



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 13-03-2025

DPNT.401.81.2025.WL.OJ

**Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji**

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazaniem do wiadomości organu nadzorczego pismem z 6 marca 2025 r. (znak: DPiS.WWKS.002.42.1.2025), dotyczącym **projekt ustawy o zmianie ustawy o systemie ubezpieczeń społecznych oraz niektórych innych ustaw (UD114)**

(dalej: „projekt”), skierowanego do zaopiniowania przez osoby uczestniczące w posiedzeniach Komitetu Rady Ministrów do spraw Cyfryzacji, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ (dalej: „rozporządzenie 2016/679”) oraz art. 51 ustawy o ochronie danych osobowych², Prezes UODO jako organ nadzorczy zgłasza następujące uwagi.

Poprzednia wersja projektu ustawy o zmianie ustawy o systemie ubezpieczeń społecznych oraz niektórych innych ustaw (projekt z 22 października 2024 r.) była przedmiotem pogłębionej analizy i opinii organu nadzorczego, ponieważ wprowadzała nowy model przetwarzania danych osobowych dla wydawania orzeczeń i kontroli zaświadczeń lekarskich przez Zakład Ubezpieczeń Społecznych (ZUS), w tym przy użyciu nowych technologii oraz pozyskiwana dokumentacji medycznej w formie elektronicznej. Projektowana ustawa zawierała także rozwiązania umożliwiające

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

przetwarzanie przez ZUS danych biometrycznych za pomocą rozwiązań wykorzystujących sztuczną inteligencję³.

Przekazany na Komitet Rady Ministrów do spraw Cyfryzacji projekt ustawy (**projekt z 3 marca 2025 r.**), jak wynika z załączonego do zgłoszonego projektu dokumentu „Zestawienie uwag z konsultacji publicznych i opiniowania”⁴, **uwzględnia znaczną część uwag organu nadzorczego**. W szczególności – jak wskazuje projektodawca – z projektu ustawy usunięte zostały regulacje przewidujące automatyzację połączeń telefonicznych dotyczących zawiadomienia o terminie badania przy zastosowaniu technologii wykorzystującej automatyczne przetwarzanie danych osobowych (tzw. voicebotów), a zatem ewentualne przetwarzanie danych biometrycznych w związku z nagrywaniem rozmów telefonicznych. W aktualnym projekcie ustawy zrezygnowano także z przepisów w zakresie pozyskiwania za pośrednictwem systemu informacji w ochronie zdrowia – a zatem bez udziału podmiotów udzielających świadczeń zdrowotnych – informacji o zdarzeniach medycznych zawartych w art. 85g poprzedniej wersji projektu.

Dodatkowo, projektodawca przedstawił wyjaśnienia odnośnie do uregulowanego w projektowanej ustawie narzędzia technologicznego w postaci certyfikatu umożliwiającego podpisywanie dokumentów elektronicznych z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym ZUS (dalej: jako certyfikat) oraz kwestionowanego wcześniej przez organ nadzorczy projektowanego art. 56 ust. 5 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, wskazując uzasadnienie dla sposobu udostępnienia danych osobowych na podstawie projektowanego przepisu.

Biorąc pod uwagę powyższe Prezes Urzędu Ochrony Danych Osobowych dziękuje za uwzględnienie uwag do projektowanej ustawy i korektę jej rozwiązań dokonaną przez projektodawcę.

Niemniej należy wskazać, że wejście w życie projektowanych rozwiązań w dalszym ciągu będzie się wiązało się z przetwarzaniem **znacznej ilości i na dużą skalę** danych osób fizycznych, w tym **danych szczególnych kategorii** (w rozumieniu w art. 9 ust 1 rozporządzenia 2016/679⁵), podlegających wzmocnionej ochronie prawnej, w tym danych dotyczących stanu zdrowia. **Na podstawie projektowanych przepisów będą też przetwarzane w systemach informatycznych informacje objęte tajemnicą prawnie chronioną, zawarte w dokumentacji medycznej oraz krajowy numer identyfikacyjny PESEL**, podlegający ochronie na podstawie i w warunkach określonych

³ Opinia Prezesa Urzędu Ochrony Danych Osobowych do projektu ustawy o zmianie ustawy o systemie ubezpieczeń społecznych oraz niektórych innych ustaw z 22 listopada 2024 r. znak: DOL.401.430.2024.WL.OJ.

⁴ Zob. Pkt nr: 1, 10, 32, 52 dokumentu „Zestawienie uwag z konsultacji publicznych i opiniowania”.

⁵ 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.

w art. 87 rozporządzenia 2016/679⁶. Podobnie należy podkreślić, że pomimo Państwa wyjaśnień, że certyfikat, o którym mowa w projektowanym art. 68b ustawy o systemie ubezpieczeń społecznych, jest już w praktyce wykorzystywany od 1 grudnia 2018 r. do podpisywania elektronicznych zaświadczeń lekarskich o czasowej niezdolności do pracy, to w istocie z Państwa odpowiedzi nie wynika czy projektowane rozwiązanie było objęte oceną skutków dla ochrony danych, a także jakie zastosowano rozwiązania, by certyfikat ZUS oferował odpowiednie mechanizmy zabezpieczające dane osobowe oraz integralność i autentyczność podpisywanych dokumentów a także gwarancje w zakresie cyberbezpieczeństwa. Uzasadnienie projektu lub dokument oceny skutków regulacji powinien zostać uzupełniony o tę informację.

Prezes Urzędu Ochrony Danych Osobowych w dalszym ciągu uznaje więc za zasadne objęcie w toku procesu legislacyjnego zawartych w projekcie rozwiązań dotyczących przetwarzania danych osobowych, w tym dotyczących ww. certyfikatu, **testem prywatności, w tym oceną skutków dla ochrony danych** (art. 35 rozporządzenia 2016/679), co ułatwiłaby projektodawcy przeprowadzenie analizy niezbędności wprowadzenia określonych rozwiązań tak, by stworzyć regulacje z poszanowaniem zasad przetwarzania danych osobowych i in. przepisów rozporządzenia 2016/679⁷. Taki test pozwoliłby ocenić czy rozwiązania zawarte w projekcie przewidują jednocześnie odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą – co przy projektowanych rozwiązaniach związanych z przetwarzaniem danych sensytywnych dotyczących stanu zdrowia – należy uznać za konieczne.

Jednocześnie pragnę zauważyć, 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

⁶ 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.

⁷ 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").

za zapewnienie ich zgodności z przepisami o ochronie danych osobowych. Organ nadzorczy wyraża 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

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pani

Agnieszka Dziemianowicz-Bąk

Ministra Rodziny, Pracy i

Polityki Społecznej

ePUAP

/4g447ytes7/skrytka