



Warszawa, 31-08-2021

**PREZES  
URZĘDU OCHRONY  
DANYCH OSOBOWYCH**

*Jan Nowak*

**DOL.413.5.2021.WL.OJ**

**Pan  
Janusz Cieszyński  
Sekretarz Stanu  
w Kancelarii Prezesa Rady Ministrów  
ePUAP: /eKPRM/SkrytkaESP**

Szanowny Panie Ministrze,

w ramach konsultacji wdrażania systemu EZD RP został upubliczniony i poddany konsultacji **dokument *Strategia dystrybucji, wdrażania i utrzymania EZD RP od 2022 r. - projekt***, dalej: *Dokument wdrażania EZD RP*<sup>1</sup>. Ze względu na fakt, że w projektowanym systemie EZD RP mają być przetwarzane na wielką skalę dane osobowe organ nadzorczy z uwagą śledzi rozwiązania dotyczące założeń ww. systemu, które powinny być projektowane z poszanowaniem przepisów *rozporządzenia 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*

---

<sup>1</sup> Przedsięwzięcie EZD RP prowadzone jest przez Kancelarię Prezesa Rady Ministrów (KPRM) i ministra właściwego do spraw informatyzacji i ma na celu udostępnienie jednolitego i bezpłatnego narzędzia do elektronicznego zarządzania dokumentacją w administracji publicznej – systemu EZD RP. Prace nad projektem prowadzi Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy w partnerstwie z Wojewodą Podlaskim i pod nadzorem KPRM.

rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.<sup>2)</sup>), dalej: rozporządzenie 2016/679.

Należy w tym miejscu zwrócić uwagę, że w *Dokumencie wdrażania EZD RP* nie zostały zawarte postanowienia poświęcone ochronie danych i sposobowi przetwarzania danych osobowych. Tymczasem realizacja tak istotnego projektu, dla realizacji którego będą przetwarzane na masową skalę dane osobowe, w tym dane szczególnych kategorii i dane z art. 10 rozporządzenia 2016/679, wymaga rozważenia, wybrania i zastosowania najlepszych rozwiązań organizacyjno – prawnych, w szczególności zastosowania szeregu instrumentów prawnych przewidzianych ww. aktem prawa unijnego.

Realizując kompetencje określone w art 57 ust. 1 lit. c) rozporządzenia 2016/679<sup>3</sup>, a także mając na uwadze kluczowe znaczenie ww. projektu dla informatyzacji państwa, należy zwrócić uwagę na rozwiązania, o które powinien zostać wzbogacony *Dokument wdrażania EZD RP*. Przedstawione poniżej kwestie powinny zostać uwzględnione we wdrażanym systemie w celu zapewnienia zgodności z przepisami rozporządzenia 2016/679, z uwagi na potencjalne ryzyka dla prawidłowego przetwarzania danych osobowych.

### **Ocena skutków dla ochrony danych.**

Na wstępie należy podkreślić, że w upublicznionym *Dokumencie wdrażania EZD RP* nie znalazła się informacja o przeprowadzeniu lub planach przeprowadzenia wskazanej w art. 35 rozporządzenia 2016/679 oceny skutków dla ochrony danych.

Ocena taka, zgodnie z art. 35 ust. 7 rozporządzenia 2016/679, powinna zawierać co najmniej: a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora, b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1 rozporządzenia 2016/679, d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia 2016/679, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

<sup>2)</sup> Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35.

<sup>3)</sup> Zgodnie z art 57 ust. 1 lit. c) rozporządzenia 2016/679 bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia każdy organ nadzorczy na swoim terytorium doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;

Wsparciem dla autorów *Dokumentu wdrażania EZD RP* powinien być inspektor ochrony danych (art. 37-39 rozporządzenia 2016/679) - osoba, która ze względu na posiadaną wiedzę z zakresu ochrony danych osobowych powinna wspomóc w przeprowadzeniu stosownej analizy i oceny.

Należy wskazać, że przyjęte w dniu 4 kwietnia 2017 r. *Wytyczne Grupy roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679* (WP248 rev.01) wskazują na konieczność wybrania metodyki dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 do wytycznych.

Wynik takiej, prawidłowo przeprowadzonej, oceny skutków dla ochrony danych pozwoli projektującym *Dokumentu wdrażania EZD RP* na ustalenie, czy dedykowane przetwarzaniu danych rozwiązania przewidziane w planowanym system EZD RP są proporcjonalne do zakładanego celu pod kątem ochrony danych. Tylko po uzyskaniu pozytywnego rozstrzygnięcia w tej kwestii, nadany zostanie temu systemowi najkorzystniejszy kształt z punktu widzenia zapewnienia ochrony praw osób, których dane będą w tym systemie przetwarzane.

Biorąc pod uwagę powyższe, uzasadniony jest postulat przeprowadzenia oceny skutków dla ochrony danych planowanego systemu EZD RP <sup>4)</sup>.

### **Przetwarzanie danych osobowych w systemie teleinformatycznym.**

*Dokument wdrażania EZD RP*, w zawartym na str. 29 kalendarium, nie zawiera żadnych informacji o wdrożeniu, wynikających z rozporządzenia 2016/679, procedur i czynności niezbędnych do tworzenia nowego systemu teleinformatycznego. Dlatego też kluczowe znaczenie, oprócz ww. oceny skutków dla ochrony danych, powinien mieć także mechanizm **uwzględniania ochrony danych w fazie projektowania** (art 25 ust. 1<sup>5)</sup> oraz **domyślna ochrona danych** (art 25 ust. 2 rozporządzenia 2016/679<sup>6)</sup>).

---

<sup>4)</sup> Wskazany wymóg wynika również wprost z komunikatu Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 666).

<sup>5</sup> Zgodnie z art 25 ust. 1 rozporządzenia 2016/679 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.

<sup>6</sup> W art 25 ust. 2 rozporządzenia 2016/679 określono, że 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

W związku z tym, że projektowany system EZD RP wiąże się z tworzeniem nowych baz i systemów teleinformatycznych, w których przetwarzane będą dane osobowe na wielką skalę, wskazać należy na niezbędność uwzględnienia mechanizmów przewidzianych w art. 25 ust. 1 i 2 rozporządzenia 2016/679 już w fazie określenia sposobów przetwarzania tych danych w systemie EZD RP. Informacje dotyczące zastosowania ww. mechanizmów powinny zostać niewątpliwie uwzględnione w *Dokumencie wdrażania EZD RP*.

### **Zasady dotyczące przetwarzania danych osobowych.**

Niezależnie od konieczności dokonania oceny skutków dla ochrony danych dla projektowanego systemu EZD RP oraz uwzględnienia mechanizmów przewidzianych w art. 25 ust. 1 i 2 rozporządzenia 2016/679 tworzone rozwiązanie musi uwzględniać **zasady przetwarzania danych osobowych wynikające z art. 5 rozporządzenia 2016/679**. Wdrożenie zasad pozwoli na wykazanie zgodności planowanego przedsięwzięcia z przepisami o ochronie danych osobowych, a także pozwoli zweryfikować czy dla jego realizacji jest niezbędne nowe ukształtowanie norm prawa krajowego, które wraz z rozporządzeniem 2016/679 stworzą spójny system ochrony danych osobowych.

### **Zasada legalizmu.**

Kluczową informacją dotyczącą projektowanego systemu EZD RP jest określenie, jaka będzie podstawa prawna do przetwarzania w nim danych osobowych. Podkreślenia wymaga, że wskazana w *Dokumencie wdrażania EZD RP*, oczekująca na wejście w życie, ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2020 r. poz. 2320, z późn. zm.) reguluje tylko niektóre funkcje projektowanego systemu.

Nie może umknąć uwadze, że w systemie EZD RP oprócz danych zwykłych będą przetwarzane dane szczególnych kategorii, jak np. dane o stanie zdrowia czy niepełnosprawności, objęte szczególnym reżimem przetwarzania. Tymczasem -art. 9 rozporządzenia 2016/679 wymaga spełnienia dla ich przetwarzania warunków określonych w ust. 2 tego przepisu. Podobne rozwiązania – ze względu na specyficzne wymagania przetwarzania danych osobowych - wynikają z art. 10 rozporządzenia 2016/679 w odniesieniu do wykonywania operacji na danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, które to dane potencjalnie także będą przetwarzane w systemie EZD RP.

---

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.

Odnosząc się do zasady legalizmu należy także podkreślić, że – zgodnie z deklaracjami projektodawców – system EZD RP będzie zapewniał integrację z kluczowymi systemami teleinformatycznymi i rejestrami. Dlatego też zwrócić należy uwagę na treść motywu 31 rozporządzenia 2016/679, zdanie drugie w brzmieniu: Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania. Warto wskazać również na wyrok TSUE C-201/14<sup>7</sup> w sprawie Sarmanda Bara,

z którego treści wynika, że odrębne organy w ramach administracji publicznej należy traktować jako odrębnych administratorów z własnymi przesłankami, co w konsekwencji oznacza, że organ któremu w ramach administracji przekazuje się dane osobowe jest odbiorcą.

A zatem, celem uniknięcia ryzyka łączenia zbiorów i baz danych należałoby wprowadzić rozwiązania, które z jednej strony przyczynią się do usprawnienia procesów przetwarzania danych za pomocą systemu EZD RP, a z drugiej ograniczą ryzyko powstania megabazy na warunkach nie wynikających wprost z obowiązujących przepisach prawa.

Wprowadzenie zaplanowanych w *Dokumencie wdrażania EZD RP* rozwiązań będzie zatem wymagało odpowiednich podstaw w szeregu przepisach prawa, które będą musiały odpowiadać postanowieniom i warunkom przewidzianym w art. 6 i 9 rozporządzenia 2016/679. Takie przepisy szczegółowe muszą precyzować: jakie dane osobowe oraz w jaki dokładnie sposób, w jakich ściśle określonych celach i odpowiadających im procesach, dla realizacji jakich obowiązków, będą przetwarzane. Istotne jest także określenie poziomów zarządzania systemem zawierającym dane osobowe (centralny, lokalne), tak aby właściwie został ukształtowany zakres odpowiedzialności za wszelkie procesy związane z ich przetwarzaniem.

Przepisy prawa powinny określać role poszczególnych podmiotów w procesie (procesach) przetwarzania danych osobowych w systemie EZD RP<sup>8)</sup> (administrator, współadministrowanie, ew. wykonywanie przetwarzania w imieniu administratora) oraz zasady korzystania z danych

---

<sup>7</sup> Wyrok Trybunału (trzecia izba) z dnia 1 października 2014 r.(wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Curtea de Apel Cluj - Rumunia) - Smaranda Bara i in./Casa Națională de Asigurări de Sănătate, Președintele Casei Naționale de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF).

<sup>8)</sup> Dokument wdrażania EZD RP wskazuje, że zostaną utworzone takie podmioty jak: Operator EZD RP, Centrum Kompetencji Administracji, czy Lokalne Centra Kompetencji. Dokument nie wskazuje w żaden sposób na status tych podmiotów w procesach przetwarzania danych (administrator, współadministrator, podmiot przetwarzający). Jak wynika z dokumentu (str. 34) Lokalnymi Centrami Kompetencji będą mogły być również firmy świadczące usługi informatyczne. Biorąc pod uwagę fakt, że za pośrednictwem systemu EZD RP mają być udostępniane dane z całego szeregu rejestrów centralnych (str. 8), stwarza to znaczne ryzyko partycypacji w prowadzeniu rejestrów publicznych przez podmioty komercyjne na warunkach nie wynikających z obowiązujących przepisów prawa.

zgromadzonych w tym systemie. Należy podkreślić, że dokument wdrażania EZD RP w żadnym miejscu nie określa w jaki sposób system EZD RP, za pomocą którego będzie możliwy dostęp do całego szeregu rejestrów centralnych (str. 5), ma zapewnić, że dane osobowe nie będą przetwarzane przez konkretne podmioty w zakresie szerszym niż wynika to z ich ustawowych obowiązków/uprawnień. Przepisy te powinny uwzględniać zasadę minimalizacji danych, określoną w art. 5 ust. 1 lit. c) rozporządzenia 2016/679<sup>9</sup> oraz zasadę ograniczenia celu wskazaną w art. 5 ust. 1 lit. b) rozporządzenia 2016/679<sup>10</sup>. Przetwarzanie danych osobowych w systemie EZD RP powinno zatem wiązać się z precyzyjnie określonym statusem podmiotów odpowiedzialnych za to przetwarzanie. Powinny być także precyzyjnie określone zadania, prawa i obowiązki związane z przetwarzaniem danych osobowych tak aby można było dokonać analizy, czy mamy do czynienia z przetwarzaniem przez administratora/ współadministratorów, czy przez podmioty przetwarzające. Ustalenie ról w procesie przetwarzania danych osobowych ma kluczowe znaczenie z punktu widzenia odpowiedzialności za stan realizacji obowiązków wynikających z przepisów o ochronie danych osobowych<sup>11</sup>. Niewykluczone, że analiza wszystkich procesów przetwarzania danych zachodzących w ramach funkcjonowania systemu EZD RP unaoczní konieczność wprowadzenia odrębnych przepisów dedykowanych temu systemowi. Jako przykład podobnych rozwiązań można wskazać art. 19a-19d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U.

z 2021 r. poz.670, z późn. zm.) regulujące zasady działania ePUAP. Warto mieć również na względzie kierunkowy wymiar *opinii Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz na temat wniosku w sprawie decyzji Rady powierzającej agencji ustanowionej na mocy rozporządzenia XX zadania dotyczące zarządzania operacyjnego systemami SIS II i VIS w zastosowaniu tytułu VI Traktatu UE (2010/C 70/02)*. Europejski Inspektor Ochrony Danych zwrócił w tym dokumencie uwagę na obawy związane z tzw. „niezamierzonym rozrostem funkcji”. W myśl 26 punktu przywołanej opinii EIOD (...) *obawa o niezamierzony rozrost funkcji to obawa, że nowa agencja będzie mogła z własnej*

---

<sup>9</sup> Zgodnie z art 5 ust. 1 lit. c) rozporządzenia 2016/679 dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

<sup>10</sup> Zgodnie z art. 5 ust. 1 lit. b) rozporządzenia 2016/679 dane osobowe muszą być 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.

<sup>11</sup> Wytyczne 7/2020 EROD w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO przyjęte 7 lipca 2021 r.

*inicjatywy - w stopniu, którego na razie nie sposób przewidzieć - tworzyć i łączyć już istniejące i nowe wielkoskalowe systemy informatyczne. Inspektor zaleca w jaki sposób zjawiska tego można uniknąć, jeżeli po pierwsze w akcie prawnym ustanawiającym agencję ograniczy się i ściśle zdefiniuje zakres jej (ewentualnej) działalności, a po drugie dopilnuje się, by zakres ten rozszerzać w myśl demokratycznej procedury decyzyjnej, którą na ogół jest zwykła procedura ustawodawcza.*

Projektując założenia systemu EZD RP należy także dokonać oceny, jakie podmioty i na jakiej podstawie prawnej będą miały dostęp do danych osobowych różnych kategorii zawartych w tym systemie. Tworząc wskazane rozwiązania należy mieć na względzie, że projektowany system ma dotyczyć podmiotów publicznych dla realizacji ich rozlicznych zadań, w ramach których będą przetwarzane objęte tajemnicami prawnie chronionymi więc zasadne jest rozważenie, czy będzie dochodzić do powierzenia przetwarzania danych osobowych zewnętrznym podmiotom i czy takie rozwiązanie jest bezpieczne z punktu widzenia dostępu do tych tajemnic, jak również szeregu zagrożeń związanych m.in. z cyberbezpieczeństwem a także, czy taka konstrukcja pozwala na bezpieczne i zgodne z rozporządzeniem 2016/679 przetwarzanie danych w chmurze i przekazywanie danych do krajów trzecich (ma to szczególne znaczenie w świetle wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie C-311/18 - Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillianowi Schremsowi - szerzej opisanym w dalszej części pisma). W tym kontekście istotny jest sposób, zakres i forma partycypacji podmiotów zewnętrznych dla realizacji procesów przetwarzania danych w EZD RP. Szereg wątpliwości wyeliminowałoby przyjęcie instrumentu prawnego zawierającego wszystkie wymagane przez art. 28 ust. 3 rozporządzenia 2016/679 wymogi. Jego przyjęcie w akcie obowiązującego prawa niewątpliwie podwyższy standard ochrony danych osobowych w relacjach pomiędzy podmiotami publicznymi i prywatnymi przy obsłudze tworzonego systemu. Taka konstrukcja pozwala także w sposób bardziej przejrzysty uregulować komplementarnie relacje podmiotów w przypadku przyjęcia partnerstwa publiczno-prywatnego niż ma to miejsce w umowach cywilnoprawnych.

### **Zasada przejrzystości.**

**Informowanie o przetwarzaniu danych osobowych i realizacja praw osób, których dane są przetwarzane.**

Ważnym aspektem projektowanego systemu EZD RP, związanym z poszanowaniem zasady przejrzystości<sup>12</sup>), jest kwestia spełnienia obowiązków informacyjnych określonych w art. 13 i 14 rozporządzenia 2016/679, a także realizacji praw przysługujących osobie, której dane dotyczą wskazanych w art. 15-20 rozporządzenia 2016/679, z uwzględnieniem wymogów wynikających z art. 12 rozporządzenia 2016/679 (oraz poszanowaniem dopuszczalnych wyłączeń). W przypadku jeżeli prawa te miałyby być w jakimś stopniu ograniczone, rozwiązania te również powinny znaleźć odzwierciedlenie w normach prawnych budowanych na zasadach przewidzianych w art. 23 rozporządzenia 2016/679.

O konieczności respektowania obowiązku informacyjnego oraz prawa do informacji, jako emanacji prawa do prywatności, w sposób szczególny wypowiedziała się *Grupa Robocza art. 29 w opinii na temat zasady przejrzystości na podstawie rozporządzenia 2016/679 (ostatnio zmienionej i przyjętej w dniu 11 kwietnia 2018 r.)*.

Organ nadzorczy zwraca także uwagę na *Wytyczne 10/2020 Europejskiej Rady Ochrony Danych (EROD) w sprawie ograniczeń na podstawie art. 23 rozporządzenia 2016/679*. Celem tych wytycznych jest wskazanie warunków stosowania ograniczeń z art. 23 rozporządzenia 2016/679 w świetle przepisów Karty praw podstawowych UE i rozporządzenia 2016/679. Analiza wskazanego dokumentu pozwoli odpowiednio zaprojektować akt prawny regulujący funkcjonowanie systemu EZD RP pod kątem wprowadzania ograniczeń nie wynikających z ww. przepisu.

### **Zasada ograniczenie przechowywania.**

#### **Retencja – ograniczenie przechowywania – danych osobowych.**

Kolejną kwestią, która powinna być uwzględniona w *Dokumencie wdrażania EZD RP* to zaplanowanie prawidłowej **retencji przetwarzanych w tym systemie danych osobowych** uwzględniającej kategorię i specyfikę danych osobowych oraz cele przetwarzania danych, tak by nie dochodziło do naruszenia zasady ograniczenia przechowania określonej w art 5 ust. 1 lit. e) rozporządzenia 2016/679<sup>13</sup>.

---

<sup>12</sup> Zgodnie z art 5 ust. 1 lit. a) rozporządzenia 2016/679 dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”)

<sup>13</sup> Zgodnie z art 5 ust. 1 lit. e) rozporządzenia 2016/679 dane osobowe muszą być 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



Projektując system EZD RP należy również zbadać zgodność projektowanych rozwiązań m.in. z przepisami prawa archiwalnego<sup>14</sup> w celu oceny, czy przepisy zawarte w ustawie o narodowym zasobie archiwalnym i archiwach dają podstawy nie tylko do postępowania z nośnikami informacji ale także z przechowywaniem zawartych na tych nośnikach danych osobowych. Ocenie powinny być poddane wszelkie dokumenty zawierające dane osobowe, jako że część z nich może nie stanowić zasobu archiwalnego podlegającego dalszemu przechowywaniu. Retencja danych polega także na właściwym oszacowaniu procesów usuwania danych osobowych zbędnych dla realizacji zakładanych celów, który to proces powinien mieć charakter nieodwracalny<sup>15</sup>.

### **Zasada integralności i poufności.**

#### **Bezpieczeństwo – prawidłowość, poufność i integralność - danych osobowych**

Projektowany system EZD RP powinien także gwarantować prawidłowość, integralność i poufność przetwarzanych w nim danych zgodnie z zasadą poufności i integralności<sup>16</sup>. W kontekście ww. zasady, odnosząc się do *Dokumentu wdrażania EZD RP*, należy również wskazać na wątpliwości w zakresie, opisanych na str. 14–15 ww. dokumentu, planów stworzenie usługi chmurowej SaaS EZD RP. W *Dokumencie wdrażania EZD RP* stwierdzono, że „Dostawcami usługi chmurowej SaaS EZD RP będą mogły być zarówno podmioty komercyjne świadczące popularne na rynku usługi chmurowe, jak i inne niekomercyjne organizacje oraz podmioty zrzeczające instytucje zainteresowane budową wspólnej, współdzielonej infrastruktury” (str. 15).

W związku ze wskazaną deklaracją autorów *Dokumentu wdrażania EZD RP* powstaje ryzyko przetwarzania danych osobowych poza Europejskim Obszarem Gospodarczym, w państwach trzecich niezapewniających odpowiedniego stopnia ochrony w rozumieniu rozporządzenia 2016/679. W opinii organu nadzorczego *Dokument wdrażania EZD RP* powinien wprost wskazywać, że usługi chmurowe, które będą udostępnione użytkownikom systemu EZD RP, nie będą prowadziły do przekazywania danych osobowych do państw trzecich, bez zapewnienia odpowiednich gwarancji ochrony, zwłaszcza w kontekście wyroku Trybunału

---

środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą

<sup>14</sup> Przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164), dalej: ustawa o narodowym zasobie archiwalnym i archiwach.

<sup>15</sup> Opinia Grupy Roboczej art. 29 w sprawie technik anonimizacji z dnia 10 kwietnia 2014 r. (Opinia 05/2014).

<sup>16</sup> Zgodnie z art 5 ust. 1 lit. f) rozporządzenia 2016/679 dane osobowe muszą być 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.

*Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie C-311/18 - Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillianowi Schremsowi.* Analiza tych okoliczności będzie miała także kluczowe znaczenie z punktu widzenia cyberbezpieczeństwa oraz bezpieczeństwa narodowego. Rozporządzenie 2016/679 nakłada szereg obowiązków związanych z przekazywaniem danych podmiotom przetwarzającym. Niezbędne jest więc, aby dane były przekazywane tylko do podmiotów gwarantujących odpowiednie środki techniczne i organizacyjne niezbędne m.in. do zapewnienia rzetelności i przejrzystości przetwarzania (co powinien uwzględniać *Dokument wdrażania EZD RP*). W opinii organu nadzorczego ewentualne powierzenie przetwarzania danych osobowych związane z świadczeniem usług w formie SaaS powinno zostać poddane szczególnej analizie pod kątem oszacowania wszystkich ryzyk, o którym powyżej była mowa. Konieczne jest podjęcie wszelkich środków wymaganych na mocy art. 32 rozporządzenia 2016/679, czy zapewnienie bezpieczeństwa danych, np. przez pseudonimizację lub szyfrowanie.

### **Procedury ochrony danych osobowych.**

Biorąc pod uwagę znaczenie projektowanego systemu, w opinii organu nadzorczego w *Dokumentcie wdrażania EZD RP* powinny znaleźć się zalecenia, aby system EZD RP podlegał kompleksowym procedurom ochrony danych osobowych uwzględniającym przepisy rozporządzenia 2016/679 oraz przepisy prawa krajowego, jak również przegląd tychże procedur. Istotne jest także uwzględnienie mechanizmów przewidzianych w art. 25 ust. 1 rozporządzenia 2016/679 na każdym etapie przetwarzania danych, jak i po zakończeniu ich przetwarzania. Wszystkie jednostki korzystające z tego systemu powinny mieć obowiązek uwzględnienia ochrony danych i prywatności na każdym etapie funkcjonowania systemu, tj. w fazie projektowania (privacy by design), rozwoju, utrzymania i wygaszania. Co więcej, podmioty te powinny być odpowiedzialne za przestrzeganie przepisów wynikających z rozporządzenia 2016/679, a także być w stanie wykazać ich przestrzeganie **zgodnie z zasadą rozliczalności określonej w art. 5 ust. 2 rozporządzenia 2016/679**<sup>17</sup>, dokumentując podejmowane przez siebie czynności mające na celu ochronę danych osobowych.

### **Zautomatyzowane podejmowanie decyzji, w tym profilowanie oraz sztuczna inteligencja.**

---

<sup>17</sup> 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").

Podobnie, przepisy prawa powinny jednoznacznie określać, czy za pośrednictwem systemu EZD RP będzie dokonywane profilowanie osób (zautomatyzowanego podejmowania decyzji w indywidualnych sprawach), oczywiście przy uwzględnieniu warunków dozwolonych przepisami rozporządzenia 2016/679<sup>18</sup>.

Odnosząc się do wykorzystania mechanizmów sztucznej inteligencji w systemie EZD RP, na co wskazuje *Dokument wdrażania EZD RP*, organ nadzorczy podkreśla, że temat ten został przedstawiony bardzo ogólnikowo, a tymczasem możliwość gromadzenia i przetwarzania przez urządzenia wykorzystujące sztuczną inteligencję ogromnej ilości informacji będących danymi osobowymi może prowadzić do zwiększonego ryzyka naruszenia prywatności osób. Temat ten jest przedmiotem szczególnego zainteresowania organów UE z uwagi na ryzyka nie tylko w wymiarze ochrony danych osobowych. W dniu 18 kwietnia 2021 r. Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) wydali *oświadczenie 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*<sup>19</sup>. Jako inny istotny dokument dotyczący zagadnienia należy wskazać opublikowaną przez Komisję w dniu 19 lutego 2020 r. *białą księgę w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania*<sup>20</sup>. We wskazanym dokumencie określono warianty strategiczne dotyczące sposobów osiągnięcia podwójnego celu, jakim jest promowanie stosowania sztucznej inteligencji i zajęcie się zagrożeniami związanymi z niektórymi zastosowaniami tej nowej technologii. Wśród innych ważnych aktów, które powinny być brane pod uwagę przy tworzeniu założeń funkcjonowania EZD RP są również *Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii*<sup>21</sup> oraz *konkluzje prezydencji z dnia 21 października 2021 r. dotyczące karty praw podstawowych w kontekście sztucznej inteligencji i przemian*

---

<sup>18</sup> Zgodnie z art 22 ust. 1 rozporządzenia 2016/679 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.

<sup>19</sup> Na stronie Urzędu Ochrony Danych Osobowych w dniu 23 czerwca 2021 r. została opublikowana informacja, odnośnie wspólnej opinii EROD i EIOD dotyczącej projektu rozporządzenia w sprawie sztucznej inteligencji (<https://uodo.gov.pl/pl/138/2090>).

<sup>20</sup> Zob. Komisja Europejska „Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania”, COM(2020) 65 final, 2020 r.

<sup>21</sup> Zob. Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii, 2020/2012(INL).

cyfrowych<sup>22</sup> w których to dokumentach podkreślano zarówno korzyści, jak i zagrożenia związane ze sztuczną inteligencją w tym zagrożenia związane z dyskryminacją osób, których dane będą przetwarzane z jej wykorzystaniem.

W świetle wytycznych organów UE, jak również mając na uwadze przepisy rozporządzenia 2016/679 niezbędne jest, aby w sytuacji wykorzystania mechanizmów sztucznej inteligencji taki proces był kontrolowany przez człowieka w celu wychwycenia potencjalnych błędów i ich ewentualnej korekty. Istotne jest także przeprowadzenie analizy ryzyka oraz przewidywanie skutków działania algorytmów sztucznej inteligencji. W opinii organu nadzorczego bieżąca kontrola danych osobowych przetwarzanych w EZD RP pomoże w weryfikacji jakości otrzymanych rezultatów i dostarczy informacji, czy algorytmy działają zgodnie z założonym celem. Zasady kontroli mechanizmów sztucznej inteligencji powinny mieć odzwierciedlenie w przepisach ustawowych. Istotne jest więc by *Dokument wdrażania EZD RP* został rozbudowany o opisane zagadnienia.

Wykorzystywanie sztucznej inteligencji przez podmioty publiczne w ramach tworzenia EZD RP powinna poprzedzać jednak w pierwszej kolejności analiza podstaw prawnych dla realizacji tego zadania i zbadanie nie tylko wachlarza korzyści jakie niosą technologie sztucznej inteligencji ale także ryzyk z tym związanych.

Należy w tym miejscu wskazać, że na zagrożenia związane z wykorzystaniem algorytmów do profilowania osób zwraca też uwagę *Grupa Robocza art. 29 w Wytycznych w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679 przyjętych w dniu 3 października 2017 r. w dniu (ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.)*. W dokumencie tym podkreślono, że profilowanie dotyczy również procesów decyzyjnych, które nie przebiegają wyłącznie w sposób zautomatyzowany. Wytyczne z wyżej wskazanego dokumentu powinny znaleźć odzwierciedlenie w *Dokumencie wdrażania EZD RP* tak by system EZD RP nie zawierał rozwiązań umożliwiających profilowanie osób niezgodne z przepisami rozporządzenia 2016/679.

### **Podsumowanie.**

Dostrzegając istotne znaczenie dla procesu informatyzowania państwa stworzenie systemu EZD RP, nie sposób pominąć także szeregu ryzyk dla ochrony danych osobowych, które to powinny być oszacowane przez projektodawcę systemu na jak najwcześniejszym etapie i w całym ciągu dokonywanych w nim zmian. Niewątpliwie w analizie zagrożeń dla ochrony danych

<sup>22</sup> Zob. Rada Unii Europejskiej, Konkluzje prezydencji – Karta praw podstawowych w kontekście sztucznej inteligencji i przemian cyfrowych, 11481/20, 2020 r.

pomocne będzie wsparcie specjalistów z zakresu ochrony danych jakimi są Inspektorzy Ochrony Danych.

Biorąc pod uwagę powyższe, celowe jest uzupełnienie *Dokumentu wdrażania EZD RP* o wskazane aspekty. W przypadku podjęcia prac legislacyjnych w tej sprawie, Urząd Ochrony Danych Osobowych deklaruje swoje wsparcie eksperckie na każdym etapie procedowania.

Z wyrazami szacunku,

Prezes Urzędu Ochrony Danych Osobowych  
Jan Nowak

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem/