Warszawa, 30.04.2025 r.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

DPNT.401.101.2025

Pan
Izabela Leszczyna
Minister Zdrowia
Ministerstwo Zdrowia

Szanowna Pani Minister,

w odpowiedzi na pismo z 21 marca br. (znak: DIWP.0210.5.2024), w związku z przedłożeniem do zaopiniowania projektu ustawy **o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych i niektórych innych ustaw** (UD169; dalej jako „projekt"), 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], uprzejmie przedstawiam następujące uwagi.

1. Projekt ustawy zakłada prowadzenie centralnej elektronicznej rejestracji, w której będą przetwarzane, **za pomocą systemu informatycznego**, **w szerokim zakresie dane osobowe** osób fizycznych, w tym **dane mogące być przetwarzane biometrycznie** (pozyskiwane, w tym nagrywane, z wykorzystaniem asystenta głosowego) i **dane dotyczące zdrowia**. Projektodawca przewiduje bowiem, że centralna elektroniczna rejestracja będzie obejmowała dane dotyczące usługobiorców, o których mowa w ustawie o systemie informacji w ochronie zdrowia[3] (projektowany **art. 23c ust. 8 w zw. z art. 23 ust. 3**), dane zawarte w centralnym

---

[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 jako „rozporządzenie 2016/679.
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[3] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia; tj. usługobiorców o których mowa w art. 4 ust. 3 pkt 1 lit. a, b, g, i, n, o ustawy o systemie informacji w ochronie zdrowia (imię i nazwisko, nazwisko rodowe, numer PESEL lub seria i numer paszportu albo innego dokumentu stwierdzającego tożsamość albo niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji, w przypadku osób, które nie mają nadanego numeru PESEL, informację o posiadaniu orzeczenia o niepełnosprawności albo orzeczenia o stopniu niepełnosprawności; informacje o uprawnieniach dodatkowych).

wykazie oczekujących[4] (projektowany **art. 23c ust. 8 w zw. z art. 23 ust. 6**), dane zawarte w zgłoszeniu centralnym stanowiącym oświadczenie świadczeniobiorcy o zamiarze uzyskania wybranego świadczenia opieki zdrowotnej[5] (projektowany **art. 23c ust. 8 w zw. z art. 23d ust. 3**). Jednocześnie – co istotne – projekt przewiduje, że centralna elektroniczna rejestracja jest prowadzona z wykorzystaniem **asystenta głosowego** (projektowany **art. 23f ust. 1**). Jak wynika z projektowanego **art. 23f ust. 2** nagrania dźwięku lub transkrypcja nagrania uzyskane w wyniku prowadzenia centralnej elektronicznej rejestracji z wykorzystaniem asystenta głosowego, o którym mowa w ust. 1, zawierające dane, o których mowa w art. 23c ust. 8, minister właściwy do spraw zdrowia przetwarza wyłącznie do celów, dla których zostały one zebrane, i przechowuje przez okres nie dłuższy niż 5 lat licząc od końca roku kalendarzowego, w którym nagranie zostało zarejestrowane.

Jak wskazano w uzasadnieniu, „w założeniu projektodawcy system ten ma pozwolić na uproszczenie i przyspieszenie procesu rejestracji na świadczenia opieki zdrowotnej oraz zapewnić świadczeniobiorcom łatwiejszy dostęp do informacji o dostępności terminów u wszystkich świadczeniodawców".

Ze względu na planowane stosowanie technologii, sposób, zakres i charakter przetwarzanych danych **niezwykle istotne jest** – stosownie do zasad i wymagań rozporządzenia 2016/679 – aby projektowane przepisy przewidywały rozwiązania adekwatne do celów, konieczne i jedynie niezbędne dla realizacji *ratio legis*, a także przewidywały właściwe gwarancje ochrony danych osobowych dla podmiotów danych.

1.1. Zgodnie z art. 5 ust. 1 lit a w zw. z art. 6 ust. 1 lit e oraz art. 6 ust. 3 rozporządzenia 2016/679 w związku z art. 7 Konstytucji RP, podstawa przetwarzania danych osobowych powinna być określona – w sposób **jasny i precyzyjny** – w przepisach ustawy. Te zasady fundamentalne mają szczególne znaczenie w przypadkach przetwarzania danych przez podmioty publiczne, czy w celach publicznych. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e), musi być ono **niezbędne** do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[6].

Dane dotyczące zdrowia oraz dane biometryczne – zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 – należą do danych szczególnych kategorii, należy więc mieć na względzie, że ich przetwarzanie wymaga zachowania szczególnego reżimu,

---

[4] M.in. dane świadczeniobiorców, o których mowa a art. 20 ust. 2 pkt 3 lit. b-h ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych: imię i nazwisko świadczeniobiorcy, numer PESEL, a w przypadku jego braku - serię i numer paszportu lub innego dokumentu potwierdzającego tożsamość świadczeniobiorcy, rozpoznanie lub powód przyjęcia, adres świadczeniobiorcy, numer telefonu lub adres poczty elektronicznej służący do komunikacji ze świadczeniobiorcą lub jego opiekunem; a także dane diagnostyki i leczenia onkologicznego, dane pracownika medycznego, dane zawarte w skierowaniu.

[5] Dane świadczeniobiorcy, informacje o kategorii medycznej, inne dane dotyczące zdrowia; projektowany.

[6] Zob. wyrok TSUE z 9 marca 2017 r., Manni, C 398/15, podobnie wyrok z 22 czerwca 2021 r., Latvijas Republikas Saeima (Punkty karne), C 439/19, i przytoczone tam orzecznictwo.

w tym mogą być przetwarzane wyłącznie w przypadkach, gdy jest to **niezbędne** do realizacji konkretnych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa oraz po zapewnieniu gwarancji wymaganych art. 9 ust. 2 i 3 rozporządzenia 2016/679.

Odstępstwa od prawa do ochrony danych osobowych i prawa do prywatności – gwarantowane w art. 7 i 8 Karty praw podstawowych UE oraz art. 47 i 51 Konstytucji RP – powinny mieć podstawę ustawową i ograniczać się do tego, co absolutnie konieczne[7]. Klauzule ograniczeń wynikają zaś z art. 31 ust. 3, art. 51 ust. 2 Konstytucji RP oraz art. 52 ust. 1 Karty praw podstawowych.

1.2. Odnosząc się do **charakteru** przetwarzanych danych należy zauważyć, że projektodawca przewiduje automatyzację połączeń telefonicznych dotyczących dokonywania rejestracji w centralnej elektronicznej rejestracji przy zastosowaniu technologii wykorzystującej automatyczne przetwarzanie danych osobowych, tzw. voicebotów, a zatem wątpliwości budzi, czy w takim przypadku będzie dochodziło do przetwarzania danych biometrycznych w związku z nagrywaniem rozmów telefonicznych (projektowany art. 23f). Jak wyjaśniono w uzasadnieniu, „usługa asystenta głosowego (voicebot) przypomni o zbliżającej się wizycie, potwierdzi obecność pacjenta na wizycie, a w razie konieczności przełoży lub anuluje wizytę. Celem implementacji tego rozwiązania jest zaoferowanie usług wzmacniających komunikację i interakcję świadczeniobiorcy w obszarze zapisu na świadczenia opieki zdrowotnej z wykorzystaniem usług centralnej elektronicznej rejestracji, w szczególności w przypadku świadczeniobiorców wykluczonych cyfrowo".

Zautomatyzowane przetwarzania danych, w tym danych biometrycznych, jest **wyjątkowo inwazyjną formą przetwarzania danych osobowych**, która jest obarczona **bardzo wysokim ryzykiem naruszenia praw i wolności osób nagrywanych.** Analiza unikalnej cechy biometrycznej, jaką jest głos człowieka, pozwala bowiem nie tylko dokonać jego identyfikacji, ale może pomóc w określeniu m.in. jego stanu emocjonalnego, chorób, na które dana osoba cierpi czy określić jego wiek i płeć. Należy przy tym mieć na względzie, że automatyczne przetwarzanie danych za pomocą tzw. voicebotów jest narzędziem w istocie wspieranym sztuczną inteligencją. W asystencie głosowym może więc dochodzić do specjalnego przetwarzania głosu osób fizycznych użytkujących system.

Brak jest przy tym wyjaśnienia, czy przetwarzanie danych będzie się rzeczywiście opierać na identyfikacji lub weryfikacji osoby fizycznej przez asystenta głosowego, co mogłoby prowadzić do zastosowania nieproporcjonalnych środków w odniesieniu do realizacji zakładanego przez projektodawcę celu i konieczność zastosowania środków prawnych dotyczących przetwarzania danych biometrycznych. Należy w tym miejscu przypomnieć, że w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie

[7] Zob. też np. wyrok TK z 20 stycznia 2015 r., sygn. akt K 39/12 oraz wyrok TK z 20 listopada 2002 r., sygn. akt K 41/02; a także wyrok TSUE z 9 listopada 2010 r., Volker und Markus Schecke i Eifert, w sprawach C-92/09 i C-93/09.

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), w motywie 39 podkreślono, że „wszelkie przetwarzanie danych biometrycznych i innych danych osobowych związane z wykorzystaniem systemów AI do identyfikacji biometrycznej, inne niż w związku z wykorzystywaniem systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej w celu ścigania przestępstw zgodnie z przepisami niniejszego rozporządzenia, powinno pozostawać zgodne z wymogami wynikającymi z art. 10 dyrektywy (UE) 2016/680. Do celów innych niż ściganie przestępstw art. 9 ust. 1 rozporządzenia (UE) 2016/679 i art. 10 ust. 1 rozporządzenia (UE) 2018/1725 **zakazują przetwarzania danych biometrycznych** z 11 uwzględnieniem ograniczonej liczby wyjątków określonych w tych artykułach. W ramach stosowania art. 9 ust. 1 rozporządzenia (UE) 2016/679 wykorzystywanie zdalnej identyfikacji biometrycznej do celów innych niż ściganie przestępstw było już przedmiotem decyzji zakazujących takiego wykorzystywania, wydawanych przez krajowe organy ochrony danych”[8].

Projektowane rozwiązanie należy więc także ocenić z punktu widzenia ww. aktu prawnego, w tym konieczne jest **przeprowadzenie oceny skutków regulacji zakresie praw podstawowych**, o której mowa w art. 27 aktu w sprawie sztucznej inteligencji.

Niezależnie od powyższego należy zwrócić uwagę, że projektowane przepisy dotyczące automatycznego przetwarzania danych osobowych osób korzystających z centralnej elektronicznej rejestracji **nie zawierają rozwiązań dotyczących sposobów i procedur przetwarzania tych danych,** w tym danych dotyczących zdrowia**, a także ich zabezpieczania** (np. brak regulacji w zakresie sposobu dokonywania identyfikacji świadczeniobiorcy).

Brak jest również regulacji dotyczących realizacji praw osób fizycznych, takich jak prawa do sprostowania danych, dostępu do danych, usunięcia danych oraz innych **instrumentów ochrony praw osób fizycznych**, takich jak prawa do interwencji ludzkiej, kontroli przez człowieka.

Zgodnie z art. 22 rozporządzenia 2016/679 każdej osobie fizycznej przysługuje prawo do niepodlegania decyzjom opartym wyłącznie o zautomatyzowane przetwarzanie danych, w tym profilowanie, które wywołują wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływają. W przypadku podejmowania takich decyzji, które opierają się na szczególnych kategoriach danych, art. 22 ust. 2b i art. 22 ust. 4 rozporządzenia 2016/679, przewiduje konieczność zastosowania art. 9 ust. 2 lit. a) lub g) oraz zapewnienia właściwych środków

---

[8] Zob. też oświadczenie Europejskiej Rady Ochrony Danych (EROD) i Europejskiego Inspektora Ochrony Danych (EIOD) z 18 kwietnia 2021 r. wzywające do zakazu wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej oraz niektórych innych zastosowań sztucznej inteligencji, które mogą prowadzić do niesprawiedliwej dyskryminacji: https://www.edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_pl

ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą[9].

Z uwagi zatem na potrzebę zapewnienia ochrony praw świadczeniobiorców i wysokiego poziomu dostępności i dokładności systemu należy wskazać, że **w przypadku nieskutecznego dialogu z asystentem głosowym projektodawca powinien przewidzieć instrumenty zapewniające właściwe środki ochrony tych praw**, w tym prawa do interwencji ludzkiej, tak, aby zapewnić dostęp do usługi w inny sposób, np. przez połączenie z infolinią obsługiwaną przez człowieka (usługa „chcę rozmawiać z człowiekiem").

Projektowane przepisy – jako mogące głęboko ingerować w prywatność osób fizycznych korzystających z usługi centralnej elektronicznej rejestracji oraz zagrażające realizacji zasad dotyczących przetwarzania danych osobowych: przejrzystości i legalizmu (5 ust. 1 lit. a rozporządzenia 2016/679), ograniczenia celu (5 ust. 1 lit. b rozporządzenia 2016/679) minimalizacji danych (5 ust. 1 lit. c rozporządzenia 2016/679) integralności i poufności (5 ust. 1 lit. f rozporządzenia 2016/679) ograniczenia przechowania (5 ust. 1 lit. e rozporządzenia 2016/679) oraz rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679), także nie zapewniające odpowiednich środków chroniących prawa osób fizycznych – budzą poważne wątpliwości Prezesa UODO.

---

[9] Zgodnie z art. 22 zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie 1. 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. 2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) 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; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą. 3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. 4. 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
Zgodnie z art. 9 ust. 1. 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. 2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków: a) osoba, której dane dotyczą, **wyraziła wyraźną zgodę** na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; g) przetwarzanie jest **niezbędne** ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
Należy przy tym zauważyć, jak wskazał TSUE w wyroku z 7 grudnia 2023 r., C-634/21 dotyczącym wykładni art. 22 rozporządzenia 2016/679, status „decyzji", o której mowa w tym przepisie, należy przyznać już samej zautomatyzowanej ocenie osoby fizycznej, dokonanej przez inny podmiot (w tym przypadku przez biura informacji kredytowej) niż rzeczywisty decydent (bank).

1.3. Istotnym narzędziem oceny proporcjonalności i niezbędności projektowanych rozwiązań oraz szacowania ryzyk towarzyszących takiemu przetwarzaniu dla praw i wolności podmiotów danych, jest **ocena skutków regulacji dla ochrony danych**, do której przeprowadzenia zobowiązuje art. 35, w szczególności, w procesie tworzenia prawa ust. 10 rozporządzenia 2016/679 oraz art. 25 ust. 1 i 2 rozporządzenia 2016/679. Przeprowadzenie oceny skutków ułatwiła także wykazanie zgodności z dotyczącymi przetwarzania danych osobowych zasadami wynikającymi z art. 5 rozporządzenia 2016/679 a także wykazanie spełnienia warunków przetwarzania danych osobowych określonych w art. 6 ust. 3 i art. 9 ust. 2 i 3. Ocena taka pozwala ocenić czy rozwiązania zawarte w projekcie przewidują jednocześnie odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Odnotować przy tym należy – jak wynika z dołączonych do projektu dokumentów – że projektodawca dokonał analizy skutków regulacji dla ochrony danych. Niemniej jednak zauważyć trzeba, że **przeprowadzona analiza budzi zastrzeżenia**. Przetwarzanie danych na podstawie projektowanych regulacji ma bowiem nastąpić za pomocą zautomatyzowanych systemów i dotyczyć ma szerokiego zakresu danych, w tym danych szczególnych kategorii, a zatem **z dużym prawdopodobieństwem należy uznać, że takie przetwarzanie danych powodować może wysokie ryzyko naruszenia praw lub wolności osób fizycznych**. Z analizy dołączonej do projektu wynika zaś, że ryzyko przetwarzania projektodawca oszacował jako niskie i nie przewidział żadnych gwarancji ochrony danych osobowych.

Przeprowadzenie oceny skutków regulacji dla ochrony danych na etapie projektowania regulacji dotyczących przetwarzania danych osobowych powinno prowadzić do wykazania **niezbędności przetwarzania danych osobowych, w określony sposób**, we wskazanym konkretnie celu i zakresie oraz oceny ryzyka projektowanych rozwiązań w zakresie przetwarzania danych osobowych, a w konsekwencji wpływu na prywatność osób fizycznych. Projektodawca nie wykazał natomiast, aby konieczne było przetwarzania wszystkich kategorii danych, w szczególności nie wyjaśnił kwestii przetwarzania danych biometrycznych, dotyczących wszystkich usługobiorców, we wskazanym celu jakim ma być łatwiejszy dostęp do informacji o dostępności terminów u wszystkich świadczeniodawców. Brak jest również wykazania zgodności z przepisami rozporządzenia 2016/679, w tym zasadą rozliczalności (art. 5 ust. 2), a także spełnienia warunków przetwarzania danych osobowych określonych w art. 6 ust. 3 i art. 9 ust. 2 i 3 rozporządzenia 2016/679 oraz odpowiednich gwarancji - zabezpieczeń praw i wolności osób, których dane dotyczą, w tym prawa niepodlegania decyzjom o których mowa w art. 22 rozporządzenia 2016/679.

W związku z powyższym, należy uznać, że **projektodawca nie wykazał w wystarczający sposób niezbędności przetwarzania danych osób fizycznych w przyjęty w tych regulacjach sposób** dla realizacji zakładanego celu.

2. Jednocześnie należy wskazać – stosownie do zasady legalności, o której mowa w art. 5 ust. 1 lit. a rozporządzenia 2016/679 – że **dookreślenia i doprecyzowania wymagają przepisy** odnoszące się do zakresu przetwarzania danych w centralnej elektronicznej rejestracji, a także trybu ich pozyskiwania.

Projektodawca wskazuje w projektowanym **art. 23c ust. 6**, że centralny wykaz oczekujących zawiera „dane dotyczące karty diagnostyki i leczenia onkologicznego", zgłoszenie centralne „inne dane dotyczące stanu zdrowia świadczeniobiorcy lub dane dotyczące świadczenia opieki zdrowotnej istotne do przyjęcia centralnego zgłoszenia, jeżeli dotyczą", **bez określenia jakie konkretne dane będą gromadzone w przedmiotowych wykazach**. Projektodawca nie wskazuje jaki konkretnie katalog danych dotyczących zdrowia będzie przetwarzany w tym rejestrze w odniesieniu do celu regulacji, jakim jest rejestracja wizyty u lekarza. Tak sformułowane regulacje **stwarzają ryzyko przetwarzania nadmiarowych danych osobowych** w projektowanym systemie (art. 5 ust. 1 lit. a, b, c rozporządzenia 2016/679), dlatego wskazane jest sprecyzowanie jakie konkretnie dane będą w tym celu przetwarzane.

Ponadto w **art. 23c ust. 3** projektodawca wskazuje, że świadczeniodawca ma „udostępnić" w systemie teleinformatycznym harmonogramy przyjęć prowadzone przez świadczeniodawców oraz „przekazywać" do systemu teleinformatycznego dane usługobiorców. Projektodawca **nie precyzuje jednak trybu w jakim ma nastąpić udostępnienie danych** do centralnej elektronicznej rejestracji. Art. 24 i 32 rozporządzenia 2016/679 nakłada natomiast na projektodawcę obowiązek zaprojektowania takich rozwiązań prawnych, w tym trybu udostępniania i pozyskiwania, które zapewnią odpowiednią ochronę danych osobowych eliminując ryzyka dla dowolnego przetwarzania danych przez osoby nieuprawnione lub niezgodnie z celem ich uzyskania (por. wyrok NSA z 3 grudnia 2021 r., III OSK 590/21)[10].

Jednocześnie zauważyć należy, że w **projektowanym art. 59b ust. 1 pkt 5a i 5b, 6a-f, 7, 9, 13** przewidziano poszerzenie zakresu danych przetwarzanych w skierowaniu w postaci elektronicznej, poprzez wskazanie m.in. danych dotyczących płci, daty urodzenia, adresu zamieszkania świadczeniobiorcy. Brak jednak uzasadnienia dla realizacji jakich celów mają być wskazywane te dodatkowe dane osobowe w przedmiotowych skierowaniach elektronicznych oraz ich niezbędności dla realizacji tych celów. Wyjaśnienia i wykazania wymaga zatem rozszerzenie zakresu danych przetwarzanych w skierowaniach elektronicznych.

W związku z powyższym, w celu zapewnienia zgodności projektowanych regulacji ze standardami ochrony danych osobowych, wymagają wyjaśnienia bądź stosownego uzupełnienia powyżej wskazane kwestie.

---

[10] Jak wskazał NSA w tym wyroku „zróżnicowanie podmiotów uprawnionych do dostępu do rejestru PESEL nie może powodować zaniechania przez administratora danych podejmowania działań zmierzających do zlikwidowania (lub co najmniej ograniczenia) zidentyfikowanego ryzyka dla danych przetwarzanych w ramach rejestru PESEL".

Projektowane regulacje powinny również uwzględniać regulacje wynikające z rozporządzenia 2025/327[11], którego celem jest m.in. poprawa dostępu osób fizycznych do ich elektronicznych danych osobowych dotyczących zdrowia i kontrolę nad nimi w kontekście opieki zdrowotnej.

Mając powyższe na uwadze, uprzejmie informuję, 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 również 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

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847.