PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, *21-12-2025*

DPNT.401.502.2025

Pan
Jurand Drop
Podsekretarz Stanu

Ministerstwo Finansów

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 3 grudnia 2025 r. (znak: FN .700.11.2025), dotyczące **projektu ustawy o osobistych kontach inwestycyjnych** (projekt z grudnia 2025 r.), działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy **zgłasza następujące uwagi.**

1. **Art. 2** projektu ustawy odnoszący się do definicji, w **punkcie 18** odwołuje się do przepisów ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi i określa „rejestr uczestników" jako „rejestr uczestników funduszu inwestycyjnego, o którym mowa w art. 87 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi". Art. 87 ust. 2 pkt 1 ustawy o funduszach inwestycyjnych (…) wskazuje, że „Rejestr uczestników funduszu zawiera w szczególności: dane identyfikujące uczestnika funduszu" bez doprecyzowania tych danych, w związku z czym rejestr uczestników definiowany w projektowanej ustawie powinien dookreślać katalog danych osobowych identyfikujących uczestnika funduszu inwestycyjnego (zasada minimalizacji danych – art. 5 ust. 1 lit c rozporządzenia 2016/679).

2. Wątpliwości budzi **art. 5** projektu ustawy dotyczący **umowy o prowadzenie osobistych kont inwestycyjnych (OKI)**.

[1] 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Wstęp do wyliczenia elementów umowy – poprzez sformułowanie „w szczególności” i pomimo wyróżnienia w pkt 2 zamkniętego katalogu „danych identyfikacyjnych inwestującego” – zawiera otwarty katalog informacji, a tym samym także danych osobowych identyfikujących inwestującego. Projektowany przepis powinien zatem zostać doprecyzowany, poprzez zamknięcie katalogu danych, celem zapewnienia stosowania zasad wynikających z art. 5 rozporządzenia 2016/679[3], zwłaszcza zgodności z zasadami: zgodności z prawem, rzetelności i przejrzystości, celowości oraz minimalizacji danych.

Ponadto, wśród danych identyfikujących inwestującego, projektodawca wskazał zarówno numer PESEL, jak i identyfikator podatkowy NIP, jeżeli został nadany (**art. 5 pkt 2 lit. c-d**). Projektodawca nie uzasadnił niezbędności pozyskiwania numeru PESEL w sytuacjach, gdy przetwarzany jest równocześnie numer NIP. W ocenie organu nadzorczego, o ile osoba posiada NIP powinna być właśnie przez ten numer identyfikowana. Numer PESEL jest daną, która w sposób unikatowy pozwala na zidentyfikowanie osoby, a pozyskiwanie tej danej w celu weryfikacji osoby fizycznej należy ocenić jako nadmiarowe (zasada minimalizacji danych). Numer PESEL powinien być przetwarzany jedynie, gdy jest to adekwatne i konieczne do realizacji konkretnego celu, dla realizacji którego niewystarczający jest numer NIP. Jeżeli numer PESEL miałby być również przetwarzany, konieczne jest wskazanie celu pozyskiwania tej danej osobowej przy jednoczesnym przetwarzaniu w rejestrze numeru NIP.

Tożsama uwaga dotyczy **art. 8 ust. 2** oraz **art. 16 ust. 1 pkt 1** projektu ustawy.

3. Projektowany **art. 13** ust. 1 ustawy przewiduje, że: „Instytucja finansowa z chwilą zawierania umowy o prowadzenie OKI jest obowiązana uzyskać od klienta lub potencjalnego klienta adekwatne informacje dotyczące jego wiedzy i doświadczenia w zakresie inwestowania na rynku finansowym, zgodnie z art. 55 i art. 56 rozporządzenia delegowanego Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniającego

[3] Art. 5 rozporządzenia 2016/679 stanowi: „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").”.

dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy (Dz. Urz. UE L 87 z 31.03.2017, str. 1, z późn. zm.[4)]).”.

Projektodawca, nakładając przedmiotowy obowiązek, obejmujący nie tylko instytucję finansową, ale i klienta lub potencjalnego klienta, nie wskazał jednak w jaki sposób będą weryfikowane ww. informacje dotyczące ich wiedzy i doświadczenia w zakresie inwestowania na rynku finansowym oraz czy, a jeśli tak, to w jaki będą one odnotowywane (art. 56 ww. aktu unijnego wskazuje, że firmy inwestycyjne prowadzą rejestry dotyczące dokonanych ocen adekwatności). Przepis ten wymaga dookreślenia w ww. zakresie.

4. **Art. 16 ust. 1 pkt 1** wskazuje zakres danych identyfikujących inwestującego, które dotychczasowa instytucja finansowa prowadząca OKI sporządza i przekazuje w postaci elektronicznej przyszłej instytucji finansowej (po dokonaniu wypłaty transferowej). Przepis ten – projektodawca wskazuje w nim zakres danych inwestującego poprzez „**pierwsze imię** i nazwisko” – jest niespójny z art. 5 pkt 1 projektu ustawy również określającym dane identyfikujące inwestującego poprzez **„imię** i nazwisko”, a zatem regulacje te wymagają ujednolicenia.

5. **Art. 27 ust. 1** projektu ustawy stanowi, że „instytucje finansowe są obowiązane sporządzać w postaci elektronicznej informacje o prowadzeniu OKI i przesyłać te informacje za pomocą środków komunikacji elektronicznej zgodnie z odrębnymi przepisami właściwym naczelnikom urzędów skarbowych”, przy czym projektodawca nie precyzuje jakie to przepisy. **Art. 27 ust. 2 pkt 1** projektu ustawy określa zaś, że: „Informacja o prowadzeniu OKI zawiera dane identyfikacyjne instytucji finansowej i podatnika”, nie precyzując katalogu danych podatnika. Przez wzgląd na zasadę celowości i zasadę minimalizacji danych przepis ten wymaga dookreślenia poprzez wyraźne wskazanie konkretnych danych osobowych podatnika.

Analogiczna uwaga dotyczy **art. 29 ust. 2 pkt 1** projektu ustawy.

Podobnie **art. 27 ust. 2 pkt 4** wskazuje na „dane niezbędne do udostępnienia zeznania podatkowego w e-Urzędzie Skarbowym” bez dookreślenia przedmiotowych danych.

Zwrócić także uwagę należy na **ust. 5** ww. przepisu w brzmieniu: „Minister właściwy do spraw finansów publicznych określi, w drodze rozporządzenia, szczegółowy zakres danych zawartych w informacji o prowadzeniu OKI, uwzględniając konieczność prawidłowego rozliczenia podatku oraz kontroli wykonania tego obowiązku przez organ podatkowy”. Rozważenia wymaga czy w katalogu informacji o prowadzeniu OKI miałyby być przetwarzane także dane osobowe z art. 9 (szczególne kategorie danych) lub art. 10 (dane osobowe dotyczące wyroków skazujących i czynów zabronionych) rozporządzenia

4) Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 246 z 26.09.2017, str. 12, Dz. Urz. UE L 329 z 13.12.2017, str. 4, Dz. Urz. UE L 113 z 29.04.2019, str. 18, Dz. Urz. UE L 165 z 21.06.2019, str. 1, Dz. Urz. UE L 190 z 16.07.2019, str. 18, Dz. Urz. UE L 106 z 26.03.2021, str. 30 oraz Dz. Urz. UE L 277 z 02.08.2021, str. 1 i 6.

2016/679 – wówczas podstawa do ich przetwarzania powinna być ustanowiona mocą przepisów rangi ustawy, zgodnie z art. 51 w zw. z art. 31 ust. 3 Konstytucji RP.

Tożsama uwaga odnosi się do **art. 29 ust. 3** projektu ustawy.

6. Wątpliwości budzi **art. 39** projektu ustawy wprowadzający **zmiany w ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej** (Dz.U. z 2025 r. poz. 1131 i 1423), dotyczące automatycznego udostępniania i wypełniania dokumentów. **Art. 35 ca ust. 1-2** wskazuje, że: „1. Na kontach w e-Urzędzie Skarbowym mogą być udostępniane automatycznie pisma, do których składania, na podstawie odrębnych przepisów, są obowiązani podatnicy. 2. Pisma podlegające udostępnieniu na koncie w e--Urzędzie Skarbowym są wypełniane automatycznie danymi pozostającymi w posiadaniu Szefa Krajowej Administracji Skarbowej, jeżeli znajdują się w CRDP".

Zwrócić uwagę należy na kwestie związane z zastosowaniem technologii wykorzystującej automatyczne przetwarzanie danych. Projektowane przepisy zakładają zautomatyzowane przetwarzanie danych, zatem zachodzi prawdopodobieństwo, że mogą być również wykorzystywane systemy sztucznej inteligencji. W związku z powyższym projektodawca powinien wziąć pod uwagę nie tylko przepisy rozporządzenia 2016/679, ale także akt w sprawie sztucznej inteligencji[5], którego zapewnienie stosowania w krajowym porządku prawnym jest i będzie niezwykle istotne. Należy bowiem m.in. podkreślić, że z art. 27 aktu w sprawie sztucznej inteligencji wynika **odrębny obowiązek dokonania przez organy publiczne oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (FRIA)**. Motyw 96 AI Act podkreśla, że **FRIA ma na celu uzupełnienie oceny ochrony danych, a nie jej zastąpienie.** Jeżeli wykonywanie projektowanych norm będzie wiązało się z wykorzystaniem systemów sztucznej inteligencji, to projektodawca powinien również uwzględnić dokonanie takiej oceny. Transparentne systemy AI, działające w oparciu o szczegółowe przepisy wypracowane przez projektodawcę, gwarantować powinny m.in. dostęp do dokładnych informacji o działaniu modelu sztucznej inteligencji oraz do rzetelnego wyjaśnienia, obejmującego zarówno procesy techniczne systemu, jak i uzasadnienie decyzji dokonywanej przez system sztucznej inteligencji czy przy jego wsparciu. Wykonawcy norm powinni być bowiem świadomi, że dana interakcja odbywa się ze sztuczną inteligencją, a regulacja o odpowiedniej randze (ustawa) powinna określać cele, których realizacji służy, jakim podmiotom przypisany zostanie status administratora danych, jak również jakie gwarancje ochrony praw i wolności osób zostaną określone jej przepisami. Systemy sztucznej inteligencji, które stwarzają wysokie ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych osób fizycznych, mogą być dopuszczone do obrotu wyłącznie **pod warunkiem spełnienia określonych wymogów i przeprowadzenia oceny zgodności**. Z dokumentów przedstawionych do zaopiniowania nie wynika, aby projektodawca wykonał tego rodzaju analizy i oceny, a w konsekwencji, by wyważył wpływ planowanego przetwarzania danych osobowych na autonomię

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji, AI Act).

informacyjną oraz prywatność osób, których te dane dotyczą i proponował rozwiązania odpowiadające poszanowaniu zasad i standardów przetwarzania danych osobowych. Projektowane rozwiązania, w szczególności związane z zautomatyzowanym przetwarzaniem danych osobowych, powinny być przejrzyście, wyczerpująco i szczegółowo ujęte w przepisach ustawy. O ile ingerencja taka ma następować, to powinna być odpowiednio uzasadniona, proporcjonalna i niezbędna do celu, jaki projektowana regulacja ma realizować (zgodnie z art. 31 ust. 3 Konstytucji RP). Zgodnie natomiast z **art. 22 rozporządzenia 2016/679** – co do zasady – osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Odstępstwa od tej zasady są możliwe po spełnieniu jednego z warunków ustanowionych w art. 22 ust. 2 rozporządzenia 2016/679, m.in. gdy decyzja ta jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Z przepisu tego jasno wynika, że jeżeli profilowanie ma być stosowane czy dozwolone na podstawie przepisów prawa, to przepisy te powinny gwarantować właściwe środki ochrony praw osób, których dane dotyczą (regulacja w kontekście profilowania istnieje i jest ustanowiona np. w art. 105a ust. 1a ustawy Prawo bankowe).

Tworzenie regulacji prawnych wymaga względu projektodawcy na **spoczywające na administratorach** obowiązki wynikające wprost z ogólnego rozporządzenia o ochronie danych, tj. informowania osób, których dane dotyczą, w przypadku przetwarzania danych osobowych, w tym zautomatyzowanego podejmowania decyzji i profilowania. Realizacja zasady przejrzystości wybrzmiewa szczególnie w przypadku zautomatyzowanego podejmowania decyzji, w tym profilowania w rozumieniu art. 22 ust. 1 rozporządzenia 2016/679. Osoba, której dane dotyczą, ma prawo dostępu do danych przewidziane w art. 15 ust. 1 ww. rozporządzenia (jak również zgodnie z dodatkowymi obowiązkami informacyjnymi, które ciążą na administratorze na podstawie art. 13 ust. 2 lit. f i art. 14 ust. 2 lit. g) tego rozporządzenia, do: informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia 2016/679, istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Administrator musi zapewnić osobie, której dane dotyczą, dostateczne informacje, aby przetwarzanie było rzetelne i przejrzyste[6]. Administrator powinien znaleźć proste sposoby, aby poinformować osobę, której dane dotyczą, o przesłankach lub kryteriach, na których opiera się decyzja. Rozporządzenie 2016/679 wymaga od administratora dostarczenia istotnych informacji na temat założeń przetwarzania, niekoniecznie złożonego wyjaśnienia zastosowanych algorytmów lub ujawnienia pełnego

[6] Motyw 60 rozporządzenia 2016/679: „Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania."

algorytmu[7]. Dostarczone informacje powinny jednak być wystarczająco wyczerpujące, aby osoba, której dane dotyczą, zrozumiała przyczyny decyzji[8]. Motyw 63 rozporządzenia 2016/679 wyjaśnia, że: „(…) każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. W miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. **Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji.** Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie”.

Z uzasadnienia do projektu ustawy nie wynika jednak, aby projektodawca wykonał test prywatności, analizę i ocenę pod kątem ryzyk towarzyszących proponowanemu przetwarzaniu danych osobowych. Przepisy dotyczące przetwarzania danych osobowych wprowadzane w projektowanej ustawie determinują natomiast zasadność przeprowadzania testu prywatności – projektowania ochrony danych osobowych w procesie tworzenia prawa[9], w tym przeprowadzenia oceny skutków dla ochrony danych[10]. Przeprowadzony test prywatności ułatwiłby projektodawcy dokonanie analizy ryzyk towarzyszących przetwarzaniu danych osobowych, jak również zweryfikowanie niezbędności wprowadzenia określonych rozwiązań, jak np. automatycznego przetwarzania danych, aby stworzyć regulacje zgodne ze standardami i zasadami wynikającymi z przepisów rozporządzenia 2016/679 i zagwarantować w przepisach odpowiednie zabezpieczenia praw i wolności osób, których dane mają być przetwarzane

---

[7] Motyw 58 rozporządzenia 2016/679 stanowi, że zasada przejrzystości dotyczy „w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie”.

[8] Wytyczne Grupy roboczej art. 29 dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679.

[9] Art. 25 ust. 1 rozporządzenia 2016/679 stanowi: „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”.

[10] Uzasadnionym jest dokonanie oceny skutków dla ochrony danych – zgodnie z art. 35 ust. 10 rozporządzenia 2016/679 - już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych, co przy dokonaniu prawidłowej oceny i wypracowaniu przepisów szczególnych uwzględniających stosowanie ogólnego rozporządzenia o ochronie danych może zastąpić dokonywanie takiej oceny przez podmioty stosujące / wykonujące następnie tak ustalone przepisy.

dla realizacji obowiązków wynikających z projektowanych przepisów. Przeprowadzona ww. analiza pozwoliłaby m.in. zbadać czy projektowane przepisy odpowiadają wymogom art. 6 ust. 3 z rozporządzenia 2016/679, są proporcjonalne i stanowiące gwarancje odpowiednie do ratio legis, tj. do wyznaczonego, prawnie uzasadnionego celu regulacji.

Pragnę jednocześnie podkreślić, że uwagi organu nadzorczego przedstawiane w toku prac legislacyjnych mają charakter eksperckich wskazówek dla projektodawcy, który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych. Wyrażam nadzieję, że uwzględnienie wyrażonych wskazówek będzie pomocne w tym procesie i przyczyni się do podwyższenia poziomu ochrony danych osobowych w projektowanych przepisach.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych