



PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

Warszawa, 21.03.2023 r.

DOL.401.84.2023.WL.MW.

Sz. P.
Kazimierz Kleina
Przewodniczący
Komisji Budżetu i Finansów Publicznych
Kancelaria Senatu
ul. Wiejska 6/8
00-902 Warszawa

Szanowny Panie Przewodniczący,

w związku z pismem z dnia 15 marca 2023 r. (znak: BPS.DKS.KBFP.0330.7.2023) informującym o posiedzeniu Komisji w dniu 28 marca br. dotyczącym rozpatrzenia projektu **ustawy o zmianie ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, ustawy o obligacjach, ustawy o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji oraz niektórych innych ustaw** (druk senacki nr 939 , druki sejmowe nr 2992, 3045 i 3045-A), uprzejmie wskazuję na aktualność stanowisk organu nadzorczego, przedstawionych w toku procesu legislacyjnego¹ (w załączeniu), które nie zostały uwzględnione przez projektodawcę.

Aktualność zachowują poniższe uwagi organu nadzorczego, który poleca je uwadze Komisji:

1. Konieczność przeprowadzenia oceny skutków dla ochrony danych - uwaga ta została zgłaszana na wcześniejszym etapie procesu legislacyjnego. Projektowane przepisy ze względu na rodzaj przetwarzania, w szczególności następującego przy

¹ Stanowiska organu nadzorczego: pismo z 31 lipca 2020 r., znak: DOL.401.301.2020; pismo z 30 lipca 2021 r., znak: DOL.401.369.2021; pismo z 10 listopada 2022 r., (znak: DOL.401.369.2022), pismo z 28 lutego 2023 r. (DOL.401.84.2023).

użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób. Wskazać w tym miejscu należy chociażby na przepisy dotyczące prowadzenia rejestru osób uprawnionych z obligacji kapitałowych. Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędności przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych.

2. Konieczność określenia ról poszczególnych podmiotów, które biorą udział w procesie przetwarzania danych (m.in. administratora) – precyzyjne określenie ról poszczególnych podmiotów, odpowiadających procesom przetwarzania danych osobowych - rzeczywistym celom i potrzebom związanym z przetwarzaniem danych osobowych, jest niezbędne dla zapewnienia rozwiązań zgodnych z przepisami o ochronie danych osobowych. Istotne jest doprecyzowanie projektowanych przepisów w kontekście korzystania z nowych technologii, w tym systemów teleinformatycznych, wskazując na zapewnienie bezpieczeństwa i funkcjonalności przetwarzanych danych w systemie, m.in. poprzez precyzyjne określenie ról i obowiązków – w odniesieniu do także precyzyjnie określonych celów przetwarzania, operacji (zestawów operacji) przetwarzania – podmiotów czerpiących dane osobowe z systemu teleinformatycznego oraz zasilających system danymi osobowymi.
3. Brak doprecyzowania w zakresie przetwarzania danych o charakterze osobowym - **art. 330 ust. 1² ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji** (Dz. U. 2022 r. poz. 793, 872 i 1692). Projektowany przepis jest zbyt ogólny, nie wskazuje bowiem zakresu przetwarzanych danych osobowych. Dane osobowe mogą być udostępniane jedynie, o ile jest to niezbędne i w zakresie minimalnym dla wypełnienia celów projektowanej regulacji, przy czym cel (cele) przetwarzania danych także powinny być określone przejrzysto. Nie został wskazany tryb pozyskiwania informacji. Projektodawca powinien uzupełnić ww. przepis w taki sposób, aby zapewnić stosowanie przepisów rozporządzenia

²„Fundusz może uzyskiwać bezpośrednio od podmiotu informacje niezbędne do realizacji zadań Funduszu, w szczególności niezbędne do wykonania oszacowania, o którym mowa w art. 137 ust. 1, a także wyceny, o której mowa w art. 24 rozporządzenia nr 2021/23, oraz przygotowania przymusowej restrukturyzacji albo restrukturyzacji i uporządkowanej likwidacji CCP, a także żądać wyjaśnień dotyczących uzyskanych informacji w przypadku zobowiązania takiego podmiotu do wdrożenia planu naprawy, podjęcia wobec niego działań wczesnej interwencji lub ustanowienia w nim zarządu komisarycznego lub zarządcy komisarycznego”.

2016/679 w zakresie zasad wynikających z art. 5 ust. 1, jak również zasady rozliczalności (art. 5 ust. 2)³.

4. W odniesieniu do zmiany w **ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi** (Dz. U. z 2022 r. poz. 1500, 1488, 1933, 2185 i 2640 oraz z 2023 r. poz. 180):
 - a) **art. 7aa** dotyczący utworzenia rejestru osób uprawnionych z obligacji kapitałowych oraz zapisywanie instrumentów finansowych za pomocą technologii rozproszonego rejestru nie określa zakresu przetwarzanych danych osobowych, ról podmiotów w tym rejestrze. Istotną kwestią jest zagadnienie związane z zabezpieczeniem dokumentacji, wdrożeniem odpowiednich środków technicznych i organizacyjnych. Aktualność zachowują zatem uwagi do projektowanego przepisu zawarte w opiniach z 31 lipca 2020 r., 30 lipca 2021 r. oraz 10 listopada 2022 r. i 28 lutego br., które nie zostały uwzględnione na wcześniejszym etapie procesu legislacyjnego.
 - b) nieprecyzyjny **dodawany art. 173e ust. 1 pkt 1** wskazujący, że Komisja może, w drodze decyzji podać do publicznej wiadomości informację wskazującą osobę fizyczną, CCP lub inną osobę prawną odpowiedzialną za naruszenie i charakter tego naruszenia. Komisja Nadzoru Finansowego posiada uprawnienie, natomiast nie określa w jakich przypadkach, na jakich zasadach, jaki zakres danych osobowych oraz przez jaki czas będzie podany do publicznej wiadomości, co stanowi naruszenie zasad wynikających z art. 5 rozporządzenia 2016/679.
5. Projektowany **art. 362a ust. 5 i 6⁴** w **ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej** (Dz. U. z 2022 r. poz. 2283 i 2640) nie został przez projektodawcę uzasadniony. Podanie do publicznej

³ Zgodnie z art. 5 rozporządzenia 2016/679 „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")”.

⁴ „Organ nadzoru przekazuje do publicznej wiadomości informacje o treści rozstrzygnięcia, o którym mowa w ust. 1, rodzaju i charakterze naruszenia, imieniu i nazwisku osoby fizycznej lub firmie (nazwie) podmiotu, na który została nałożona sankcja. Informacje, o których mowa w ust. 5, dotyczące imienia i nazwiska osoby, na którą została nałożona sankcja, organ nadzoru udostępnia na stronie internetowej przez okres 5 lat, licząc od dnia ich udostępnienia”.

wiadomości (udostępnienie na stronie internetowej) danych osobowych w postaci imienia i nazwiska wymaga ponownej analizy i zachowania zgodności z przepisami ogólnego rozporządzenia o ochronie danych osobowych.

Jednocześnie za bezprzedmiotowe uznać należy dwie uwagi organu nadzorczego przekazane projektodawcy pismem z dnia 30 lipca 2021 r. (znak: DOL.401.369.2021.WL.MW) dotyczące katalogu informacji, które są określane w uchwale walnego zgromadzenia - w ustawie z dnia 15 stycznia 2015 r. o obligacjach - art. 27n ust. 2 oraz w ustawie z dnia 15 września 2000 r. – Kodeks spółek handlowych - art. 454² ust. 2 – wskazać należy, że przedmiotowe przepisy dotyczą danych/informacji finansowych.

Uwzględnienie powyższych kwestii wskazanych jako eksperckie wsparcie z zakresu przetwarzania danych osobowych niewątpliwie przyczyni się do właściwego wdrożenia zasad ochrony danych w wynikających z przepisów rozporządzenia 2016/679 w procedowanym akcie normatywnym.

Załączniki:

- stanowiska organu nadzorczego: pismo z 31 lipca 2020 r., znak: DOL.401.301.2020; pismo z 30 lipca 2021 r., znak: DOL.401.369.2021; pismo z 10 listopada 2022 r. (znak: DOL.401.369.2022), pismo z 28 lutego 2023 r. (DOL.401.84.2023).

Z wyrazami szacunku,

Prezes Urzędu
Ochrony Danych Osobowych
Jan Nowak

/-dokument w postaci elektronicznej
podpisany kwalifikowanym
podpisem elektronicznym/