



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa, dnia 16 lutego 2026 r.

DPNT.401.17.2026.WL.OJ

**Pan
Dariusz Standerski
Sekretarz Stanu
w Ministerstwie Cyfryzacji**

Szanowny Panie Ministrze,

w odpowiedzi na przekazane do wiadomości organu nadzorczego pismo z 9 lutego 2026 r. znak: DPiS.WWKS.002.18.1.2026, przekazujące, w celu rozpatrzenia przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji, **projektu rozporządzenia Prezesa Rady Ministrów zmieniającego rozporządzenie w sprawie postępowania przy rozpoznawaniu odwołań przez Krajową Izbę Odwoławczą** wersja z 4 lutego 2026 r. (wpisanego do Wykazu prac legislacyjnych Prezesa Rady Ministrów pod numerem 84), 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, organ nadzorczy zauważa uprzejmie co następuje.

Uwagi ogólne.

1. Prezes Urzędu Ochrony Danych Osobowych przedstawił uwagi do **projektu rozporządzenia** w wersji z 1 grudnia 2025 r. oraz wersji z 12 stycznia 2026 r. Zgłosił

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, poz. 1781).

szereg zastrzeżeń do proponowanych koncepcji przetwarzania danych osobowych na podstawie procedowanego aktu prawnego. W sprawie projektowanych zmian odbyło się także spotkanie (2 lutego 2026 r.) przedstawicieli Urzędu Zamówień Publicznych z przedstawicielami Urzędu Ochrony Danych Osobowych – omówiono wątpliwości odnośnie projektu, **w tym podstawy prawnej w przepisach Pzp³ dla części rozwiązań w zakresie przetwarzania danych osobowych na podstawie projektowanego rozporządzenia.**

W uzasadnieniu do projektu wskazano: „Projekt nowelizacji rozporządzenia wydanego na podstawie art. 544 ust. 4 ustawy Pzp ma przede wszystkim na celu dostosowanie przepisów tego aktu wykonawczego do szeregu zmian w ustawie Pzp dotyczących postępowania odwoławczego, wprowadzonych na podstawie art. 28 ustawy z dnia 21 maja 2025 r. o zmianie niektórych ustaw w celu deregulacji prawa gospodarczego i administracyjnego oraz doskonalenia zasad opracowywania prawa gospodarczego (Dz. U. poz. 769), które wejdą w życie z dniem 13 marca 2026 r. Ustawą tą zostały wprowadzone regulacje umożliwiające stronom oraz uczestnikom postępowania odwoławczego przed KIO udział w jawnych rozprawach lub posiedzeniach jawnych za pośrednictwem urządzeń informatycznych pozwalających na komunikowanie się na odległość, jak również zmiany dotyczące prowadzenia postępowania odwoławczego przed Krajową Izbą Odwoławczą mające na celu zachowanie efektywności i szybkości postępowania odwoławczego.”.

Zgodnie z art. 508a ust. 1, dodanym ustawą deregulacyjną do ustawy Pzp, jawne rozprawy lub posiedzenia jawne mogą być przeprowadzane przy użyciu urządzeń technicznych umożliwiających ich przeprowadzenie na odległość (zdalna rozprawa lub zdalne posiedzenie), jeżeli nie stoi temu na przeszkodzie charakter czynności, które mają być dokonane na tych rozprawach lub posiedzeniach, nie występują inne okoliczności utrudniające przeprowadzenie zdalnej rozprawy lub zdalnego posiedzenia, i jeżeli zostaną zagwarantowane pełna ochrona praw procesowych stron i uczestników postępowania odwoławczego oraz prawidłowy tok tego postępowania.

Projektowany akt wykonawczy ma więc doprecyzować zasady prowadzenia jawnych rozpraw lub jawnych posiedzeń za pośrednictwem urządzeń informatycznych pozwalających na komunikowanie się na odległość, określone w ww. przepisie Pzp.

2. Prezes Urzędu Ochrony Danych Osobowych konsekwentnie w swoich stanowiskach do projektu przypomniał, że **w procesie legislacyjnym ustawy**

deregulacyjnej zgłaszał szereg uwag do jej przepisów⁴, w tym do przedmiotowego art. 508a Pzp⁵.

W swoim stanowisku organ nadzorczy wskazywał w szczególności, że „zapis obrazu i dźwięku z czynności procesowych odbywających się na sali rozpraw oznacza m.in. przetwarzanie danych osobowych. Proces ten powinien odbywać się więc z poszanowaniem zasad wynikających z rozporządzenia 2016/679 i prawodawca w procesie tworzenia przepisów powinien w tym zakresie kierować się również kryterium bezpieczeństwa danych. W związku z powyższym analiza wymaga również dodany art. 508a ust. 3 regulujący sposób informowania o standardach technicznych i wymaganiach sprzętowych niezbędnych do udziału w zdalnej rozprawie lub zdalnym posiedzeniu. Przekazywanie tego zapisu do miejsca przebywania osób uczestniczących w zdalnej rozprawie lub zdalnym posiedzeniu powinno odbywać się przy zachowaniu najwyższych standardów technicznych, ze względu na ryzyko dla naruszenia praw lub wolności osób fizycznych, jakie niesie ze sobą przetwarzanie danych z użyciem nowych technologii. Prawodawca powinien w treści proponowanych przepisów uwzględnić obowiązki

⁴ Pisma Prezesa Urzędu Ochrony Danych Osobowych z 7 maja 2024 r. oraz 6 września 2024 r. z uwagami do projektu ustawy o zmianie niektórych ustaw w celu deregulacji prawa gospodarczego i administracyjnego oraz doskonalenia zasad opracowywania prawa gospodarczego (znak: DOL.401.121.2024).

⁵ Zgodnie z pr. 508a. Pzp „1. Jawne rozprawy lub posiedzenia jawne mogą być przeprowadzane przy użyciu urządzeń technicznych umożliwiających ich przeprowadzenie na odległość (zdalna rozprawa lub zdalne posiedzenie), jeżeli nie stoi temu na przeszkodzie charakter czynności, które mają być dokonane na tych rozprawach lub posiedzeniach, nie występują inne okoliczności utrudniające przeprowadzenie zdalnej rozprawy lub zdalnego posiedzenia i jeżeli zostaną zagwarantowane pełna ochrona praw procesowych stron i uczestników postępowania odwoławczego oraz prawidłowy tok tego postępowania. 2. W przypadku zdalnej rozprawy lub zdalnego posiedzenia na sali rozpraw są obecni skład orzekający i protokolant, a pozostałe osoby uczestniczące w zdalnej rozprawie lub zdalnym posiedzeniu, w szczególności strony i uczestnicy postępowania odwoławczego, nie muszą być na sali rozpraw obecne. Zapis obrazu i dźwięku z czynności procesowych odbywających się na sali rozpraw przekazuje się z sali rozpraw do miejsca przebywania osób uczestniczących w zdalnej rozprawie lub zdalnym posiedzeniu oraz z miejsca przebywania tych osób do sali rozpraw. 3. Prezes Urzędu podaje, w drodze obwieszczenia, w Biuletynie Informacji Publicznej, na stronie podmiotowej Urzędu, informacje o standardach technicznych oprogramowania i wymaganiach sprzętowych niezbędnych do uczestniczenia w zdalnej rozprawie lub zdalnym posiedzeniu.”.

administratora wynikające z art. 32 rozporządzenia 2016/679⁶ i zasad ochrony danych w sposób odpowiadający celom regulacji. Ponadto, dla realizacji zasady przejrzystości oraz legalizmu, standardy techniczne oprogramowania, o których mowa w proponowanym art. 508a ust. 3, określone powinny **być w drodze rozporządzenia wykonawczego do ustawy, a nie w drodze obwieszczenia.**”.

Niestety przepisy projektowanej ustawy nie zostały uzupełnione zgodnie ze wskazanym stanowiskiem Prezesa Urzędu Ochrony Danych Osobowych, a także nie zostały objęte testem prywatności **wraz z oceną skutków dla ochrony danych** (art. 25⁷ i 35 ust. 1 rozporządzenia 2016/679⁸), o co również wnosił organ nadzorczy. Przeprowadzenie takiego testu dla projektu ustawy pozwoliło by m.in. uwzględnić luki tworzonych przepisów ustawowych które wpływają obecnie także na projektowane rozporządzenie.

Test prywatności.

⁶ 1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych; b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. 2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42. 4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.”.

⁷ Ust. 1 Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. 2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

⁸ Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Analiza projektowanych przepisów rozporządzenia wskazuje, że dla ich realizacji będą przetwarzane – w tym **z użyciem nowych technologii** (w trakcie zdalnych rozpraw lub zdalnych posiedzeń oraz w ramach przesyłania korespondencji przy użyciu środków komunikacji elektronicznej w związku z postępowaniem odwoławczym przed Krajową Izbą Odwoławczą) – w znacznej ilości dane osobowe przetwarzane na podstawie Pzp zawarte w dokumentach, a także ujawniane w trakcie postępowania w formie zdalnej przed Krajową Izbą Odwoławczą. Będą to zarówno tzw. **dane zwykłe**, jak i dane wprost w przepisach prawa określone jako **szczególne kategorie danych** objęte ochroną na podstawie art. 9 ust. 1 rozporządzenia 2016/679⁹, np. dane dotyczące zdrowia, dane biometryczne (nagrania głosu i wizerunku). Projektowane zmiany – w związku z przetwarzaniem na podstawie przepisów Pzp danych o niekaralności pozyskanych z Krajowego Rejestru Karnego – będą powodować również przetwarzanie danych podlegających wzmocnionemu reżimowi ochrony w rozumieniu art. 10 rozporządzenia 2016/679¹⁰. Nie można bowiem pominąć, że w trakcie transmitowanej rozprawy może dojść do ujawnienia informacji znajdujących się w aktach spraw zebranych w ramach realizacji przepisów Pzp. Oprócz ww. danych, na podstawie projektowanych rozwiązań będą przetwarzane **numery PESEL**, stanowiące krajowy numer identyfikacyjny zgodnie z art. 87 rozporządzenia 2016/679¹¹, którego przetwarzanie podlega wzmocnionej ochronie prawnej. W ramach projektowanych przepisów mają być również przetwarzane dane objęte tajemnicami prawnie chronionymi które na podstawie odrębnych przepisów wymagają szczególnej ochrony.

To oznacza, że przetwarzanie danych powinno być nie tylko **zgodne ze standardami i zasadami dotyczącymi przetwarzania danych osobowych**

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

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

¹¹ 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.

ukształtowanymi mocą art. 5 rozporządzenia 2016/679¹², ale i objęte testem prywatności wraz z oceną skutków dla ochrony danych. Pozwoliłoby to m.in. zbadać, czy projektowane przepisy – zgodnie z art. 6 ust. 3 z rozporządzenia 2016/679 – są proporcjonalne i zawierają gwarancje odpowiednie do *ratio legis* projektu. Istotne jest zatem, aby projektowane przepisy zapewniły stosowanie norm ogólnego rozporządzenia o ochronie danych dla realizacji rozwiązań przyjętych w ustawie Pzp i były przeanalizowane z uwzględnieniem ryzyk towarzyszących operacjom przetwarzania takich danych osobowych, bez obniżenia standardów wynikających z ogólnego rozporządzenia, a tym samym zapewniały gwarancje wynikające z przepisów dotyczących przetwarzania danych osobowych, m.in. co do realizacji praw i wolności osób, których dane dotyczą (podmiotów danych). Projektodawca, już na etapie tworzenia podstawy prawnej przetwarzania danych, powinien ocenić czy projektowane przepisy spełniają kryteria zapewniające bezpieczeństwo, autentyczność, poufność, jak i rozliczalność, w tym przynajmniej podstawowe standardy / kryteria jakie powinny spełniać wykorzystywane środki techniczne i organizacyjne zgodnie z art. 32 rozporządzenia 2016/679. Jest to jest szczególnie ważne w przypadku takiej formy przetwarzania danych osobowych do jakiej ma dochodzić przy rozpoznawaniu odwołań przez Krajową Izbę Odwoławczą w ramach transmisji i nagrywaniem obrazu i dźwięku zdalnych rozpraw lub zdalnych posiedzeń.

Wskazane rozwiązania powinny być również ponownie przeanalizowane przez projektodawcę pod kątem przepisów dotyczących cyberbezpieczeństwa, w tym dyrektywy NIS – 2¹³ w związku z zagrożeniami jakie wiążą się z przekazywaniem za pośrednictwem środków komunikacji elektronicznej danych osobowych o charakterze sensytywnym (art. 9 i 10 rozporządzenia 2016/679 oraz dane objęte tajemnicami prawnie chronionymi).

Uwagi szczegółowe.

¹² Zgodnie z art. 5 ust. 1 rozporządzenia 2016/679 dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość"); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania"); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwoloną lub niezgodną z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność"). Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679 Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

¹³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

1. Przedmiotowy opiniowany **projekt w wersji z 4 lutego 2026 r. analogicznie jak wersja projektu z 12 stycznia 2026 r.** – w porównaniu do rozwiązań zawartych w wersji z 1 grudnia 2025 r. – nie zawiera przepisów dotyczących korzystania z systemu teleinformatycznego, w którym miałyby być przetwarzane dane osobowe w ramach przekazywania dokumentacji spraw, a także transmisji i nagrywania dźwięku rozpraw i zdalnych posiedzeń).

Jak wyżej wskazano, rozwiązania te budziły szereg wątpliwości Prezesa Urzędu Ochrony Danych¹⁴, w szczególności dlatego, że nie miały umocowania w przepisach rangi ustawowej (Pzp).

Niestety, usunięcie w nowej wersji opiniowanego projektu przepisów dotyczących systemu teleinformatycznego nie rozwiązuje problemu podstawy prawnej do przetwarzania danych osobowych objętych projektem.

W aktualnej wersji projektowanego rozporządzenia **brak jest w ogóle określenia, gdzie i w jaki sposób będą przetwarzane dane osobowe w toku rozpoznawania spraw przez Krajową Izbę Odwoławczą. Takich rozwiązań brak jest nadal w przepisach rangi ustawy, tj. w Pzp.**

Z informacji przekazanych przez przedstawicielki Urzędu Zamówień Publicznych na spotkaniu z pracownikami Urzędu Ochrony Danych Osobowych¹⁵ wynika, że do realizacji projektowanego rozporządzenia ma służyć system teleinformatyczny, którego administratorem jest Minister Sprawiedliwości, a podstawą do przetwarzania w nim danych osobowych **ma być wyłącznie umowa cywilnoprawna.**

Wskazana koncepcja wzbudza poważne zaniepokojenie Prezesa Urzędu Ochrony Danych Osobowych co do jej legalności w kontekście przetwarzania danych osobowych. Rozwiązania obejmujące przetwarzanie danych osobowych, w tym możliwych także danych o charakterze sensytywnym (art. 9 i 10 rozporządzenia 2016/679, tajemnice prawnie chronione) do jakiego będzie dochodzić w związku z rozpoznawaniem spraw przez Krajową Izbę Odwoławczą z wykorzystaniem systemu teleinformatycznego **muszą mieć bowiem podstawę w przepisach powszechnie obowiązujących**, a nie w umowie cywilnoprawnej, a zakres i sposób przetwarzania danych osobowych musi być zgodny z rozwiązaniami ukształtowanymi mocą Pzp. Podstawą prawną do przetwarzania danych osobowych nie może więc być w tym przypadku umowa cywilnoprawna, gdyż takie rozwiązanie narusza zasady zgodności z prawem, rzetelności i przejrzystości, integralności i poufności oraz rozliczalności. Jednocześnie należy wskazać, że przetwarzanie danych osobowych w systemie informatycznym musi odbywać się zgodnie z warunkami zgodności z prawem (art. 6 ust. 3 rozporządzenia 2016/679 w zw. z art. 6 ust. 1 lit. c i e rozporządzenia 2016/679 oraz art 9 ust.2 lit. g rozporządzenia 2016/679).

Rozwiązanie to budzi również wątpliwości w świetle norm Konstytucji RP (art. 7 stanowiącego, że organy władzy publicznej działają na podstawie i w granicach prawa, art. 31 ust. 3 i art. 51 ust. 5 Konstytucji RP statuujących zasady ograniczania praw i

¹⁴ Opinia Prezesa Urzędu Ochrony Danych Osobowych z 27 stycznia 2026 r. (znak: DPNT.401.17.2026.WL.OJ).

¹⁵ Które odbyło się 2 lutego 2026 r. w formie zdalnej.

wolności konstytucyjnych, w tym prawa do ochrony danych osobowych, oraz zasady i tryb gromadzenia oraz udostępniania informacji o osobach, które określać powinna ustawa).

Prezes Urzędu Ochrony Danych Osobowych wskazuje więc na pilną potrzebę nowelizacji Pzp, tak, by **regulacje dotyczące zasad i trybu przetwarzania danych osobowych w związku z rozpoznawaniem spraw przez Krajową Izbę Odwoławczą z wykorzystaniem systemu teleinformatycznego oraz ról i zadań podmiotów uczestniczących w procesach przetwarzania danych osobowych zostały uregulowane w przepisach rangi ustawowej a jedynie doprecyzowywane w przepisach projektowanego rozporządzenia** (oraz by nie odbywały się jedynie na podstawie umowy).

2. Niezależnie od braku podstawy prawnej do przetwarzania danych osobowych w związku z rozpoznawaniem spraw przez Krajową Izbę Odwoławczą w systemie teleinformatycznym Ministra Sprawiedliwości koncepcja ta wiąże się z szeregiem ryzyk, których analiza powinna być przeprowadzona w tekście prywatności.

Jednym z nich są możliwe zmiany celów przetwarzania tych danych. Zmiany takie – zgodnie z art. 6 ust. 4 rozporządzenia 2016/679¹⁶ – mogą zachodzić jedynie na podstawie prawa państwa członkowskiego stanowiącego w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu jedynie celów, o których mowa w art. 23 ust. 1 rozporządzenia 2016/679¹⁷ oraz powinny być wprowadzone z uwzględnieniem zasad i warunków z tego przepisu wynikających.

¹⁶ Zgodnie z rt.. 6 ust. 4 rozporządzenia 2016/679 jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator - aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane - bierze pod uwagę między innymi: a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania; b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10; d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

¹⁷ Zgodnie z art 23 ust. 1 rozporządzenia 2016/679 Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym: a) bezpieczeństwu narodowemu; b) obronie; c) bezpieczeństwu publicznemu; d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; e) innym ważnym celem leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronie niezależności sądów i postępowania sądowego; g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu; h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) - e) oraz g); i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucji roszczeń cywilnoprawnych.

Rozwiązanie to budzi również wątpliwości w świetle konstytucyjnej zasady praworządności.

3. W projektowanym **§ 5b** rozporządzenia w sprawie postępowania przy rozpoznawaniu odwołań przez Krajową Izbę Odwoławczą wskazano, że: „W przypadku gdy dokument elektroniczny, o którym mowa w art. 3 pkt 35 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), przekazywany w toku postępowania odwoławczego, w tym podczas zdalnej rozprawy lub zdalnego posiedzenia, zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 oraz z 2025 r. poz. 794), strona oraz uczestnik postępowania odwoławczego, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.”.

W związku z koniecznością realizacji przez projektodawcę zasady zgodności z prawem, rzetelności i przejrzystości, integralności i poufności oraz rozliczalności Prezes Urzędu Ochrony Danych Osobowych wnosi o **rozbudowę przedmiotowego przepisu** tak, by obowiązek stron oraz uczestników postępowań odwoławczych przekazywania dokumentów elektronicznych w wydzielonym i odpowiednio oznaczonym pliku (w celu utrzymania w poufności zawartych w nim informacji) **został rozszerzony** na dokumenty, w których zawarto dane osobowe chronione na podstawie art. 9, 10 i 87 rozporządzenia 2016/679. Dodatkowo zgodnie z art. 32 ust. 1 lit. a rozporządzenia 2016/679 przesyłanie dokumentów zawierających ww. chroniące kategorie danych osobowych powinno uwzględniać **mechanizmy pseudonimizacji i szyfrowania** danych osobowych, a zatem ustawodawca powinien rozbudować projektowany przepis także w tym zakresie.

4. Jak wskazano w projektowanym **§ 24 ust. 1-4** rozporządzenia w sprawie postępowania przy rozpoznawaniu odwołań przez Krajową Izbę Odwoławczą: „1. Osobom, o których mowa w § 23 ust. 6, przewodniczący składu orzekającego może wyrazić zgodę na utrwalanie przebiegu rozprawy lub posiedzenia, w tym zdalnej rozprawy lub zdalnego posiedzenia, za pomocą urządzeń rejestrujących obraz lub dźwięk, gdy przemawia za tym uzasadniony interes społeczny, a ważny interes strony oraz uczestnika postępowania odwoławczego temu się nie sprzeciwia, i gdy dokonywanie tych czynności nie utrudni przeprowadzenia rozprawy lub posiedzenia. Zgoda, o której mowa w zdaniu pierwszym, może być wyrażona w zakresie, w jakim nie wyłączono jawności rozprawy lub posiedzenia. 2. Nie jest wymagana zgoda przewodniczącego składu orzekającego na utrwalanie przez strony oraz uczestników postępowania odwoławczego przebiegu rozprawy lub posiedzenia, w tym zdalnej rozprawy lub zdalnego posiedzenia, za pomocą urządzenia rejestrującego dźwięk. W takim przypadku strony oraz uczestnicy postępowania odwoławczego uprzedzają przewodniczącego składu orzekającego o swoim zamiarze. 3. Do utrwalania przez strony oraz uczestników postępowania odwoławczego przebiegu rozprawy lub posiedzenia, w tym zdalnej rozprawy lub zdalnego posiedzenia, za pomocą urządzenia rejestrującego obraz, przepis ust. 1 stosuje się odpowiednio. 4.

Przewodniczący składu orzekającego zakazuje utrwalenia przebiegu rozprawy lub posiedzenia, w tym zdalnej rozprawy lub zdalnego posiedzenia, w sposób, o którym mowa w ust. 2-3, w zakresie w jakim wyłączono jawność rozprawy lub posiedzenia lub sprzeciwia się temu względ na prawidłowość postępowania.”.

Prezes Urzędu Ochrony Danych Osobowych zwraca uwagę, że dopuszczenie bez ścisłej kontroli nagrywania przez strony oraz uczestników postępowania odwoławczego przebiegu rozprawy lub posiedzenia należy ocenić negatywnie przez pryzmat zasad zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a), ograniczenia celu (art. 5 ust. 1 lit. b), minimalizacji danych (art. 5 ust. 1 lit. c), integralności i poufności (art. 5 ust. 1 lit. f), ograniczenia przechowania oraz rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679). W trakcie rozprawy lub posiedzenia mogą być bowiem ujawniane dane osobowe znajdujące się w dokumentach postępowania w tym dane o charakterze sensytywnym (art. 9 i 10 rozporządzenia 2016/679, tajemnice prawnie chronione). Dopuszczenie by osoby fizyczne mogły pozyskiwać te dane i dalej przetwarzać nawet na niezabezpieczonych nośnikach w istocie prowadzi do tego, że administrator traci jakąkolwiek kontrolę nad tymi danymi. Generuje to również szereg zagrożeń także w sferze cyberbezpieczeństwa.

Z tego powodu w ocenie organu nadzorczego niezbędna jest rozbudowa przepisów dotyczących nagrywania przebiegu zdalnych rozpraw lub zdalnych posiedzeń przez osoby trzecie o rozwiązania gwarancyjne dla podmiotów danych. Rozwiązania te powinny w szczególności uwzględniać:

1. zobowiązania osób nagrywających do wykorzystania nagranych danych wyłącznie w celu dotyczącym tego postępowania a także ich usunięcia gdy przestały być niezbędne dla tego postępowania (wraz z przewidzianymi sankcjami za złamanie takich zobowiązań);
2. warunki techniczne jakie musiałoby spełniać takie urządzenie by gwarantować integralności, poufności i prawidłowość nagranych informacji oraz możliwość weryfikacji takich warunków przez administratora.

Powyższe rozwiązania powinny zostać wprowadzone wprost do przepisów Pzp, a jedynie doprecyzowane w akcie wykonawczym przy poszerzeniu delegacji do wydania rozporządzenia.

5. Wbrew zasadzie ograniczenia przechowania (art. 5 ust. 1 lit. e rozporządzenia 2016/679) w przepisach Pzp nie określono okresu usuwania zawierających dane osobowe nagrań zdalnych rozpraw lub zdalnych posiedzeń.

W ocenie organu nadzorczego projektodawca w celu zapewnienia stosowania przepisów rozporządzenia 2016/679 w przepisach krajowych Prawa zamówień publicznych w ramach najbliższej nowelizacji Pzp powinien uzupełnić przepisy tego aktu prawnego we wskazanym zakresie.

Jednocześnie pozwalam sobie 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 za zapewnienie ich zgodności z przepisami o ochronie danych

osobowych. Wyrażam nadzieję, że uwzględnienie powyższych 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/