



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 22-04-2025

DPNT.401.132.2025.WL.OJ

Pan
Dariusz Salamończyk
Zastępca Szefa
Kancelarii Sejmu RP
Kancelaria Sejmu RP

ePUAP
/KS RP/Skrytka ESP

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 15 kwietnia 2025 r. znak SPS-III.020.77.4.2025, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², uprzejmie informuję, że do przedstawionego **rządowego projektu ustawy o zmianie ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych oraz niektórych innych ustaw (druk nr 1172)**, dalej: projekt, Prezes Urzędu Ochrony Danych Osobowych zgłasza następujące uwagi.

I. Uwagi ogólne.

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.), dalej: rozporządzenie 2016/679.

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Jak deklaruje w uzasadnieniu projektodawca, celem rządowego projektu jest **zmniejszenie obciążeń finansowych osób pokrywających koszty pogrzebu.**

Ze zaskoczeniem należy więc przyjąć wiadomość, że na ostatnim etapie prac legislacyjnych (Rada Ministrów) nad projektem³ – zmieniającym 11 ustaw – jego przepisy zostały rozszerzone o rozwiązanie wiążące się z **szeregiem ryzyk dla ochrony danych osobowych i prywatności** potencjalnie tysięcy osób fizycznych, w postaci poszerzenia przepisów ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych⁴ o rozwiązanie⁵ przyjęte w art. 118a. Projektowany przepis zapewnia bowiem Zakładowi Ubezpieczeń Społecznych (ZUS) możliwość podejmowania w sposób zautomatyzowany rozstrzygnięć w sprawach świadczeń należących do zakresu działania ZUS regulowanego przepisami ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych przy jednoczesnym braku zapewnienia właściwych środków ochrony prawa, wolności i prawnie uzasadnionych interesów podmiotów danych, co jest wymagane przepisem art. 22 ust. 2 lit. b RODO. W konsekwencji, **projektowany przepis ustawy wprowadza ograniczenie praw osób otrzymujących świadczenia, których dane są przetwarzane przez ZUS, wynikających z unijnego rozporządzenia 2016/679, w sposób naruszający europejskie normy ochrony danych osobowych.**

W piśmie resortu⁶, przekazującym do rozpatrzenia przez Radę Ministrów projekt zawierający jako autopoprawkę dodawany ww. art. 118a, wskazano, że: „wprowadzenie tego przepisu wynika z faktu, że od 1 stycznia 2025 r. Zakład Ubezpieczeń Społecznych realizuje przepisy ustawy z dnia 26 lipca 2024 r. o zmianie ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych oraz niektórych innych ustaw (Dz. U. poz. 1243), które wprowadziły możliwość wypłaty własnego świadczenia emerytalno-rentowego w zbiegu z rentą rodzinną (tzw. renta wdowia). Zmiana zawarta w art. 118a ustawy o emeryturach i rentach z FUS umożliwia wydawanie decyzji w sprawach przyznania bądź odmowy tego świadczenia w pełnym procesie automatycznym, bez udziału czynnika ludzkiego. Zmiana została przygotowana na prośbę Prezesa Zakładu Ubezpieczeń Społecznych i w jego ocenie ma charakter pilny.”.

Powyższe pismo nie zawiera jednak analizy wprowadzonych do projektowanej ustawy rozwiązań związanych z pozbawieniem osób fizycznych – wynikającego z art. 22 ust. 1 rozporządzenia 2016/679 – prawa, by nie podlegać

³ Przed skierowaniem do Sejmu RP projektu.

⁴ Ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2025 r. poz. 350), dalej: ustawa o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych.

⁵ Zgodnie z projektowanym art. 108 a ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych:

„1. Decyzja w sprawie świadczenia może być podejmowana w oparciu o wyłącznie zautomatyzowane przetwarzanie danych osobowych, pod warunkiem zapewnienia osobie, której dotyczy podejmowane rozstrzygnięcie, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętego rozstrzygnięcia oraz prawa do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania takiego rozstrzygnięcia. W stosunku do rozstrzygnięć następujących w drodze decyzji osoba, której dotyczy decyzja, może skorzystać z tych uprawnień w terminie miesiąca od dnia doręczenia decyzji.

2. Do decyzji wydanej zgodnie z ust. 1 przepisów odrębnych o konieczności zamieszczenia w decyzji podpisu osoby upoważnionej do wydania decyzji lub nadruku jej imienia i nazwiska nie stosuje się.”.

⁶ Pismo Ministra Rodziny, Pracy i Polityki Społecznej do Sekretarza Rady Ministrów przekazujące projekt ustawy o zmianie ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych oraz niektórych innych ustaw do rozpatrzenia przez Radę Ministrów (znak: DUS-III.0210.5.2024.EO).

decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu ich danych osobowych, w tym profilowaniu. Tymczasem pozbawienie podmiotów danych tego prawa wymaga pogłębionej refleksji projektodawcy, nie tylko w świetle przepisów rozporządzenia 2016/679, ale także pod kątem gwarancji ochrony praw konstytucyjnych, tj. prawa do ochrony danych osobowych (art. 51) i prawa do prywatności (art. 47 Konstytucji RP), czego do tej pory nie uczyniono.

Jednocześnie, pomimo, że projektowany przepis ustawowy jednoznacznie odnosi się do przetwarzania danych osobowych – wbrew dyspozycji art. 51 ustawy o ochronie danych osobowych oraz art. 57 ust. 1 lit. c rozporządzenia 2016/679 – nie został przekazany organowi nadzorcemu celem wydania wymaganej prawem opinii. Nie sposób nie zwrócić uwagi (choć okoliczność ta na etapie parlamentarnego procesu legislacyjnego ma mniejsze znaczenie), iż projektodawca nie wypełnił w tym zakresie także dyspozycji przepisów Regulaminu pracy Rady Ministrów⁷. Warto przy tym podkreślić, że na ustawowe gwarancje dotyczące obowiązku przedstawiania projektowanych regulacji dotyczących danych osobowych do zaopiniowania organowi do spraw ochrony danych osobowych zwrócił uwagę w istotny sposób ostatnio Przewodniczący Komitetu Stałego Rady Ministrów Pan Minister Maciej Berek w piśmie z 31 marca 2025 roku⁸.

Dopiero więc na etapie prac Sejmu RP Prezes Urzędu Ochrony Danych Osobowych może zaopiniować proponowane rozwiązanie i odnieść się do projektowanego modelu przetwarzania danych przez ZUS.

II. Test prywatności.

W ramach przyznawania decyzji w sprawie świadczenia ZUS, na podstawie projektowanego art. 118a, mają być przetwarzane przy pomocy nowych technologii w znacznej ilości i na dużą skalę dane osób fizycznych różnych kategorii, w tym dane zwykłe, dane szczególnych kategorii objęte ochroną na podstawie art. 9 ust. 1

⁷ Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów M. P. z 2024 r. poz. 806).

⁸ Pismo Pana Ministra M. Berka, Przewodniczącego Komitetu Stałego Rady Ministrów z 31 marca 2025 r. znak: DPPR.WPPR.0635.1.2025. W niniejszym piśmie Pan Minister wskazał m.in, że „drugim narzędziem, ustanowionym w przepisach prawa, które ma na celu zagwarantowanie odpowiedniego standardu ochrony danych osobowych w projektowanych regulacjach, jest wyrażony w art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych obowiązek przekazywania założeń i projektów aktów prawnych dotyczących danych osobowych do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych. Dodatkowo kompetencje do opiniowania projektów przekazanych przez Prezesa Urzędu Ochrony Danych Osobowych posiada również Rada do Spraw Ochrony Danych Osobowych. Te ustawowe gwarancje znajdują swoje odzwierciedlenie w przepisach Regulaminu pracy RM. Zgodnie bowiem z § 38 ust. 1 pkt 3 Regulaminu pracy RM każdy projekt dokumentu rządowego, który dotyczy danych osobowych, powinien zostać skierowany do zaopiniowania przez Prezesa Urzędu Ochrony Danych Osobowych. Gwarancję realizacji tego obowiązku stanowi natomiast regulacja § 21a Regulaminu pracy RM, która zobowiązuje Rządowe Centrum Legislacji do weryfikowania wykonania przez organ wnioskujący obowiązków związanych z przekazaniem projektu do zaopiniowania.”.

rozporządzenia 2016/679⁹ (np. dane dotyczące stanu zdrowia ujawniane dla potrzeb przyznania świadczenia), dane dotyczące wyroków skazujących i czynów zabronionych chronione na podstawie art. 10 rozporządzenia 2016/679¹⁰ (np. informacje dotyczące przebywania w zakładach karnych osób objętych świadczeniem), a także numer identyfikacyjny PESEL podlegający ochronie na podstawie i w warunkach określonych w art. 87 rozporządzenia 2016/679¹¹. To oznacza, że **ich przetwarzanie** musi być nie tylko **zgodne z zasadami dotyczącymi przetwarzania danych osobowych ukształtowanymi mocą art. 5 rozporządzenia 2016/679¹²**, ale i **objęte testem**

⁹ Zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

¹⁰ Zgodnie z art. 10 rozporządzenia 2016/679 przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

¹¹ Zgodnie z art. 87 rozporządzenia 2016/679 państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.

¹² Zgodnie z art. 5 ust. 1 rozporządzenia 2016/679 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"). Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679 Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

prywatności wraz z oceną skutków dla ochrony danych (art. 25¹³ i 35 ust. 1¹⁴ rozporządzenia 2016/679). Pozwoliłoby to m.in. zbadać czy projektowane przepisy, zgodnie z art. 6 ust. 3 z rozporządzenia 2016/679, są **proporcjonalne i stanowiące gwarancje odpowiednie do *ratio legis***, tj. do wyznaczonego, prawnie uzasadnionego celu. Istotne jest zatem, aby projektowane przepisy zapewniły stosowanie norm ogólnego rozporządzenia o ochronie danych dla realizacji proponowanych rozwiązań i były przeanalizowane z uwzględnieniem ryzyk towarzyszących operacjom przetwarzania takich danych osobowych, a tym samym dawały gwarancje realizacji praw i wolności osób, których dane dotyczą (podmiotów danych).

Przeprowadzenie testu prywatności pozwoliłoby w szczególności ocenić czy projektowane w przepisach rozwiązanie przewiduje środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą wskazane w art. 22 ust. 2 lit. b rozporządzenia 2016/679 oraz czy środki te są właściwe, co stanowi przesłankę do legalnego stosowania zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach na podstawie prawa państwa członkowskiego.

III. Uwagi szczegółowe.

Projektowany art. 118a określa, że „decyzja w sprawie świadczenia udzielanego przez ZUS może być podejmowana w oparciu o wyłącznie zautomatyzowane przetwarzanie danych osobowych, pod warunkiem zapewnienia osobie, której dotyczy podejmowane rozstrzygnięcie, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętego rozstrzygnięcia oraz prawa do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania takiego rozstrzygnięcia”. Dodatkowo, „w stosunku do rozstrzygnięć następujących w drodze decyzji osoba, której dotyczy decyzja, może skorzystać z tych uprawnień w ograniczonym czasie czyli w terminie miesiąca od dnia doręczenia decyzji”.

¹³ Ust. 1 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. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

¹⁴ 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.

Jak deklaruje w uzasadnieniu projektodawca, statuując w przepisach uprawnienie do podejmowania przez ZUS decyzji w sprawie świadczeń w sposób całkowicie zautomatyzowany, „warunkiem takiego działania jest jednocześnie zapewnienie przez ZUS odpowiednich środków ochrony osobie, której dane są przetwarzane. Należą do nich: warunek zapewnienia osobie, której dotyczy podejmowane rozstrzygnięcie, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji oraz prawa do uzyskania interwencji ludzkiej oraz do wyrażenia własnego stanowiska i do zakwestionowania takiego rozstrzygnięcia. Wskazane prawa są realizowane w sposób wskazany w rozdziale III RODO: Prawa osoby, której dane dotyczą.”.

Z tym stanowiskiem projektodawcy nie można się jednak w pełni zgodzić. Korzystając z możliwości wypowiedzi w odniesieniu do projektu ustawy na etapie sejmowego procesu legislacyjnego **wskazać trzeba, że projektowany art. 118a cechuje się następującymi brakami.**

I. Prezes Urzędu Ochrony Danych Osobowych pragnie przypomnieć, że **ograniczenie prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu należy oceniać w świetle**

standardów RODO, m.in. przez pryzmat art. 23 rozporządzenia 2016/679¹⁵. Jak wynika z ust. 1 ww. przepisu, ograniczenie takie nie może naruszać istoty podstawowych praw i wolności oraz powinno być w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym. Do zagadnienia tego odniosła się Europejska Rada Ochrony Danych w Wytycznych 10/2020 w sprawie ograniczeń na mocy art. 23 RODO,

¹⁵ Zgodnie z art. 23 rozporządzenia 2016/679 1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

- a) bezpieczeństwu narodowemu;
- b) obronie;
- c) bezpieczeństwu publicznemu;
- d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
- e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
- f) ochronie niezależności sądów i postępowania sądowego;
- g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
- h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) - e) oraz g);
- i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
- j) egzekucji roszczeń cywilnoprawnych.

2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej - w stosownym przypadku - o:

- a) celach przetwarzania lub kategorii przetwarzania;
- b) kategoriach danych osobowych;
- c) zakresie wprowadzonych ograniczeń;
- d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
- e) określeniu administratora lub kategorii administratorów;
- f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;
- g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz
- h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Wersja 2.0, przyjętych 13 października 2021 r.¹⁶, określając przesłanki, które powinny być spełnione w teście konieczności i proporcjonalności, którym powinien być objęty projektowany art. 118a. Przepis ten nie pozbawia wprawdzie osób korzystających ze świadczeń ZUS prawa do otrzymania stosownych wyjaśnień co do podstaw podjętego rozstrzygnięcia oraz prawa do uzyskania interwencji ludzkiej, do wyrażenia własnego stanowiska i do zakwestionowania takiego rozstrzygnięcia, niemniej w ocenie organu nadzorczego nie można uznać tych środków za wystarczające, konieczne i proporcjonalne w rozumieniu rozporządzenia 2016/679 i zgodne z ww. Wytocznymi EROD.

II. Aby można było przyjąć, że ustawodawca realizuje w pełni zasadę legalizmu: zgodności z prawem, rzetelności i przejrzystości (art. 5 ust.1 lit. a) **art. 118a powinien zostać rozbudowany o szczegółowe wskazania:**

- 1) zgodnie z art. 23 ust. 2 lit. a rozporządzenia 2016/679 o wskazanie w jakich konkretnie **celach** w oparciu o wyłącznie zautomatyzowane przetwarzanie danych osobowych w związku z wydawaniem decyzji w sprawie świadczenia udzielanego przez ZUS, oraz
- 2) zgodnie z art. 23 ust. 2 lit. b rozporządzenia 2016/679 o wskazanie, jakie **kategorie danych osobowych** będą na podstawie tego przepisu przetwarzane, w oparciu o jakie kategorie danych dotyczących osoby fizycznej mają być wydawane decyzje w ramach zautomatyzowanego przetwarzania danych osobowych w konkretnych procedurach.

III. Dla zautomatyzowanego przetwarzania mogą być przez ZUS wykorzystywane dane osobowe jedynie **adekwatne i niezbędne** do wydania decyzji w sprawie świadczenia – w tym aspekcie wymagane jest od ZUS postępowanie zgodne z zasadami: ograniczenia celu, minimalizacji danych czy rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679). Projektodawca powinien także **rozważyć odstąpienie od wykorzystywania do zautomatyzowanego przetwarzania danych o charakterze sensytywnym** (dane określone w art. 9 ust. 1 i art. 10 rozporządzenia 2016/679),

¹⁶ We wskazanym dokumencie EROD podkreśla, że test konieczności i proporcjonalności zazwyczaj oznacza ocenę zagrożeń dla praw i wolności osób, których dane dotyczą. Zgodnie z zasadą proporcjonalności treść aktu ustawodawczego nie może wykraczać poza to, co jest absolutnie niezbędne do ochrony celów wymienionych w art. 23 ust. 1 lit. a)–j) RODO. Ograniczenie to powinno zatem być odpowiednie do osiągnięcia uzasadnionych celów, do których dąży sporne uregulowanie, i nie wykraczać poza to, co jest właściwe i konieczne do osiągnięcia tych celów. Zgodnie z orzecznictwem TSUE art. 23 RODO nie może być interpretowany jako mogący przyznawać państwom członkowskim uprawnienie do naruszania poszanowania życia prywatnego, z naruszeniem art. 7 karty lub jakiegokolwiek z innych gwarancji w niej zawartych. W szczególności uprawnienie przyznane państwom członkowskim na mocy art. 23 ust. 1 RODO może być wykonywane wyłącznie zgodnie z wymogiem proporcjonalności, zgodnie z którym odstępstwa i ograniczenia w odniesieniu do ochrony danych osobowych muszą mieć zastosowanie wyłącznie w zakresie, w jakim jest to bezwzględnie konieczne. Proponowany środek ograniczający powinien być poparty dowodami opisującymi problem, który ma zostać rozwiązany w ramach tego środka, sposobu jego rozwiązania oraz tego, dlaczego istniejące lub mniej inwazyjne środki nie są w stanie rozwiązać tego problemu w wystarczającym stopniu. Istnieje również wymóg wykazania, w jaki sposób proponowana ingerencja lub ograniczenia rzeczywiście spełniają cele leżące w ogólnym interesie państwa i UE lub potrzebę ochrony praw i wolności innych osób. Ograniczenie praw do ochrony danych będzie musiało koncentrować się na konkretnych zagrożeniach.

wprowadzając do projektowanej ustawy stosowne ograniczenia (zob. art. 22 ust. 4 rozporządzenia 2016/679)¹⁷. Jako przykład takich rozwiązań można wskazać art. 105a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2024 r. poz. 1646 ze zm.).

IV. ZUS jako państwowa jednostka organizacyjna działa na podstawie ustaw¹⁸. Jego zadania i sposoby realizacji tych zadań powinny odbywać się więc na podstawie i w granicach prawa, co wynika z zasady legalizmu określonej w art. 7 Konstytucji RP. W demokratycznym państwie prawa ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być wprowadzane z kolei jedynie, gdy są one konieczne, jak wskazuje treść art. 31 ust. 3 Konstytucji RP. **Projektowane rozwiązania ustawowe powinny być zatem rozbudowane co najmniej o:**

- sposoby i narzędzia dotyczące przetwarzania danych osobowych oraz wskazanie, jaki podmiot odpowiada za nie w związku z zautomatyzowanym przetwarzaniem danych w celu wydania decyzji w sprawie świadczenia udzielanego przez ZUS. Ma to szczególnie istotne znaczenie w dobie korzystania z nowych technologii, przetwarzania maszynowego i stosowaniu rozwiązań o różnym stopniu ryzyka. Rozważeniu powinno podlegać stosowanie mechanizmów objętych Aktem w sprawie sztucznej

¹⁷ Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

¹⁸ Art. 66 ust. 1 i 3 z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2025 r. poz. 350).

inteligencji¹⁹, z uwzględnieniem jego art. 27, także ust. 4 tego przepisu²⁰, tj. oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych.

- regulacje postępowania kształtujące sposoby realizacji praw wskazanych w projektowanym art. 118a ustawy, skoro warunkują one możliwość podejmowania decyzji w sprawie świadczenia w oparciu o wyłącznie zautomatyzowane przetwarzanie danych osobowych, tak, by w ramach tego postępowania nie było realnego zagrożenia, iż osoba, której dane dotyczą, nie będzie mogła zastosować środków ochrony swoich praw, np. w wyniku braku wiedzy o przysługujących jej prawach, faktycznych możliwości skorzystania z nich (wykluczenie cyfrowe), tego w jaki konkretnie sposób może ze środków tych skorzystać.

V. Kolejnym istotnym brakiem projektowanej regulacji jest niewskazanie jak osobie, której dotyczy podejmowane rozstrzygnięcie, zapewniane będą w praktyce przez ZUS prawa wynikające z rozporządzenia 2016/679, tj.:

¹⁹ 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).

²⁰ Przed wdrożeniem systemu AI wysokiego ryzyka, o którym mowa w art. 6 ust. 2, z wyjątkiem systemów AI wysokiego ryzyka przeznaczonych do stosowania w obszarze wymienionym w załączniku III pkt 2, podmioty stosujące będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b) i c), przeprowadzają ocenę skutków w zakresie praw podstawowych, jakie może wywołać wykorzystanie takiego systemu. W tym celu podmioty stosujące przeprowadzają ocenę obejmującą:

a) opis procesów podmiotu stosującego, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem;

b) opis okresu, w którym każdy system AI wysokiego ryzyka ma być wykorzystywany i opis częstotliwości tego wykorzystywania;

c) kategorie osób fizycznych i grup, na które może mieć wpływ wykorzystywanie systemu;

d) szczególne ryzyko szkody, które może mieć wpływ na kategorie osób fizycznych lub grupy osób zidentyfikowane zgodnie z lit. c) niniejszego ustępu, z uwzględnieniem informacji przekazanych przez dostawcę zgodnie z art. 13;

e) opis wdrożenia środków nadzoru ze strony człowieka, zgodnie z instrukcją obsługi;

f) środki, jakie należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym ustalenia dotyczące zarządzania wewnętrznego i mechanizmów rozpatrywania skarg.

2. Obowiązek ustanowiony w ust. 1 ma zastosowanie do wykorzystania systemu AI wysokiego ryzyka po raz pierwszy. W podobnych przypadkach podmiot stosujący może polegać na wcześniej przeprowadzonych ocenach skutków dla praw podstawowych lub na istniejących ocenach skutków przeprowadzonych przez dostawcę. Jeżeli w trakcie wykorzystania systemu AI wysokiego ryzyka podmiot stosujący uzna, że którykolwiek z elementów wymienionych w ust. 1 uległ zmianie lub nie jest już aktualny, podmiot ten podejmuje niezbędne kroki w celu aktualizacji informacji.

3. Po przeprowadzeniu oceny, o której mowa w ust. 1 niniejszego artykułu, podmiot stosujący powiadamia organ nadzoru rynku o jej wynikach, przedkładając jako element tego powiadomienia wypełniony wzór, o którym mowa w ust. 5 niniejszego artykułu. W przypadku, o którym mowa w art. 46 ust. 1, podmioty stosujące mogą zostać zwolnione z obowiązku dokonania powiadomienia.

4. Jeżeli którykolwiek z obowiązków ustanowionych w niniejszym artykule został już spełniony w wyniku oceny skutków dla ochrony danych przeprowadzonej zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680, ocena skutków w zakresie praw podstawowych, o której mowa w ust. 1 niniejszego artykułu, stanowi uzupełnieniem tej oceny skutków dla ochrony danych.

5. Urząd ds. AI opracowuje wzór kwestionariusza, w tym za pomocą zautomatyzowanego narzędzia, aby ułatwić podmiotom stosującym spełnianie ich obowiązków wynikających z niniejszego artykułu w sposób uproszczony.

- 1) prawo do otrzymania stosownych wyjaśnień co do podstaw podjętego rozstrzygnięcia,
 - 2) prawo do uzyskania interwencji ludzkiej,
 - 3) prawo do wyrażenia własnego stanowiska,
 - 4) prawo do zakwestionowania takiego rozstrzygnięcia.
- Odpowiedzi w tym zakresie nie przynosi także treść uzasadnienia projektu.

VI. Wzgląd na zasady: przejrzystości, integralności i poufności, a także rozliczalności oraz art. 23 ust. 2 lit. d rozporządzenia 2016/679 wymaga również **poszerzenia projektowanych przepisów o szczegółowe rozwiązania wprowadzające standardy techniczne i organizacyjne gwarantujące bezpieczeństwo przetwarzanych w ramach zautomatyzowanego podejmowania decyzji danym osobowym.** W Wytycznych Grupy Roboczej art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679²¹ podkreślono bowiem, że „administratorzy powinni przeprowadzać częste oceny zbiorów danych, które przetwarzają, pod kątem występowania elementów stronniczości i opracować sposoby wyeliminowania elementów szkodliwych, w tym przypadków nadmiernego polegania na korelacjach. Innymi przydatnymi środkami są systemy, w ramach których przeprowadza się audyty algorytmów oraz regularne przeglądy prawidłowości i adekwatności zautomatyzowanego podejmowania decyzji, w tym profilowania.”. Nie bez znaczenia jest także aspekt cyberbezpieczeństwa przetwarzanych w sposób zautomatyzowany danych – jego zagwarantowanie przyczynia się dla ochrony danych osobowych.

VII. W ocenie organu nadzorczego projektodawca powinien więc rozważyć rozbudowę projektu ustawy o przepisy, które określiłyby szczegółowe rozwiązania w zakresie technicznych i organizacyjnych aspektów zautomatyzowanego przetwarzania danych osobowych w ramach wydawania decyzji przez ZUS. Takie przepisy powinny określać standardy mające gwarantować integralność, poufność i prawidłowość danych, a także dookreślać procedury przetwarzania tych danych, w tym także ich zabezpieczania i usuwania.

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,

²¹ Wytyczne grupy roboczej art. 29 w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE, Przyjęte w dniu 3 października 2017 r., Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r., WP251rev.01.

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan Maciej Berek
Minister
Członek Rady Ministrów
Przewodniczący Komitetu Stałego Rady Ministrów
ePUAP: /eKPRM/SkrytkaESP

Pani Agnieszka Dziemianowicz-Bąk
Ministra Rodziny, Pracy i
Polityki Społecznej
ePUAP: /4g447ytes7/skrytka

Pan Zbigniew Derdziuk
Prezes Zakładu Ubezpieczeń Społecznych
ePUAP: /ZUS/SkrytkaESP