



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Jan Nowak

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU

L.dz. *SPS-WP.020.82.11.2021*

Data wpływu *25. 03. 2021*

Warszawa, 22 marca 2021 r.

DOL.401.106 .2021.WL.MP

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu
Kancelaria Sejmu RP
ul. Wiejska 4/6/7
00-902 Warszawa
ESP: /KSRP/SKRYTKAESP

Szanowny Panie Ministrze,

w nawiązaniu do pisma z 12 marca 2021 r. (sygn. SPS-WP.020.82.3.2021) uprzejmie dziękuję za przedstawienie rządowego projektu z dnia o zmianie niektórych ustaw w związku z przeniesieniem środków z otwartych funduszy emerytalnych na indywidualne konta emerytalne do zaopiniowania przez organ właściwy w sprawie ochrony danych osobowych oraz uprzejmie informuję, że – 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.¹) – do niejszego projektu, zwanego dalej projektem ustawy, zgłaszam następujące uwagi.

1. Uwaga do art. 13 pkt 6 i 7 projektu ustawy, które nadają nowe brzmienie odpowiednio przepisom art. 33 w ust. 1 pkt 5 oraz art. 34 ust. 5 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2021 r. poz. 423), zwanej dalej ustawą o sus.

Przepisem art. 33 ust. 1 pkt 5 ustawy o sus Projektodawca proponuje zmianę dotychczas prowadzonego przez Zakład Ubezpieczeń Społecznych Centralnego Rejestru Członków OFE na

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 04.03.2021, str. 35.

Centralny Rejestr Uczestników Funduszy. Natomiast zgodnie z art. 34 ust. 5 ustawy o sus ZUS oraz fundusz inwestycyjny są obowiązane do wzajemnego udostępniania danych osobowych osób zarejestrowanych w rejestrze, o którym mowa w art. 33 ust. 1 pkt 5.

Niemniej jednak, z obecnych przepisów ustawy o sus, jak i z zaproponowanych przez Projektodawcę zmian nie wynika wprost kto jest administratorem przetwarzanych danych w rejestrze, jakie role w przetwarzaniu danych pełnią ZUS i fundusz inwestycyjny (administrowanie – art. 4 pkt 7^{2/} czy współadministrowanie – art. 26³ ogólnego rozporządzenia o ochronie danych) w jakim celu przetwarza się dane, przez jaki okres czasu, jak wygląda cały proces przetwarzania danych osobowych, a w tym przekazywanie danych pomiędzy ZUS a funduszem inwestycyjnym lub też innymi podmiotami. Przepisy *rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 21 grudnia 2009 r. w sprawie szczegółowego zakresu danych zawartych w centralnych rejestrach prowadzonych przez Zakład Ubezpieczeń Społecznych* (Dz. U. z 2013 r. poz. 21) wskazują jedynie zakres przetwarzanych w rejestrze danych. Jednocześnie warto zauważyć, że na część zadanych powyżej pytań odpowiedź można znaleźć pod linkiem <https://stat.gov.pl/metainformacje/repozytorium-standardow-informacyjnych/informacje-osystemachinformacyjnych/systemy-informacyjne-objete-rsi/1237,pojecie.html> tj. na stronie internetowej Głównego Urzędu Statystycznego. Niemniej jednak kwestie, o których można dowiedzieć się ze strony internetowej GUS powinny wynikać bezpośrednio z przepisów ustawy regulującej Centralny Rejestr Uczestników Funduszy. Podobny problem braku przepisów, które określałyby i precyzowały proces przetwarzania danych dotyczy kwestii Centralnego Rejestru Płatników Składek oraz Centralnego Rejestru Ubezpieczonych, które nie są zmieniane obecną nowelizacją ustawy o sus.

Ustawa o sus wymaga zatem zapewnienia w treści jej przepisów kompleksowej regulacji doprecyzowującej kwestię przetwarzania danych w przedmiotowych rejestrach pod kątem zasad dotyczących przetwarzania danych osobowych zawartych w art. 5⁴, w tym zasady

²„Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

³Art. 26 ust. 1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą

⁴Art. 5 ust. 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 („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 („prawidłowość”); e) przechowywane w formie

zgodności z prawem, rzetelności i przejrzystości oraz przesłanek przetwarzania danych przez organy publiczne wskazanych w art. 6 ust. 1 lit. c)⁵ i e)⁶ ogólnego rozporządzenia o ochronie danych. Przejrzyste i wyczerpujące określanie praw i obowiązków wiążących organy i podmioty z sektora administracji sprzyja stosowaniu ww. zasady legalizmu (niedomniemywaniu kompetencji), co w konsekwencji eliminuje wątpliwości związane z praktycznym stosowaniem przepisów prawa.

Organ nadzorczy przypomina także o **wymogu przeprowadzenia oceny skutków dla ochrony danych⁷** w odniesieniu do planowanego przetwarzania danych osobowych za pośrednictwem Centralnego Rejestru Uczestników Funduszy oraz w odniesieniu do już działających rejestrów Centralnego Rejestru Płatników Składek oraz Centralnego Rejestru Ubezpieczonych. Uzasadnienie do projektu ustawy takiej oceny skutków dla ochrony danych nie zawiera, a zatem brak jest informacji o przeprowadzaniu analizy ryzyk i wpływu jej wyników na przyjmowane rozwiązania dotyczące przetwarzania danych osobowych. Dokonanie takiej oceny przyczyniłoby się do przyjmowania przez projektodawcę rozwiązań z zakresu przetwarzania danych osobowych poddanych wcześniejszemu testowi zgodności z zasadami ogólnego rozporządzenia o ochronie danych osobowych, w szczególności z zasadą rozliczalności. Ocena taka obejmuje bowiem planowane operacje przetwarzania i cele przetwarzania; rozważenie czy operacje są niezbędne oraz proporcjonalne w stosunku do celów regulacji wynikających z ustawy o sus; ocenę ryzyka naruszenia praw lub wolności podmiotów danych – beneficjentów ustawy o sus; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych i wykazać przestrzeganie

umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („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”).

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

⁵Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

⁶Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

⁷Art. 35 ust. 1 w związku z ust. 10 ogólnego rozporządzenia o ochronie danych reguluje obowiązek dokonania – przed rozpoczęciem przetwarzania – oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ocena skutków dla ochrony danych nie jest wymagana jeżeli operacja przetwarzania, zgodnie z art. 6 ust. 1 lit. c) lub e) ogólnego rozporządzenia o ochronie danych, ma podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej. Zgodnie z art. 35 ust. 7 ogólnego rozporządzenia o ochronie danych, ocena skutków zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje są niezbędne oraz proporcjonalne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych i wykazać przestrzeganie ogólnego rozporządzenia o ochronie danych.

ogólnego rozporządzenia o ochronie danych przez administratora (-ów) (współadministratorów), tj. organy/podioty będące wykonawcami norm ustawy o sus. Jej przeprowadzenie wykazałoby zatem potrzebę przetwarzania konkretnych danych albo jej brak jak również opisywałaby w pełni proces ich przetwarzania co pozwoliłoby uczynić ukształtowane normy prawne bardziej przejrzystymi dla zobowiązanych do ich stosowania.

2. Uwaga do art. 18 pkt 18 projektu ustawy dodającego art. 34c ust. 2 do ustawy z dnia 20 kwietnia 2004 r. o indywidualnych kontach emerytalnych oraz indywidualnych kontach zabezpieczenia emerytalnego (Dz. U. z 2019 r. poz. 1808), zwanej dalej ustawą o ike.

Projektodawca proponuje aby przepis art. 34c ust. 2 ustawy o ike brzmiał następująco:
„Specjalistyczny fundusz inwestycyjny otwarty, o którym mowa w art. 26c, dokonuje wypłaty środków należnych osobie wskazanej przez zmarłego w terminie 3miesiący, nie wcześniej jednak niż w terminie miesiąca od dnia przedstawienia funduszowi urzędowego dokumentu stwierdzającego tożsamość osoby uprawnionej, z tym że wypłata środków przypadających małżonkowi zmarłego może być przekazana na jego żądanie na IKE, o którym mowa w rozdziale 3a. W tym ostatnim przypadku do wypłaty transferowej środków przypadających małżonkowi zmarłego stosuje się odpowiednio przepisyart. 34b ust. 3 i 4”.

Zasadną byłaby zmiana sformułowania „przedstawienie” na „okazanie” gdyż z przepisów ustawy o ike nie wynika obowiązek, czy uprawnienie funduszu inwestycyjnego do przetwarzania kopii, czy też skanu dokumentu stwierdzającego tożsamość osoby uprawnionej. Obecnie sformułowana propozycja przepisu może prowadzić do nadinterpretacji i pozyskiwania nieadekwatnych do celu przetwarzania danych osoby uprawnionej poprzez ewentualne kopiowanie dokumentu stwierdzającego tożsamość. W sytuacji kiedy osoba uprawniona będzie okazywać dokument stwierdzający tożsamość przepis w jasny sposób będzie formułował sposób zachowania się osoby uprawnionej oraz administratora przetwarzanych danych dokonujących czynności przed wypłatą środków należnych, czyli weryfikacji prawa uprawnionego do otrzymania przedmiotowej wypłaty.

3. Uwaga do art. 39 ust. 15 projektu ustawy

Projektodawca proponuje aby przepis art. 34c ust. 2 ustawy o ike brzmiał następująco:
„Minister właściwy do spraw zabezpieczenia społecznego określi, w drodze rozporządzenia, szczegółowy zakres danych zawartych w deklaracji, o której mowa w ust. 1, oraz wzór tej deklaracji, biorąc pod uwagę, aby w deklaracji zawarte były wyłącznie dane niezbędne dla zapewnienia sprawności procesu składania deklaracji.”.

Podkreślenia wymaga, że zakres przetwarzania danych powinien być uzależniony od celów przetwarzania, co będzie zgodne z zasadą minimalizacji danych zawartą w art. 5 ust. 1 lit. b oraz c ogólnego rozporządzenia o ochronie danych. A zatem Projektodawca, tworząc przedmiotowe rozporządzenie, powinien ocenić jakie dane członka otwartego funduszu emerytalnego będą potrzebne do sporządzenia deklaracji o przeniesieniu środków zgromadzonych na jego rachunku do Zakładu Ubezpieczeń Społecznych, działającego w imieniu i na rzecz Funduszu Ubezpieczeń Społecznych. Ocena taka wykaże niezbędność przetwarzania konkretnych danych, które będą pozyskiwane za pośrednictwem wzoru deklaracji, co może posłużyć do wykazania – w uzasadnieniu do tworzonego rozporządzenia – przestrzegania wyżej wymienionych zasad przetwarzania danych zgodnie z zasadą rozliczalności sformułowaną w art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych.

Z wyrazami szacunku,

Prezes Urzędu
Ochrony Danych Osobowych

Jan Nowak

/-dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym-/