Warszawa, 1 marca 2022 r.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

DOL.401.6.2021.WL.MW

Pan
Andrzej Kosztowniak
Przewodniczący Komisji
Komisja Finansów Publicznych
Kancelaria Sejmu RP
ul. Wiejska 4/6/8
00-902 Warszawa

Szanowny Panie Przewodniczący,

w odpowiedzi na zawiadomienie z dnia 24 lutego 2022 r. (znak: FPB.016.272.2022) w sprawie posiedzenia Komisji Finansów Publicznych w dniu 2 marca br. w przedmiocie rozpatrzenia rządowego ***projektu ustawy o zmianie ustawy o listach zastawnych i bankach hipotecznych oraz niektórych innych ustaw*** (druk nr 2019), uprzejmie informuję, że pozostają aktualne dotychczasowe uwagi organu nadzorczego wniesione do projektu ustawy (przedstawione w pismach z dnia 26 stycznia 2021 r., 24 maja 2021 r. oraz 6 września 2021 r., znak: DOL.401.6.2021), które nie zostały uwzględnione w dotychczasowym procesie legislacyjnym.

Projektowane przepisy (m.in. **art. 1 pkt 5, art. 1 pkt 8 projektu ustawy**) zawierające otwarte katalogi informacji budzą wątpliwości, gdyż nie precyzują, czy informacje w nich zawarte zawierają dane o charakterze osobowym. Przedmiotowe przepisy należałoby doprecyzować poprzez przyjęcie zamkniętego katalogu informacji (katalogu przetwarzanych danych osobowych) zamiast używania zwrotów „w szczególności" czy „co najmniej".

Ponadto, przekazany ***projekt ustawy o zmianie ustawy o listach zastawnych i bankach hipotecznych oraz niektórych innych ustaw*** znacząco różni się od projektu, który był

przedłożony na wcześniejszych etapach prac legislacyjnych (zostały dodane nowe przepisy, które dotychczas nie były przedmiotem opinii organu nadzorczego).

W związku z powyższym - 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)*, zwanego dalej rozporządzeniem 2016/679 – nadal w projektowanych przepisach brakuje przeprowadzenia testu prywatności – art. 25 ust. 1[1] oraz oceny skutków dla ochrony danych - art. 35 ust. 1[2] rozporządzenia 2016/679. Brak zastosowania tych instrumentów powoduje, iż projektodawca nie wykazał konieczności wprowadzenia rozwiązań proponowanych niniejszym projektem a związanych z przetwarzaniem danych. Korzyści wynikające z zastosowania tych instrumentów zostały szeroko opisane projektodawcy w dotychczas prowadzonej korespondencji. Natomiast odnosząc się do konkretnych przepisów wskazać należy na:

1. **Art. 7c ust. 2** ***ustawy z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych*** (Dz. U. z 2020 r. poz. 415 oraz z 2021 r. poz. 2140), w którym wskazano, że *Komisja Nadzoru Finansowego oraz kurator mogą dokonywać wzajemnej wymiany informacji dotyczących programu emisji listów zastawnych w zakresie, w jakim jest to niezbędne do prowadzenia postępowania upadłościowego* - projektowany przepis nie precyzuje celu, zakresu oraz trybu (bezwnioskowy/ na wniosek), w którym wymiana informacji miałaby się odbywać (w szczególności, jeśli przekazywane miałyby być dane o charakterze osobowym). Zgodnie z motywem 31rozporządzenia 2016/679[3] ujawnianie

[1] Zgodnie z art. 25 ust. 1 rozporządzenia 2016/679 „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą”.

[2] Zgodnie z art. 35 ust. 1 rozporządzenia 2016/679 „Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę”.

[3] Motyw 31 rozporządzenia 2016/679 stanowi, że „Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych.

danych podmiotom publicznym powinno mieć co do zasady charakter wnioskowy (odbywać się w formie pisemnej, być uzasadnione i mieć charakter wyjątkowy);

2. **Art. 33b** ww. ustawy, w którym wskazuje się na *„wykaz banków hipotecznych”* - brak doprecyzowania jakie informacje/dane dotyczące banków przedmiotowy wykaz będzie zawierał, co wymaga uzupełnienia.
3. Budzący szereg wątpliwości jest **art. 5** projektu ustawy wprowadzający zmiany ***w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2021 r. poz. 2439 i 2447)***, które nie były przedmiotem wcześniejszej wersji projektu ustawy.
   a) W **art. 105 ust. 1 Prawa bankowego dodaje się pkt 4**, a tym samym rozszerza się zakres podmiotowy, któremu bank ma obowiązek udzielenia informacji stanowiących tajemnicę bankową. Zgodnie z proponowaną zmianą przepis dotyczy jednostki zarządzającej systemem ochrony, o której mowa w **art. 130e ust. 1 projektu ustawy**, w zakresie informacji niezbędnych do realizacji celów, o których mowa w **art. 130b ust. 1** i wsparcia, o którym mowa w **art. 130b ust. 2**, lub zadań organu zarządzającego określonych w **art. 130k ust. 1 pkt 3 i 4 oraz ust. 2**, jeżeli bank jest uczestnikiem tego systemu ochrony. Projektowana zmiana nie określa trybu, zasad udostępniania informacji oraz zakresu udostępnianych danych, zwłaszcza jeśli informacje te zawierają dane o charakterze osobowym. Jeśli tak miałoby być, to należy wskazać katalog tych danych oraz zakres ich przetwarzania, co ma to ogromne znaczenie dla zapewnienia stosowania w przedmiotowych przepisach zasad dotyczących przetwarzania danych osobowych, wynikających z art. 5 rozporządzenia 2016/679[4]. Projektowana zmiana związana jest również z zasadnością przeprowadzenia oceny skutków dla ochrony danych, na którą wskazano powyżej.

Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania”.

[4] Art. 5 rozporządzenia 2016/679 stanowi: „ 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

Projektowany art. 105 ust. 1 pkt 4 Prawa bankowego umożliwi przekazanie tajemnicy bankowej przez bank na rzecz powołanej na podstawie tych przepisów jednostki zarządzającej systemem ochrony (**art. 5 pkt 7 projektu ustawy**).

Projektowana zmiana dotyczy dodania **art. 130b-130l** do **ustawy Prawo bankowe.**

b) Zgodnie z projektowanym **art. 130b ust. 1** *„Celem funkcjonowania systemu ochrony jest zapewnienie płynności i wypłacalności każdego jego uczestnika na zasadach określonych w ustawie i w umowie systemu ochrony, w szczególności przez udzielanie pożyczek, gwarancji i poręczeń na warunkach określonych w umowie systemu ochrony”* - przepis ten zawiera otwarty katalog czynności związanych systemem ochrony, co powinno zostać wyeliminowane, aby nie budziło wątpliwości w tym zakresie.

Utworzenie systemu ochrony ma następować na podstawie umowy systemu ochrony, a udział banków w systemie ochrony ma dobrowolny charakter. Jak wskazano w uzasadnieniu do projektu ustawy: *„System ochrony jest emanacją współpracy, mechanizmów samopomocy oraz odpowiedzialności uczestników sektora bankowego za jego stabilność i prawidłowe funkcjonowanie, nie zastępuje natomiast nadzoru czy zadań właściwych organów publicznych”*. Zatwierdzeniem projektu umowy systemu ochrony będzie zajmował się KNF.

Projektowane przepisy nie zawierają regulacji czy w ramach danego systemu ochrony będzie funkcjonował nowy administrator danych przetwarzanych (czy będą gromadzone dane o charakterze osobowym, a jeśli tak, powinny być wskazane zadania administratora, cele i zasady przetwarzania danych).

Nowe rozwiązanie wprowadzane do ustawy Prawo bankowe jakim jest **umowa systemu ochrony** wymaga przeprowadzenia oceny skutków dla ochrony danych - wykonanie testu prywatności w postaci takiej oceny pozwoliłoby na uniknięcie ryzyk związanych z przetwarzaniem danych osobowych w kontekście istoty i celów przyjmowanych rozwiązań oraz stosowanych technik przetwarzania danych, w szczególności z użyciem nowych technologii. Poprawnie przeprowadzona ocena skutków powinna wskazywać związek pomiędzy operacjami wykonywanymi na danych osobowych, z konkretnym celem ich przetwarzania. Cel przetwarzania musi być określony w podstawie prawnej, gdy są nią przepisy prawa powszechnie obowiązującego (art. 6 ust. 3 rozporządzenia 2016/679). Ten przepis rozporządzenia

---

organizacyjnych („integralność i poufność”). 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”)”.

2016/679 wskazuje również, że podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, jak i inne elementy, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX.

c) Określone w projektowanym **art. 130k ust. 1 Prawa bankowego** zadania organu zarządzającego systemem ochrony stanowią otwarty katalog, co powoduje, że mogą w nim także znaleźć się inne, nie wskazane w tym przepisie zadania. **Ust. 8 projektowanego przepisu** wskazuje, że organ zarządzający systemem ochrony lub osoby przez niego upoważnione są uprawnione do żądania pisemnych lub ustnych informacji i wyjaśnień oraz okazania dokumentów lub innych nośników informacji, jak również udostępnienia danych związanych z działalnością uczestnika systemu ochrony, który zwrócił się do systemu ochrony o udzielenie pomocy lub wsparcia, a organy tego uczestnika systemu ochrony i jego pracownicy są obowiązani udzielać żądanych wyjaśnień i informacji oraz niezbędnej pomocy; wyjaśnienia i informacje są udzielane w zakresie niezbędnym do oceny możliwości i zasadności udzielenia pomocy lub wsparcia - projektowany przepis nie precyzuje natomiast celu, zakresu oraz trybu przekazywanych informacji, co wymaga dookreślenia; przepis ten wymaga również zapewnienia stosowania zasad określonych w art. 5 rozporządzenia 2016/679. Kolejne ustępy **art. 130k (ust. 9 i 10)** również budzą wątpliwości pod kątem braku doprecyzowania o wskazane powyżej informacje.

4. Organ nadzorczy wskazuje również na projektowane zmiany ***w ustawie z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych*** (Dz. U. z 2021 r. poz. 1983 i 2140) **- art. 10 pkt 10 projektu ustawy**.

a) Projektowany **art. 77a ust. 2 ww. ustawy** dotyczy przekazywania zaświadczeń za pomocą systemu teleinformatycznego umożliwiającego składanie powiadomień, do którego dostęp jest zapewniany przez Komisję na jej stronie internetowej, co budzi zastrzeżenia: z przepisu nie wynika jaki system teleinformatyczny umożliwia obsługę funkcjonalności związanych z obsługą dokumentów - wszystkie systemy

teleinformatyczne służące do przetwarzania danych osobowych muszą spełniać wymagania określone w rozporządzeniu 2016/679; wynika to z bezpośredniego stosowania rozporządzenia 2016/679 w polskim porządku prawnym. Przepisy powinny precyzować w jaki sposób zapewnione jest bezpieczeństwo przetwarzanych danych, co odpowiadałoby ww. zasadzie zgodności z prawem, rzetelności i przejrzystości oraz zasadzie integralności i poufności. Projektowane przepisy nie zawierają informacji o funkcjonalności systemu teleinformatycznego (czy będzie to nowy system teleinformatyczny) oraz o rolach podmiotów z niego korzystających – wymaga to doprecyzowania;

b) Z projektowanych przepisów nie wynika jakie dane podmiotu pośredniczącego **(art. 77a ust. 4)** będą przekazywane agencjom informacyjnym, w celu publikacji. – to również wymaga doprecyzowania.

Przepisy powinny szczegółowo regulować zakres przetwarzanych danych, jak również kwestie podziału ról w procesach przetwarzania danych osobowych – istnieje konieczność ustalenia ról w procesie przetwarzania danych osobowych ale odpowiednio do rzeczywistego przetwarzania danych osobowych - co ma kluczowe znaczenie z punktu widzenia odpowiedzialności za realizację praw i obowiązków wynikających z przepisów o ochronie danych osobowych. Budowane normy powinny być przejrzyste także pod kątem ustalenia odpowiedzialności podmiotów realizujących w ich oparciu procesy przetwarzania danych tak, aby wyeliminować wszelkie ryzyka związane z niewłaściwą ich interpretacją.

Uwzględnienie powyższych kwestii przyczyniłoby się do stworzenia przepisów czyniących zadość przepisom o ochronie danych osobowych, zapewniających stosowanie rozporządzenia 2016/679.

Z wyrazami szacunku,

Prezes Urzędu
Ochrony Danych Osobowych
Jan Nowak

/- dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/