

Warszawa, 26 lutego 2021 r.



**PREZES  
URZĘDU OCHRONY  
DANYCH OSOBOWYCH**  
*Jan Nowak*

SEKRETARIAT SZEFA KS  
L.dz. *AK-020-2121*  
Data wpływu *26.02.2021*

DOL.401.74.2021.WL.MW.

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU  
L.dz. *SPS.WP.020.49.6.2021*  
Data wpływu *07.03.2021*

**Pani**

**Agnieszka Kaczmarska**

**Szef Kancelarii**

**Sejmu Rzeczypospolitej Polskiej**

**ul. Wiejska 4/6/8**

**00-902 Warszawa**

Szanowna Pani Minister,

w odpowiedzi na pismo z dnia 19 lutego 2021 r. (znak:SPS-WP.020.49.3.2021) Prezes Urzędu Ochrony Danych Osobowych uprzejmie dziękuje za przedstawienie mu do opiniowania prezydenckiego *projektu ustawy o zmianie ustawy o Sądzie Najwyższym* (dalej projekt ustawy) oraz *projektu rozporządzenia Prezydenta Rzeczypospolitej Polskiej w sprawie sposobu postępowania z aktami Sądu Najwyższego* (dalej projekt rozporządzenia) oraz przedstawia następujące stanowisko.

Ze względu na dynamikę sejmowego procesu legislacyjnego zaopiniowanie przedmiotowych projektów przed ich przyjęciem przez Sejm w dniu 25 lutego 2021 r. nie było możliwe w tak krótkim czasie, niemniej jednak uprzejmie informuję, że z punktu widzenia przepisów *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)<sup>1</sup>,

<sup>1</sup> Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018 r., s. 2.

zwanego dalej rozporządzeniem 2016/679 przedmiotowe projekty wymagają analizy i zmian w poniżej przedstawionym zakresie.

Prezes Urzędu Ochrony Danych Osobowych wskazuje, że prawem i obowiązkiem organu właściwego do spraw ochrony danych osobowych, wynikającym z obowiązujących przepisów, jest zapewnienie roli doradczej m.in. w procesie tworzenia prawa z zakresu przetwarzania danych osobowych, eksperckie wsparcie w zakresie działań, w szczególności skupiających się na tworzeniu przepisów prawa, podejmowanych w przedmiotowym zakresie. Organ właściwy w sprawie ochrony danych osobowych doradza w sprawie aktów prawnych w zakresie w jakim mogą one mieć wpływ na prawa i wolności osób fizycznych w związku z przetwarzaniem ich danych (por. art. 57 ust. 1 lit. c) rozporządzenia 2016/679), a zgodnie z prawem krajowym założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu (art. 51 ustawy o ochronie danych osobowych).

Organ właściwy w sprawie ochrony danych osobowych w pierwszej kolejności zwraca uwagę, że regulacja ustawowa dotycząca przetwarzania danych osobowych powinna określać w sposób wyraźny cel oraz zakres przetwarzanych danych osobowych, zasady ich przetwarzania na potrzeby regulacji, zapewniać stosowanie przepisów rozporządzenia 2016/679, w tym zasad przetwarzania danych określonych w jego art. 5, tj. wyznaczyć przedmiotowymi przepisami: okres przez jaki dane mają być przetwarzane, w tym przechowywane; sposób postępowania z danymi tak by przetwarzanie odbywało się zgodnie z zasadami bezpieczeństwa (poufności i integralności), w tym po wygaśnięciu celu przetwarzania.

Prezes Urzędu Ochrony Danych Osobowych poddaje pod rozwagę Projektodawcy dokonywanie (zgodnie art. 35 ust. 1 rozporządzenia 2016/679) w związku z tworzeniem przepisów regulujących operację lub zestaw operacji przetwarzania – **oceny skutków dla ochrony danych**, tj. wpływu projektowanych rozwiązań na prawo do prywatności oraz prawo do ochrony danych osobowych (art. 35 ust. 10) - ze względu na rodzaj przetwarzania, w szczególności następujący przy użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób. Uzasadnionym jest by ocena skutków dla ochrony danych była dokonywana już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych, tak, by tworzyć regulacje prawne z poszanowaniem przepisów rozporządzenia 2016/679. Uregulowana w niniejszych projektach

problematyka nie została wyczerpująco uzasadniona z punktu widzenia przepisów rozporządzenia 2016/679 (m.in. ze względu na brak oceny skutków dla ochrony danych).

I. Odnosząc się do poszczególnych rozwiązań *projektu ustawy o zmianie ustawy o Sądzie Najwyższym*, Prezes Urzędu Ochrony Danych Osobowych wskazuje co następuje.

Podkreślenia wymaga, że zagadnienie związane z prowadzeniem akt sądowych Sądu Najwyższego, w tym przetwarzaniem danych osobowych w nich zawartych z wykorzystaniem systemu elektronicznego nie znajduje się w aktualnych przepisach o Sądzie Najwyższym. Jednocześnie zasady takiego prowadzenia akt i przetwarzania danych osobowych nimi objętych, jako wprowadzające określone prawa i obowiązki powinny wynikać z przepisów rangi ustawy.

Projektodawca dodaje nową regulację w art. 96a § 2 do *ustawy o Sądzie Najwyższym*. W uzasadnieniu do projektowanej zmiany wskazano, że „(...) akta spraw sądowych przed Sądem Najwyższym są całkowicie odrębne od akt spraw przed sądami powszechnymi i wojskowymi, które przedstawia się wraz ze środkiem zaskarżenia lub innym środkiem prawnym, do którego rozpoznania jest właściwy Sąd Najwyższy, niebędący w rozumieniu Konstytucji i obowiązujących ustaw sądem powszechnym ani wojskowym. Wyłącznym dysponentem tych akt jest Sąd Najwyższy; nie są one ani łączone z aktami spraw przed sądami powszechnymi lub wojskowymi, ani zwracane do tych sądów po rozpoznaniu spraw”.

W opinii Prezesa UODO projektowane przepisy nie regulują w sposób kompleksowy zagadnienia związanego z prowadzeniem akt Sądu Najwyższego z wykorzystaniem systemu elektronicznego oraz zakresu, celów zasad i sposobów przetwarzania w nim danych osobowych, w związku z funkcjonowaniem i orzekaniem przez ten sąd w przepisach rangi ustawy, lecz stanowią odesłanie do ustawy o narodowym zasobie archiwalnym i archiwach tj. do etapu prowadzenia tych akt po okresie przechowywania w Sądzie Najwyższym. Brak takiej regulacji może prowadzić do przetwarzania danych osobowych, w tym ich szczególnych kategorii (art. 9 i art. 10 rozporządzenia 2016/679<sup>2</sup>) z naruszeniem zasady zgodności z prawem, rzetelności

---

<sup>2</sup> Zgodnie z Art. 9 rozporządzenia 2016/679:

„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;

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod

i przejrzystości (art. 5 ust. 1 lit a) rozporządzenia 2016/679). Wskazać należy, że przepisy *ustawy o narodowym zasobie archiwalnym i archiwach* nie zawierają definicji systemu elektronicznego zarządzania dokumentacją. Sam Projektodawca również dostrzega ten problem w uzasadnieniu wskazując, że „*W aktualnym stanie prawnym sposób postępowania z aktami sądowymi - w braku przepisów szczególnych - wynika jedynie z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164) oraz wydanych na jej podstawie aktów wykonawczych, które nie uwzględniają specyfiki funkcjonowania organów władzy sądowniczej*”. Podkreślić należy, że przepisy dotyczące elektronicznego zarządzania dokumentacją są zawarte nie bezpośrednio w *ustawie o narodowym zasobie archiwalnym i archiwach*, ale w *rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi*. Wskazany akt wykonawczy został wydany na podstawie delegacji z art. 5 ust. 2b *ustawy o narodowym zasobie archiwalnym i archiwach*.

W związku z powyższym, w opinii organu właściwego w sprawie ochrony danych osobowych, zawarta w **projekcie ustawy** konstrukcja powinna być na nowo przeanalizowana celem dostosowania jej do zasady zgodności z prawem i przejrzystości (art. 5 ust. 1 lit. a) rozporządzenia 2016/679). O ile przepisy *ustawy o narodowym zasobie archiwalnym i archiwach* bezpośrednio wskazują konieczność stosowania ww. rozporządzenia do określonych w art. 6 ust. 1 organów państwowych oraz państwowych jednostek organizacyjnych, organów

---

warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- 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;
- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez - lub na odpowiedzialność - pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.”

Natomiast Art. 10 rozporządzenia 2016/679 stanowi, że „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”.

jednostek samorządu terytorialnego oraz samorządowych jednostek organizacyjnych, które obowiązane są zapewnić odpowiednią ewidencję, przechowywanie oraz ochronę przed uszkodzeniem, zniszczeniem bądź utratą, to **projektowany art. 96a § 2, dodawany do ustawy o Sądzie Najwyższym** odnosi się do niedookreślonych rozwiązań z prawa archiwalnego, bez wskazania konkretnych przepisów tego aktu.

Jeżeli intencją Projektodawcy jest stworzenie podstaw prawnych dla funkcjonowania systemu informatycznego, w którym przetwarzane będą akta Sądu Najwyższego, a w konsekwencji także dane osobowe zawarte w treści tych akt, jak również dane osobowe związane z obsługą przedmiotowego systemu obsługi akt, to należy podkreślić, że nie jest to działalność archiwalna, ale związana z bieżącym funkcjonowaniem Sądu Najwyższego oraz prowadzona w systemie, w którym będą przetwarzane dane osobowe. Takie działania następować powinny z uwzględnieniem stosowania przepisów rozporządzenia 2016/679. W systemie takim będą przetwarzane znajdujące się w aktach dane osobowe, w tym szczególnie chronione (określone w art. 9 i 10 rozporządzenia 2016/679), których przetwarzanie musi spełniać warunki określone w tych przepisach i podlegać ma przewidzianym w stosownych przepisach szczegółowych odpowiednim, konkretnym środkom ochrony praw i wolności osób, których dane dotyczą (przykładem takiego aktu prawnego jest *ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej*, t.j. Dz. U. z 2019 r. poz. 1942 ze zm.).

Wskazać także należy na art. 3 ust. 1 *ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (Dz. U. z 2019 r. poz. 125), stanowiący o przewidzianych nim włączeniach<sup>3</sup>, ale nie oznacza jednak, że osoby, których dane są przetwarzane mogą być pozbawione ochrony swoich danych osobowych, praw z *Konstytucji RP*, czy z *dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającej decyzję ramową Rady 2008/977/WSiSW* (Dz. Urz. UE L 119 z 04.05.2016, str. 89).

---

<sup>3</sup> Art. 3 ust. 1 tej ustawy stanowi, że przepisów ustawy nie stosuje się do ochrony danych osobowych: znajdujących się w aktach spraw lub czynności lub urzędzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2018 r. poz. 969), ustawy z dnia 6 czerwca 1997 r. - Kodeks karny wykonawczy (Dz. U. z 2018 r. poz. 652, 1010, 1387 i 2432), ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. z 2018 r. poz. 1987 i 2399), ustawy z dnia 10 września 1999 r. - Kodeks karny skarbowy (Dz. U. z 2018 r. poz. 1958, 2192, 2193, 2227 i 2354), ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475, z późn. zm.), ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396, z 2016 r. poz. 2205 oraz z 2018 r. poz. 2435), ustawy z dnia 28 stycznia 2016 r. - Prawo o prokuraturze (Dz. U. z 2017 r. poz. 1767 oraz z 2018 r. poz. 5, 1000, 1443 i 1669).

W związku z powyższym, w ocenie organu właściwego w sprawie przetwarzania danych osobowych, szczegółowe zasady przetwarzania takich danych powinny być uregulowane w przepisach *ustawy o Sądzie Najwyższym*, zwłaszcza, że zgodnie z art. 9a § 1 obowiązującej ww. ustawy „Sąd Najwyższy jest administratorem danych osobowych przetwarzanych w postępowaniach sądowych”.

Wskazać jednocześnie należy, że nie jest jasne na czym polegać ma – związane również z przetwarzaniem w aktach sądowych danych osobowych „*wykorzystanie systemu elektronicznego zarządzania dokumentacją*” proponowane w treści **art. 96 § 2**, co również stwarza ryzyko przetwarzania danych osobowych bez zachowania zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit a) rozporządzenia 2016/679). Jeśli w ocenie Projektodawcy jest to odniesienie do art. 6 ust. 1a ustawy o narodowym zasobie archiwalnym i archiwach, to zauważyć wypada, że przepis ten nie reguluje szczegółowo przedmiotowego zagadnienia. Jeśli do *przetwarzania akt z wykorzystaniem systemu elektronicznego zarządzania dokumentacją* [w tym przetwarzania danych osobowych zawartych w tych aktach] miałyby dochodzić na podstawie innych *przepisów o narodowym zasobie archiwalnym i archiwach* to względem ww. zasadę zgodności z prawem, rzetelności i przejrzystości wymaga precyzyjnych i wyczerpujących rozstrzygnięć Projektodawcy/ Ustawodawcy w tym zakresie.

W opinii Prezesa UODO – z punktu widzenia zapewnienia stosowania przepisów ogólnego rozporządzenia o ochronie danych - projektowane przepisy w randze ustawy powinny wprost i wyczerpująco regulować wskazane kwestie.

Ponadto organ właściwy w sprawie ochrony danych osobowych zwraca uwagę na **projektowany art. 96a § 4** ustawy, który dotyczy przechowywania akt wszystkich zakończonych prawomocnie spraw sądowych Sądu Najwyższego „(...) *przez okres niezbędny ze względu na rodzaj i charakter sprawy oraz znaczenie materiałów zawartych w aktach jako źródła informacji*”. W opinii Prezesa UODO zgodnie z ww. zasadą zgodności z prawem, rzetelności i przejrzystości, ale i z zasadą ograniczenia przechowywania (wynikającą z art. 5 ust. 1 lit. e) rozporządzenia 2016/679) okres przechowywania akt, nierozdzielnie związany z przetwarzaniem w nich, w tym przechowywaniem danych osobowych, wymaga doprecyzowania. Niezrozumiałe jest - w kontekście przetwarzania danych osobowych zawartych w aktach - co w praktyce ma oznaczać i dla jakich działań oraz przez jaki czas ma stanowić podstawę prawną sformułowanie: „*akta jako źródła informacji*”. Konieczne jest dookreślenie jakim podmiotom, na jakich zasadach, w jakim celu oraz przez jaki okres miałyby być udostępniane z akt dane osobowe, skoro akta mają być „*źródłem informacji*”.

Wskazać należy, że w **projektowanym art. 96a § 7 ustawy** odnoszącym się do *wytycznych do wydania rozporządzenia* należałoby wziąć pod uwagę – oprócz ujętych w tym przepisie warunków – także okoliczności, do których odnosi się art. 4 pkt 12 rozporządzenia 2016/679<sup>4</sup> (ww. przepis wprowadza definicję „naruszenia ochrony danych osobowych”). Dla zapewnienia stosowania przepisów ogólnego rozporządzenia o ochronie danych uzasadnionym jest uzupełnienie przedmiotowych wytycznych o uwzględnienie również okoliczności np. *„przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”*.

**II. Prezes UODO wskazuje również na konieczność dookreślenia przepisów projektowanego rozporządzenia Prezydenta Rzeczypospolitej Polskiej w sprawie sposobu postępowania z aktami Sądu Najwyższego.**

Na wstępie wskazać należy, że poszanowanie hierarchii norm prawnych wymaga aby przepisy rangi rozporządzenia regulowały nie podstawę prawną lecz wykonanie norm, które w pierwszej kolejności posiadają rangę regulacji ustawowej w zakresie postępowania z danymi osobowymi zgromadzonymi w aktach Sądu Najwyższego, w tym z wykorzystaniem systemu elektronicznego.

Użyte w **§ 4 projektu rozporządzenia** sformułowanie „w szczególności” powoduje, że oprócz wymienionych w ww. paragrafie informacji mogą znaleźć się inne, wyczerpujące definicję danych osobowych<sup>5</sup> co powodowałoby brak poszanowania przepisów rozporządzenia 2016/679 (w tym z zasady minimalizacji danych – art. 5 ust. 1 lit. c). Należałoby stworzyć zamknięty katalog elementów składających się na wskazany w tym przepisie dokument.

Organ właściwy w sprawie ochrony danych osobowych wskazuje również, że zagadnienie przewidywane w **§ 7 projektu rozporządzenia** dotyczące *systemu teleinformatycznego Sądu Najwyższego* wymaga powtórnej analizy i doprecyzowania.

W pierwszej kolejności zauważyć wypada, że powtórnego rozważenia przez Projektodawcę wymaga uregulowanie tego zagadnienia – dotyczącego tworzenia systemu teleinformatycznego na poziomie przepisów rangi ustawy – bowiem prowadzenie akt sądowych

<sup>4</sup> Zgodnie z art. 4 pkt 12 rozporządzenia 2016/679 „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

<sup>5</sup> Zgodnie z art. 4 pkt 1 rozporządzenia 2016/679 „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Sądu Najwyższego z wykorzystaniem systemu elektronicznego nie znajduje się w aktualnych przepisach *ustawy o Sądzie Najwyższym*.

Ponadto, wskazanie w przepisach (i to tylko na poziomie aktu wykonawczego) jedynie na bezpieczeństwo i integralność systemu teleinformatycznego jest zbyt ogólne i niewystarczające - brak jest odniesienia np. do „*przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*”.

Na administratorze, który przetwarza dane osobowe w systemie teleinformatycznym, spoczywa obowiązek prowadzenia go w zgodzie z obowiązującymi w porządku prawnym wymogami, w tym w zakresie stosowania w przedmiotowych (projektowanych) przepisach norm ogólnego rozporządzenia o ochronie danych. To administrator odpowiada za bezpieczeństwo przetwarzanych danych, co wiąże się z przetwarzaniem danych osobowych zgodnie z określonymi szczególnymi przepisami prawami i obowiązkami, sposobami (czyli w niniejszej sprawie – w elektronicznym systemie teleinformatycznym) i celami przetwarzania danych, w tym z zastosowaniem odpowiednich zabezpieczeń systemowych (m.in. dla zapewnienia poufności, integralności, dostępności i odporności systemów oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, uszkodzeniem lub zniszczeniem).

Organ właściwy w sprawie ochrony danych osobowych wskazuje tym samym na rolę administratora, jego prawa i obowiązki wynikające z przepisów ogólnego rozporządzenia o ochronie danych – jako podmiotu odpowiedzialnego za **cele i sposoby** przetwarzania danych osobowych. Administrator danych został określony w art. 9a ustawy o Sądzie Najwyższym, zatem Projektodawca powinien dokonać analizy jaka to będzie rola i określić ją w przepisach prawa poprzez wskazanie celów przetwarzania danych osobowych oraz sposobów realizacji tych celów. W przypadku podmiotów, których kompetencje (zadania) są określone przepisami prawa, wyczerpująco należy te przepisy sformułować, wyznaczając podmiotom przetwarzającym dane określone role mocą tychże przepisów. Rola administratora ma kluczowe znaczenie w stosowaniu przepisów rozporządzenia 2016/679, ponieważ to administrator jest adresatem szeregu obowiązków wynikających z tego aktu prawnego, ale i wykonawcą praw z tych przepisów wynikających. Odpowiada on m.in. za zgodność przetwarzania z zasadami określonymi tymi przepisami, w tym art. 5 rozporządzenia 2016/679 (w tym zgodność z prawem, ograniczenie celu, integralność i poufność, rozliczalność); za realizację praw osób, których dane dotyczą, wynikających nie tylko z przepisów art. 13 i 14, ale i 15–22 rozporządzenia 2016/679, a także jest obciążony pełną odpowiedzialnością za zgodne z prawem



przetwarzanie danych, które prowadzi samodzielnie, lub które prowadzone jest w jego imieniu (motyw 74).

Projektodawca tworząc przepisy obejmujące swym zakresem także przetwarzanie danych osobowych powinien mieć na uwadze to, że ochrona danych i prywatność powinny być uwzględniane na każdym etapie funkcjonowania regulowanego projektowanymi przepisami systemu, tj. w fazie projektowania (privacy by design), rozwoju, utrzymania i wygaszania (art. 25 rozporządzenia 2016/679). Istotne jest branie pod uwagę obowiązków wynikających z art. 25 rozporządzenia 2016/679<sup>6</sup>, który odnosi się do określania sposobów przetwarzania, oraz jego uwzględnianie ma znaczenie w czasie samego przetwarzania. Uzasadnionym jest zatem branie pod uwagę wynikających z niego wymogów także przez Ustawodawcę (Projektodawcę) analizującego zasadność funkcjonowania i przydatności regulacji obowiązujących w krajowym porządku prawnym. Systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych powinny spełniać właściwości i cechy w zakresie zupełności i kompleksowości regulacji (zasada zgodności z prawem, rzetelności i przejrzystości oraz ograniczenia celu), jak również funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów. Zarówno przepisy projektu, jak i informacje zawarte w uzasadnieniu projektu, nie wskazują wprost na katalog danych osobowych przetwarzanych w systemie teleinformatycznym - jakie podmioty będą przetwarzać określone kategorie danych osobowych zawarte w aktach oraz w jakim konkretnie celu/celach będą to czynić.

Wszelkie procesy - cele i sposoby - przetwarzania danych osobowych powinny wprost wynikać z przepisów regulujących prawa i obowiązki nadawane mocą przepisów rangi ustawy, z uwzględnieniem zasad wynikających z art. 5 rozporządzenia 2016/679.

Prezes UODO wskazuje, że niezbędne jest doprecyzowanie przepisów projektów o powyższe zagadnienia, biorąc w szczególności pod uwagę brzmienie art. 5 ust. 1 lit. a) i c) rozporządzenia 2016/679, w myśl którego dane osobowe muszą być przetwarzane zgodnie z prawem, w sposób rzetelny i przejrzysty, a także muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”). Warto dodać, że dokumentacja i wynikający z niej zasób informacji o charakterze

---

<sup>6</sup> 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 (art. 25 ust. 1). Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (art. 25 ust. 2).

osobowym musi podlegać odpowiednim zabezpieczeniom, co również nie zostało wprost określone w projektowanych przepisach.

Uwzględnienie powyższych kwestii przedstawionych w trybie stanowiska eksperckiego przyczyniłoby się do stworzenia przepisów czyniących zadość przepisom o ochronie danych osobowych, zapewniających stosowanie przepisów rozporządzenia 2016/679.

Z wyrazami szacunku,

Prezes Urzędu  
Ochrony Danych Osobowych

Jan Nowak

/- dokument w postaci elektronicznej podpisany  
kwalifikowanym podpisem elektronicznym/