane, ponieważ odwołania do przedmiotowych ustaw nie są adekwatne w tym projekcie. W uzasadnieniu do projektu zostało wskazane, że realizacja uprawnienia następuje na wniosek kredytobiorcy złożony na trwałym nośniku oraz przykładowo - np. pisemnie, mailowo czy przez bankowość elektroniczną, jeżeli taką funkcjonalność posiada. W projekcie konieczne jest dookreślenie jakie narzędzia/urządzenia są zaliczane do trwałych nośników.

Istotną kwestią jest zagadnienie związane z zabezpieczeniem nośników, które zawierają dane o charakterze osobowym, wdrożeniem odpowiednich środków technicznych i organizacyjnych oraz retencją danych. Dokumentacja zawierająca dane o charakterze osobowym może być przechowywana w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (ograniczenie przechowywania - art. 5 ust. 1 lit. e rozporządzenia 2016/679). Projektodawca powinien uzupełnić ww. przepis w taki sposób, aby zachować zgodność z przepisami rozporządzenia 2016/679 w zakresie zasad dotyczących przetwarzania danych osobowych z art. 5[1].

Brak stosowania zabezpieczeń odpowiednich do ryzyk związanych z projektowanymi sposobami przetwarzania danych osobowych jest potencjalnym narażeniem na cyberzagrożenia

---

[1] Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"); b)zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"); e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania"); f) 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 („integralność i poufność"). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

i wiąże się z ryzykiem niekontrolowanego dostępu do danych osobowych, a w konsekwencji niezgodnego z prawem ich przetwarzania. Przetwarzanie danych osobowych powinno odbywać się z zachowaniem zasady integralności i poufności w sposób zapewniający bezpieczeństwo tych danych na odpowiednim poziomie, na zasadach ściśle określonych przepisami ustawy albo z uwzględnieniem wskazanych w przepisach ustawy minimalnych kryteriów zabezpieczających stosowanie wymogów rozporządzenia 2016/679[1].

Art. 12b ust. 4 - poprzez użycie zwrotu „w szczególności" przy wyliczeniu - zawiera otwarty katalog informacji, w tym danych osobowych kredytobiorcy. Zakres pozyskiwanych i przetwarzanych danych powinien wprost wynikać z przepisów tej ustawy. Przepis powinien czynić zadość zasadzie minimalizacji (art. 5 ust. 1 lit. c rozporządzenia 2016/679) powinny być przetwarzane jedynie dookreślone dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Konieczne jest także uwzględnienie zasady zgodności z prawem (art. 5 ust. 1 lit. a) oraz ograniczenia celu przetwarzania danych zebranych i przetwarzanych na potrzeby pierwotnych celów (art. 5 ust. 1 lit. b).

Przedmiotowe kwestie powinny być szczegółowo określone w przepisach ustawy tak, aby uwzględnione zostały regulacje dotyczące przetwarzania danych wynikające z ogólnego rozporządzenia o ochronie danych osobowych, a wykonawcy przepisów otrzymali jasne i wyczerpujące regulacje determinujące ich działania podejmowane dla realizacji celów ustawy.

Uwagi organu nadzorczego, przedstawiane w toku prac legislacyjnych, mają charakter eksperckich wskazówek dla Projektodawcy, który podczas formułowania przepisów prawa powinien zadbać o stosowanie przepisów rozporządzeniem 2016/679. To Projektodawca ponosi odpowiedzialność za konstrukcję przepisów, które powinny być proporcjonalne do zakładanych celów regulacji i zgodne z zasadami wynikającymi z art. 5 ogólnego rozporządzenia o ochronie danych.

Z wyrazami szacunku,

Prezes Urzędu
Ochrony Danych Osobowych
Jan Nowak

/- dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

[1] Wskazać należy na art. 24 rozporządzenia 2016/679, który w ust. 1 stanowi, że: „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, 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" oraz na art. 32 rozporządzenia 2016/679 dotyczący bezpieczeństwa przetwarzania danych osobowych.