PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 29 października 2025 r.

DOL.413.11.2024

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji

Szanowny Panie Premierze,

działając na podstawie art. 52 ust. 2 ustawy o ochronie danych osobowych[1], **zwracam się do Pana Premiera z uprzejmą prośbą o możliwie pilne dokonanie przeglądu przepisów prawa regulujących przetwarzanie danych osobowych w rejestrach publicznych**[2], celem dostosowania warunków ich przetwarzania do zasad ochrony danych osobowych wynikających z Konstytucji RP oraz rozporządzenia 2016/679[3], wykładanych zgodnie z dorobkiem orzeczniczym Trybunału Konstytucyjnego oraz sądów europejskich, tj. Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka.

I. Wstęp.

Polski system prawny stoi przed wyzwaniami związanymi z zapewnieniem stosowania szeregu aktów prawa Unii Europejskiej, które zmieniają dotychczasowe modele przetwarzania danych, w tym danych osobowych, w rejestrach publicznych.

[1] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[2] Zgodnie z art. 3 pkt 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307), dalej: ustawa o informatyzacji, rejestr publiczny to rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych.
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.), dalej: rozporządzenie 2016/679.

Prowadzone prace legislacyjne dotyczące rozporządzenia 2022/868 – aktu w sprawie zarządzania danymi[4], rozporządzenia 2024/1689 – aktu w sprawie sztucznej inteligencji[5], rozporządzenia 2022/2065 – aktu o usługach cyfrowych[6], rozporządzenia 2023/2854 – aktu w sprawie danych[7] , rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia[8], rozporządzenia w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej[9], czy też implementacji dyrektywy 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[10], jak i dyrektywy 2022/2555[11] i przyjęte w ich toku rozwiązania w prawie krajowym będą miały ogromny wpływ na rozwój i kształt cyfryzacji w Polsce.

Stosowanie tych przepisów będzie związane także z wykorzystywaniem narzędzi informatycznych z zakresu nowych technologii. Stały rozwój tych technologii, w tym nowych metod przetwarzania danych osobowych (np. z wykorzystaniem narzędzi sztucznej inteligencji), powoduje szereg wyzwań dla państwa, np. konieczność zapewnienia efektywnego nadzoru nad tymi procesami, ale niesie ze sobą także ryzyka dla praw i wolności podmiotów danych, w tym praw

---

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz. Urz. UE L 152 z 3.6.2022, str. 1 ze zm.), dalej: rozporządzenie 2022/868.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), dalej: rozporządzenie 2024/1689.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 27.10.2022 r., str. 1), dalej: rozporządzenie 2022/2065.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 27.10.2022 r., str. 1), dalej: rozporządzenie 2022/2065.

[7] Rozporządzenie Parlamentu Europejskiego i Rady UE 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych), dalej: rozporządzenie 2023/2854.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (Dz. U. UE. L. z 2025 r. poz. 327),dalej: rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia lub EHDS.

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 1183 z późn. zm.), dalej: rozporządzenie w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej.

[10] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE. L 2016/1148 z 19.07.2016), dalej: Dyrektywa 2016/1148.

[11] 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), dalej: Dyrektywa 2022/2555.

konstytucyjnych i podstawowych osób, których dane są przetwarzane przez organy państwa, jakimi są prawo do prywatności i prawo do autonomii informacyjnej.

Orzecznictwo sądów międzynarodowych w ostatnich latach zwraca szczególną uwagę na problematykę przetwarzania danych osobowych w rejestrach publicznych oraz podkreśla konieczne ograniczenia władzy publicznej w tym zakresie. Przykładami mogą być w szczególności wyroki Trybunału Sprawiedliwości Unii Europejskiej (TSUE), w których zwraca się uwagę na zagrożenia związane z przetwarzaniem danych osobowych bez stosownych gwarancji dla podmiotów danych w rejestrach publicznych, a także z pozyskiwaniem i dalszym przetwarzaniem tych danych do innych celów przez kolejne podmioty:

1) wyrok z 22 listopada 2022 r. w sprawie Luxembourg Business Registers[12] dotyczący rejestrów beneficjentów rzeczywistych prowadzonych przez państwa członkowskie, w tym Polskę,
2) wyrok z 7 grudnia 2023 r. w sprawie SCHUFA Holding (Libération de reliquat de dette)[13] odnoszący się do praktyki biur informacji kredytowej polegającej na przechowywaniu, we własnych bazach danych, informacji o osobach fizycznych pochodzących z rejestru publicznego, czy
3) wyrok z 4 października 2024 r., C-200/23, Agentsia po Vpisvaniyata przeciwko Ol[14] dotyczący legalności przetwarzania danych osobowych w rejestrze handlowym pod nadzorem państwa.

W kontekście nieprawidłowej praktyki łączenia w rejestrach publicznych danych osobowych pozyskiwanych z różnych baz danych oraz w odniesieniu do pojęcia i roli administratora istotne są również wyroki TSUE:

1) z 1 października 2015 r., C-201/14[15], w sprawie Smaranda Bara, z którego treści wynika w szczególności, 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”,
2) z 11 stycznia 2024 r., C-231/22, État belge przeciwko Autorité de protection des données[16], wskazujący że jeżeli prawo krajowe państwa członkowskiego określa cele i sposoby przetwarzania danych osobowych w danym dzienniku urzędowym za administratora danych osobowych mogą być uznane też

[12] Wyrok Trybunału Sprawiedliwości z 22 listopada 2022 r., Luxembourg Business Registers, C-37/20 i C-601/20, EU:C:2022:912.
[13] Wyrok Trybunału Sprawiedliwości z 7 grudnia 2023 r. w sprawie SCHUFA Holding (Libération de reliquat de dette) Sprawa C-26/22 (Sprawy połączone C-26/22, C-64/22), EU:C:2023:958
[14] Wyrok Trybunału Sprawiedliwości z 4 października 2024 r., C-200/23, Agentsia po Vpisvaniyata przeciwko Ol., EU:C:2024:827.
[15] Wyrok Trybunału (trzecia izba) z 1 października 2015 r.(wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Curtea de Apel Cluj - Rumunia) - Smaranda Bara i in./Casa Naţională de Asigurări de Sănătate, Preș edintele Casei Nat ionale de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF), EU:C:2015:638.
[16] Wyrok Trybunału Sprawiedliwości z 11 stycznia 2024 r., C-231/22 w sprawie État belge przeciwko Autorité de protection des données, EU:C:2024:7.

jednostka lub podmiot prowadzące dziennik urzędowy państwa członkowskiego.

Prezes Urzędu Ochrony Danych Osobowych wielokrotnie w toku opiniowania projektów aktów prawnych, jak też w stanowiskach kierowanych do Ministra Spraw Zagranicznych, omawiających konsekwencje ww. wyroków dla systemu polskiego prawa, zwracał uwagę na problematykę zapewnienia stosowania w prawie krajowym przetwarzania danych osobowych w rejestrach publicznych zgodnego z przepisami rozporządzenia 2016/679. W szczególności, analizował i zwracał szczególną uwagę na rozwiązania dotyczące Krajowego Rejestru Sądowego, systemu SEPIS[17], ewidencji gruntów i budynków, Krajowego Rejestr Zadłużonych, Rejestru Dowodów Osobistych, Systemu Obsługi Wsparcia (SOW)[18], Zintegrowanego Systemu Baz Danych w Narodowym Centrum Badań i Rozwoju, Centralnego Rejestru Osób Uprawnionych do Wykonywania Zawodu Medycznego, Rejestru PESEL, Rejestru dokumentów paszportowych oraz Rejestru obywateli Ukrainy, którym nadano numer PESEL. Prezes UODO zgłaszał również szereg wątpliwości do rozwiązań informatycznych funkcjonujących w oparciu o dane pobierane z rejestrów publicznych, takich jak aplikacja mObywatel czy Zintegrowana Platforma Analityczna.

Jak wynika z wypracowanego w trakcie prac Komitetu Rady Ministrów do spraw Cyfryzacji dokumentu „Dobre praktyki AIP tworzenia rejestrów publicznych”, **także Ministerstwo Cyfryzacji dostrzega konieczność lepszego uregulowania w przepisach rozwiązań dotyczących tworzenia rejestrów publicznych w pewnych aspektach**[19].

W ostatnim czasie Prezes UODO przedstawiał też przy różnych okazjach potrzebę brania pod uwagę problematyki stosowania rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia (EHDS), podkreślając, że „udostępnianie i dalsze wtórne wykorzystywanie danych osobowych oraz danych nieosobowych dotyczących zdrowia przetwarzanych w publicznych rejestrach – zgodnie z regulacjami dotyczącymi wtórnego przetwarzania danych – ma istotne znaczenie z punktu widzenia zarówno interesów państwa, jak i interesów (także zbiorowych) osób fizycznych (w szczególności pacjentów), których dane dotyczą, w tym w kontekście wynikającego z EHDS obowiązku wtórnego wykorzystania elektronicznych danych dotyczących zdrowia”[20].

Poszczególni **administratorzy sprawujący władztwo nad rejestrami publicznymi również informują organ nadzorczy o wątpliwościach dotyczących umocowania prawnego rozwiązań dotyczących rejestrów publicznych**,

[17] System Ewidencji Państwowej Inspekcji Sanitarnej.
[18] Administratorem Systemu Obsługi Wsparcia jest Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych (PFRON).
[19] Dobre praktyki AIP tworzenia rejestrów publicznych , Rekomendacje Ministra Cyfryzacji , wersja 1.3, 18.01.2024 r., https://www.gov.pl/web/ia/rejestry-publiczne-dobre-praktyki-architektoniczne-i-legislacyjne
[20] Zob. Opinia Prezesa Urzędu Ochrony Danych Osobowych z 7 lipca 2025 r. do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (znak: DPNT.401.224.2025).

zwłaszcza w kontekście orzecznictwa sądów międzynarodowych. Przykładem może być pismo Ministra Sprawiedliwości zgłaszającego wątpliwości odnośnie do przetwarzania danych osobowych w Rejestrze Sprawców na Tle Seksualnym[21], a także pismo Ministra Sprawiedliwości dotyczące dostępu do baz danych ksiąg wieczystych[22] oraz jego konsekwencje w postaci trwającego aktualnie procesu legislacyjnego (projekt ustawy o zmianie ustawy o księgach wieczystych i hipotece – UD310).

Z tych względów, **w ocenie Prezesa UODO istnieje pilna potrzeba dokonania komplementarnej oceny przyjętego w Polsce systemu tworzenia i funkcjonowania rejestrów publicznych w zakresie ochrony przetwarzanych w nich danych osobowych**. Rejestry publiczne – zarówno pod względem podstaw prawnych, jak i pod względem merytorycznym – wymagają zwłaszcza szczegółowego przeglądu pod kątem wdrażania nowych unijnych aktów prawnych związanych z przetwarzaniem danych osobowych, sposobu realizacji wynikających z rozporządzenia 2016/679 norm i zasad, a także analizy rozwiązań przyjętych w rejestrach pod kątem ich cyberbezpieczeństwa. Istotne znaczenie mają rejestry publiczne szczególnie w kontekście stosowania przepisów regulujących zagadnienie zarządzania danymi, czy też związane z ponownym wykorzystywaniem informacji sektora publicznego. Właściwe wykorzystywanie tak potężnego potencjału informacyjnego rejestrów publicznych musi jednak uwzględniać także poszanowanie podstawowych konstytucyjnych praw podmiotów danych, zwłaszcza że dane umieszczone w rejestrach służyć miały pierwotnie ściśle określonym celom.

Dlatego też **rejestry publiczne powinny być już na etapie projektowania przygotowane, także pod względem prawnym, z uwzględnieniem ryzyk w sferze ochrony danych osobowych oraz celem zapewnienia zgodności z prawem unijnym i krajowym**. Przykładowo, zaprojektowany nieadekwatny zakres danych, czy luki w regulacjach wpływać będą na dalsze wykorzystywanie danych zgromadzonych w rejestrach przez kolejnych administratorów.

II. Uwagi ogólne.

W celu zapewnienia realizacji postulowanych działań konieczne jest dokonanie **przeglądu funkcjonujących rejestrów publicznych i dobrego zaprojektowania nowych**. W pierwszej kolejności przegląd taki powinien polegać na szczegółowej **inwentaryzacji** istniejących rejestrów publicznych. Na podstawie wyników inwentaryzacji istotne byłoby dokonanie oceny przepisów prawa, na podstawie których rejestry są prowadzone, w ramach której należy zwrócić uwagę przede wszystkim na następujące problemy:

1. **Identyfikacja i właściwe przypisanie ról w procesach przetwarzania danych podmiotów prowadzących rejestry, i innych podmiotów**

[21] Pismo dyrektora Departamentu Analiz i Strategii Ministerstwa Sprawiedliwości z 12 sierpnia 2024 r. (znak : DAiS.0810.4.2024).
[22] Pismo Sekretarza Stanu w Ministerstwie Sprawiedliwości z 2 sierpnia 2024 r. (znak: DPCiG-III.412.5.2024).

publicznych przetwarzających dane pochodzące z rejestrów, kompletność regulacji tych procesów przetwarzania, z zachowaniem wynikających z art. 5 rozporządzenia 2016/679 zasad przetwarzania danych osobowych[23], w szczególności zasad: zgodności z prawem, rzetelności i przejrzystości, jak i rozliczalności;

2. **Ocena zawartości danych osobowych w rejestrach publicznych** pod kątem ich faktycznej niezbędności – zasady adekwatności, minimalizacji danych – jak również autentyczności i prawidłowości zebranych w nich danych. Nie kwestionując uprawnień organów władzy publicznej do pozyskiwania danych osobowych obywateli i innych osób fizycznych funkcjonujących w państwie, w tym danych o charakterze sensytywnym, w celu realizacji zadań państwa należy wskazać, że organy te jednak nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym, co wprost wskazano w art. 51 ust. 2 Konstytucji RP. Niezwykle ważna jest zwłaszcza ocena zasadności przetwarzania w rejestrach publicznych danych **szczególnych kategorii**, co do zasady objętych zakazem przetwarzania (art. 9 ust. 1)[24], chyba że spełniony jest jeden z warunków legalizujących przetwarzanie takich danych z art. 9 ust. 2 rozporządzenia 2016/679 oraz uwzględnione są warunki z ust. 3 i 4 tego artykułu. Analogicznie, szczególnej uwagi wymaga też przetwarzanie w rejestrach publicznych danych osobowych dotyczących **wyroków skazujących i czynów zabronionych** (art. 10 rozporządzenia 2016/679[25]), a

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

[24] 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.

[25] Zgodnie z art. 10 rozporządzenia 2016/679 - Przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na

także **danych osobowych objętych szczególną ochroną na podstawie przepisów krajowych** (np. dane osobowe w dokumentacji medycznej objęte tajemnicą lekarską czy informacje o osobach korzystających ze świadczeń opieki społecznej objęte tajemnicą zawodową). Rejestry publiczne, których struktura i zakres przetwarzanych w nich danych osobowych zostały odpowiednio zaprojektowane, a dane w nich zawarte są właściwie zabezpieczone służą wypełnianiu i realizacji zadań państwa w szeregu obszarach jego działalności oraz w odniesieniu do różnorodnych dziedzin życia. Przykładowo, dzięki rejestrom publicznym, w których przetwarzane są dane dotyczące zdrowia na podstawie przepisów ustawy o systemie informacji w ochronie zdrowia[26] może być realizowana polityka zdrowotna państwa, a dodatkowo dane te umożliwiają działania w ramach podnoszenia jakości i dostępności świadczeń opieki zdrowotnej, jak również mogą być wykorzystywane wtórnie zgodnie z regulacjami EHDS i odpowiednio ukształtowanym prawem krajowym służącym realizacji tego aktu;

3. **Ocena roli podmiotów i organów zaangażowanych w przetwarzanie danych osobowych w rejestrach publicznych,** w tym sposobu zasilania rejestrów i zasad eksploatacji danych w nich zawartych. Ma to istotne znaczenie dla właściwego określenia celów i sposobów przetwarzania danych w konkretnym rejestrze publicznym, a tym dla samym przejrzystego ukształtowania ról poszczególnych podmiotów i organów w procesach przetwarzania danych zawartych w takich rejestrach. Organ nadzorczy dostrzega wiele problemów, których źródłami są: nieprecyzyjne, niewystarczające a nawet niekiedy błędne określanie celów, zadań i kompetencji podmiotów i organów dla procesów przetwarzania danych osobowych w rejestrach publicznych (administratorzy, współadministratorzy, podmioty przetwarzające), sygnalizowane również przez UODO w poszczególnych procesach legislacyjnych[27]. W swoich opiniach legislacyjnych Prezes Urzędu Ochrony Danych Osobowych wskazywał m.in., że: konieczne jest doprecyzowanie w normach prawnych jaką faktycznie rolę pełni „administrator systemu" w procesie przetwarzania danych w tym systemie, w szczególności gdy miałoby dochodzić do współadministrowania danymi; dookreślić trzeba na czym polega współadministrowanie w konkretnym przypadku, jak kształtują się zakresy odpowiedzialności za dane poszczególnych podmiotów biorących udział w przetwarzaniu danych; przepisy ustawy powinny określać obowiązki współadministrotorów, a nie

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.

[26] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2025 r. poz. 302 ze zm.), dalej: ustawa o systemie informacji w ochronie zdrowia.

[27] Zob. Opinia Prezesa Urzędu Ochrony Danych Osobowych z 2 grudnia 2024 r. do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (znak: DOL.401.486.2024).

pozostawiać je do swobodnej decyzji tym podmiotom, zwłaszcza, że realizują one zadania w interesie publicznym i powinny działać na podstawie i w granicach przejrzystych i wyczerpujących przepisów prawa[28]. Jednocześnie należy zwrócić uwagę na zagadnienie braku odpowiedniego kształtowania w ustawach instytucji powierzenia na podstawie instrumentu prawnego co w rezultacie prowadzi do odsyłania przez organy i instytucje publiczne do porozumień jako podstaw do udostępniania danych i wymiany pomiędzy różnymi rejestrami. Brak odpowiedniego ukształtowania powierzenia przetwarzania jest widoczny od wielu lat np. w regulacjach przepisów ustawy o systemie informacji w ochronie zdrowia[29], w którym to akcie prawnym nie została uregulowana właściwie rola poszczególnych uczestników procesów przetwarzania danych osobowych. W szczególności jednostka właściwa w zakresie systemów informacyjnych ochrony zdrowia w stosunku do ministra właściwego do spraw zdrowia nie powinna być uznana za podmiot przetwarzający, z którym regulacje są kształtowane na podstawie umowy powierzenia, ale za współadministratora.

4. **Ocena przyjętego modelu jawności danych zgromadzonych w rejestrach publicznych**, zwłaszcza w aspekcie upubliczniania numeru PESEL. Na problem ten organ nadzorczy zwracał uwagę w dużej liczbie stanowisk[30]. Numer PESEL jako krajowy numer identyfikacyjny zgodnie z art. 87 rozporządzenia 2016/679 powinien być używany wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, przy czym istotne są także zabezpieczenia regulacyjne, a nie tylko fizyczne czy organizacyjne. Dlatego też rozwiązania przyjęte dla rejestrów publicznych, w których przetwarzany jest numer PESEL nie powinny prowadzić do upubliczniania tego numeru identyfikacyjnego ze względu na szereg ryzyk dla osób fizycznych (związanych np. z kradzieżą tożsamości czy oszustwami popełnianymi przy wykorzystaniu danych osobowych przez osoby czy podmioty trzecie). Organ nadzorczy kwestionował takie rozwiązania wielokrotnie, m.in. w opiniach legislacyjnych. Jako przykład można wskazać prace nad projektem ustawy o Krajowym Rejestrze Zadłużonych, w trakcie których organ zgłosił uwagi do modelu przetwarzania danych osobowych w Krajowym Rejestrze Zadłużonych, polegającego na upublicznianiu w Internecie informacji o dłużnikach będących osobami fizycznymi wraz z ich numerami PESEL[31]. Podobny model, zakładający ujawnienie w rejestrze publicznym i upublicznienie numerów PESEL, Prezes UODO kwestionował w toku prac legislacyjnych nad poselskim projektem ustawy o zmianie niektórych

[28] Zob. Opinia Prezesa Urzędu Ochrony Danych Osobowych z 7 lipca 2025 r. do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (znak: DPNT.401.224.2025).
[29] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2025 r. poz. 302 ze zm.), dalej: ustawa o systemie informacji w ochronie zdrowia.
[30] Pismo organu nadzorczego z 14 czerwca 2019 r. (znak: ZSPU.023.97.2019.PM).
[31] Opinia Generalnego Inspektora Ochrony Danych Osobowych z 29 września 2017 r. do projektu ustawy o Krajowym Rejestrze Zadłużonych (znak: DOLiS-023-413/17/TG/73042).

ustaw w celu naprawy ładu korporacyjnego w spółkach z udziałem Skarbu Państwa (druk nr 261)[32]. Problem upubliczniania numerów PESEL był również podnoszony w korespondencji skierowanej do Głównego Geodety Kraju ze wskazaniem zagrożenia jakie niesie zamieszczenie numerów ksiąg wieczystych w Geoportalu[33]. Także w orzecznictwie sądowym podkreśla się negatywne skutki udostępnienia numerów PESEL z rejestrów publicznych. Naczelny Sąd Administracyjny w wyroku z 3 grudnia 2021 r., sygn. akt III OSK 590/21, który dotyczył udostępniania komornikom danych osobowych z rejestru PESEL przez Ministra Cyfryzacji wskazał, że „zróżnicowanie podmiotów uprawnionych do dostępu do rejestru PESEL nie może powodować zaniechania przez administratora danych podejmowania działań zmierzających do zlikwidowania (lub co najmniej ograniczenia) zidentyfikowanego ryzyka dla danych przetwarzanych w ramach rejestru PESEL". **Obecny model jawności numeru PESEL cechuje wewnętrzna sprzeczność, którą w istocie można uznać za prowadzącą do „schizofreniczności" ochrony danych w zakresie PESEL w Polsce**, gdyż z jednej strony ustawodawca wprowadza przepisy wysoce gwarancyjne dla ochrony tego identyfikatora w zw. z art. 87 rozporządzenia 2016/679, tak jak w przepisach ustawy o ewidencji ludności[34], gdzie zamieszczono przepisy umożliwiające zastrzeżenie PESEL lub w ustawie o dokumentach publicznych, która chroni dokumenty zawierające PESEL[35]. Z drugiej strony ta sama dana osobowa jest jawna i powszechnie dostępna w licznych rejestrach publicznych często wieczyście bez prawa do żądania zaprzestania jego publikacji. Taka sytuacja nie buduje zaufania społecznego do państwa i prezentowanej w ten sposób koncepcji ochrony prywatności. Jednocześnie taki stan rzeczy – w obliczu eskalacji działań zewnętrznych wymierzonych przeciwko bezpieczeństwu państwa polskiego – budzi poważne zaniepokojenie nie tylko osób prywatnych ale i osób publicznych, czy przedstawicieli osób prawnych, których dane w tym zakresie mogą być wykorzystywane w celach zagrażających ich interesom i interesom publicznym.

5. **Ocena przyjętych w niektórych rejestrach publicznych rozwiązań dotyczących dostępu do danych, ich** (często nieprzejrzyście określonej) **wymiany, wykorzystywania przez innych administratorów niż prowadzący rejestr i tzw. teletransmisji** w kontekście zasady rozliczalności poszczególnych administratorów oraz pod kątem ryzyk dla administratorów związanych z łączeniem baz danych (por. motyw 31 rozporządzenia

[32] Zob. przebieg prac nad poselskim projektem ustawy o zmianie niektórych ustaw w celu naprawy ładu korporacyjnego w spółkach z udziałem Skarbu Państwa (druk nr 261), https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=261

[33] Zob. Pismo Prezesa Urzędu Ochrony Danych Osobowych do Głównego Geodety Kraju z 18 stycznia 2019 r. (znak: ZSPU.070.1.2019.PA).

[34] Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2025 r. poz. 274 ze. zm.), dalej: ustawa o ewidencji ludności.

[35] Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 ze zm.), dalej: ustawa o dokumentach publicznych.

2016/679[36]). Zagadnienie to było również sygnalizowane w poszczególnych procesach legislacyjnych, w trakcie których organ nadzorczy przedstawiał stanowisko krytyczne odnośnie do stosowania takich rozwiązań bez wykazania ich niezbędności, a czasem nawet bez uzasadnienia[37]. Jednocześnie organ zauważył, że nie są w takich przepisach zmieniane przepisy prawa celem wprowadzenia mechanizmów prawnych dla kontroli nad faktycznymi celami, w jakich dane są pozyskiwane i później wykorzystywane.

6. **Ocena wpływu aktów prawa Unii Europejskiej na rejestry publiczne** – **wchodzą w życie** nowe akty prawa, które zmieniają modele przetwarzania danych osobowych, regulują wtórne wykorzystywanie danych już zgromadzonych, określają nowe standardy w zakresie cyberbezpieczeństwa, czy regulują zasady wykorzystywania systemów sztucznej inteligencji w przestrzeni publicznej (w szczególności: przepisy aktu w sprawie sztucznej inteligencji, aktu w sprawie zarządzania danymi, aktu o usługach cyfrowych, aktu w sprawie danych, rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia, czy też implementacji dyrektywy 2016/1148). Przyjęte w tych aktach rozwiązania i niezbędne niekiedy towarzyszące im zmiany w prawie krajowym będą miały ogromny wpływ na dalszy rozwój i kształt cyfryzacji w Polsce. Efektem oczekiwanym takiej oceny jest to, by rejestry publiczne były dostosowane nie tylko do aktualnych norm technologicznych, ale także wynikających z prawa unijnego nowych rozwiązań prawnych w obszarze przetwarzania danych osobowych.

III. Uwagi dodatkowe.

Przy projektowaniu i kształtowaniu treści przepisów, a także sposobów przetwarzania danych, także wtórnego ich wykorzystywania i rozwiązań technologicznych w konkretnych rejestrach publicznych, nie mniej istotne jest uwzględnienie poniżej wskazanych wymagań w celu zapewnienia zgodności z przepisami rozporządzenia 2016/679 oraz eliminowania ryzyk dla praw podmiotów danych.

1. Ocena skutków dla ochrony danych w trakcie projektowania rejestrów publicznych.

[36] W motywie 31 rozporządzenia 2016/679, zdanie drugie podkreśla się, że : 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.

[37] Zob. Opinia Prezesa Urzędu Ochrony Danych Osobowych z 26 maja 2021 r. do projektu ustawy o uprawnieniach artysty zawodowego (znak: DOL.401.201.2021), także opinia Prezesa Urzędu Ochrony Danych Osobowych z 13 stycznia 2022 r. do projektu ustawy o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw (znak: DOL.401.605.2020).

Jednym z mechanizmów służących wypracowywaniu rozwiązań zgodnych z rozporządzeniem 2016/679 w projektowanych przepisach dotyczących rejestrów publicznych jest przeprowadzenie już w procesie legislacyjnym, a zatem już na etapie tworzenia rozwiązań, wskazanej w **art. 35** rozporządzenia 2016/679 **oceny skutków dla ochrony danych** – aspekt wielokrotnie wskazywany w opiniach legislacyjnych organu nadzorczego, jak i w osobnym wystąpieniu skierowanym do przewodniczącego Komitetu Stałego Rady Ministrów[38]. W odpowiedzi na przedmiotowe wystąpienie o ustawowych gwarancjach dotyczących obowiązku przedstawiania projektowanych regulacji dotyczących danych osobowych do zaopiniowania organowi do spraw ochrony danych osobowych wypowiedział się przewodniczący Komitetu Stałego Rady Ministrów (pismo z 31 marca 2025 r.[39]) podkreślając, że gwarancje te znajdują także swoje odzwierciedlenie w przepisach Regulaminu pracy Rady Ministrów. Zgodnie bowiem z § 38 ust. 1 pkt 3 Regulaminu pracy RM każdy projekt dokumentu rządowego, który dotyczy danych osobowych, powinien zostać skierowany do zaopiniowania przez Prezesa Urzędu Ochrony Danych Osobowych". Przewodniczący Komitetu wskazał również, że: „Gwarancję realizacji tego obowiązku stanowi natomiast regulacja § 21a Regulaminu pracy RM, która zobowiązuje Rządowe Centrum Legislacji do weryfikowania wykonania przez organ wnioskujący obowiązków związanych z przekazaniem projektu do zaopiniowania". Potrzeba dokonywania oceny skutków dla ochrony danych była również sygnalizowana w piśmie organu nadzorczego skierowanym do Minister Funduszy i Polityki Regionalnej[40].

Ocena skutków powinna zatem 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

[38] Wystąpienie Prezesa Urzędu Danych Osobowych do Przewodniczącego Komitetu Stałego Rady Ministrów z 14 lutego 2025 r. (znak: DOL.413.15.2024) z wnioskiem o podjęcie działań legislacyjnych mających na celu uzupełnienie Regulaminu pracy Rady Ministrów w zakresie obowiązku sporządzenia OSR prywatności do projektowanych aktów normatywnych, celem zapewnienia dostosowania ich do przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

[39] Pismo Pana Ministra Macieja Berka Ministra, Przewodniczącego Komitetu Stałego Rady Ministrów z 31 marca 2025 r. znak: DPPR.WPPR.0635.1.2025. W niniejszym piśmie Pan Minister wskazał m.in, że „drugim narzędziem, ustanowionym w przepisach prawa, które ma na celu zagwarantowanie odpowiedniego standardu ochrony danych osobowych w projektowanych regulacjach, jest wyrażony w art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych obowiązek przekazywania założeń i projektów aktów prawnych dotyczących danych osobowych do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych. Dodatkowo kompetencje do opiniowania projektów przekazanych przez Prezesa Urzędu Ochrony Danych Osobowych posiada również Rada do Spraw Ochrony Danych Osobowych. Te ustawowe gwarancje znajdują swoje odzwierciedlenie w przepisach Regulaminu pracy RM. Zgodnie bowiem z § 38 ust. 1 pkt 3 Regulaminu pracy RM każdy projekt dokumentu rządowego, który dotyczy danych osobowych, powinien zostać skierowany do zaopiniowania przez Prezesa Urzędu Ochrony Danych Osobowych. Gwarancję realizacji tego obowiązku stanowi natomiast regulacja § 21a Regulaminu pracy RM, która zobowiązuje Rządowe Centrum Legislacji do weryfikowania wykonania przez organ wnioskujący obowiązków związanych z przekazaniem projektu do zaopiniowania.".

[40] Pismo Prezesa Urzędu Danych Osobowych do Ministra Funduszy i Polityki Regionalnej z 20 lutego 2025 r. (znak: DPNT.071.4.2025).

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 (art. 35 ust. 7 rozporządzenia 2016/679).

Przyjęte 4 kwietnia 2017 r., ale nadal aktualne Wytyczne Grupy roboczej Art. 29 (poprzedniczka Europejskiej Rady Ochrony Danych – EROD), 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 wybierania metodyki dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 do wytycznych. Wynik prawidłowo przeprowadzonej oceny skutków dla ochrony danych pozwala projektującym przepisy dotyczące rejestrów publicznych na ustalenie, czy planowane i przyjmowane w odniesieniu do przetwarzania danych rozwiązania przewidziane w projekcie ustawy/ustaw są proporcjonalne do zakładanego celu pod kątem ochrony danych. W istocie więc taka ocena powinna być niezbędnym elementem wdrażania rozwiązań dotyczących przetwarzania danych w rejestrach publicznych do polskiego porządku prawnego.

2. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych w trakcie projektowania rejestrów publicznych.

Istotne znaczenie w projektowaniu rejestrów publicznych, oprócz ww. oceny skutków dla ochrony danych, powinny mieć także mechanizmy: **uwzględniania ochrony danych w fazie projektowania** (art 25 ust. 1)[41] oraz **domyślnej ochrony danych** (art. 25 ust. 2 rozporządzenia 2016/679[42]). W związku z tym, że w rejestrach publicznych przetwarzane są często dane osobowe o charakterze sensytywnym oraz na dużą czy wręcz wielką skalę, wskazać należy na niezbędność uwzględniania mechanizmów przewidzianych w art. 25 ust. 1 i 2 rozporządzenia 2016/679 już w fazie określenia sposobów przetwarzania tych danych, np. przy ocenie założeń

[41] 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.

[42] 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 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.

projektów informatycznych[43] dotyczących tych rejestrów. Informacje dotyczące zastosowania ww. mechanizmów powinny zostać niewątpliwie uwzględnione także w uzasadnieniu do projektów aktów prawnych regulujących podstawy prawne przetwarzania danych osobowych w rejestrach publicznych. W tym kontekście niezwykle istotna jest współpraca organu nadzorczego z Komitetem do spraw Cyfryzacji[44], która przyczynia się do wprowadzania procedur i dobrych praktyk przy tworzeniu projektów informatycznych[45] oraz stanowisko Sekretarza Komitetu Rady Ministrów do spraw Cyfryzacji[46], w którym zadeklarowano rozszerzenie zakresu informacji przedkładanych Komitetowi odnośnie do przetwarzanych w ramach projektów informatycznych danych osobowych, zmiany wzoru opisu założeń projektów informatycznych (OZPI), zaangażowanie dodatkowych osób wspierających proces opiniowania projektów informatycznych pod kątem ochrony danych osobowych oraz uwzględniania innych sugestii organu nadzorczego w ramach opiniowania projektów informatycznych.

3. Zmiana celów przetwarzania w stosunku do danych osobowych w rejestrach publicznych.

Ustawodawca, projektując przepisy regulujące przetwarzanie danych osobowych w rejestrach publicznych zgodnie z zasadami: przejrzystości, celowości i minimalizacji danych, powinien w sposób precyzyjny określić cele, dla realizacji których dane te będą przetwarzane. Organy państwa, dla realizacji obowiązków i zadań publicznych nie mogą w dowolny sposób korzystać z danych osobowych dotyczących obywateli (ew. innych osób fizycznych zobowiązanych czy uprawnionych), zgromadzonych i dalej przetwarzanych w rejestrach gdyż takie działanie naruszałoby zasadę legalizmu. W pierwszej kolejności, w myśl konstytucyjnej zasady legalizmu powinny kierować się wiążącymi je, konkretnymi przepisami prawa a zmiana pierwotnych celów do jakich dane zostały pozyskane na potrzeby konkretnego rejestru – zgodnie z art. 6 ust. 4 rozporządzenia 2016/679[47] –

[43] Procedowanych na podstawie zarządzenia nr 48 Prezesa Rady Ministrów z dnia 12 kwietnia 2016 r. w sprawie Komitetu Rady Ministrów do spraw Cyfryzacji (M. P. poz. 379 ze zm.).
[44] Poprzednio z Komitetem Rady Ministrów do spraw Cyfryzacji.
[45] Pismo Prezesa Urzędu Ochrony Danych Osobowych z 13 stycznia 2025 r. (znak: 071.42.2024.WL.OJ).
[46] Pismo Sekretarza Komitetu Rady Ministrów do spraw Cyfryzacji z 31 stycznia 2025 r. (znak: DPiS.WWKS.501.1.1.2025).
[47] Zgodnie z art 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;

może następować jedynie na podstawie prawa stanowiącego w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu jedynie celów, o których mowa w art. 23 ust. 1 rozporządzenia 2016/679[48] oraz z uwzględnieniem zasad i warunków z tego artykułu wynikających. W ocenie organu nadzorczego należy rozważyć wprowadzenie do systemu prawnego rozwiązań, które będą pozwalałyby administratorom w takich przypadkach na zachowanie kontroli uprzedniej celów, dla których dane są udostępniane. Rozwiązania takie powinny zostać wbudowane w projektowane systemy, co pozwoliłoby lepiej kontrolować i sprawować nadzór nad danymi osobowymi udostępnianymi z rejestrów, a zwłaszcza gdy odbywa się to w sposób zautomatyzowany. W ramach udostępniania danych osobowych z rejestrów w ramach trybu bezwnioskowego dostrzegalnym problemem jest zasadniczo brak wymogu podjęcia działań umożliwiających administratorom na bieżąco monitorować podmioty, które w trybie wniosku uproszczonego będą pozyskiwać i mieć dostęp do danych osobowych przetwarzanych w danym rejestrze. Taka sytuacja powoduje w praktyce, że administratorzy nie czują się zobowiązani do stałej kontroli udostępnianych danych osobowych i uznają, że ciężar odpowiedzialności za takie przetwarzanie spoczywa wyłącznie na pozyskujących dane. Nie jest to koncepcja zgodna z rozporządzeniem 2016/679, z uwagi na definicję administratora i zasady jego odpowiedzialności wypływające z art. 5 rozporządzenia 2016/679, co potwierdziło powoływane wyżej orzecznictwo krajowe i europejskie.

4. Retencja i zapewnienie prawidłowości danych osobowych pozyskiwanych z rejestru publicznego.

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.

[48] 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 celom 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.

Istotnym elementem, który powinien być uwzględniony w przepisach regulujących przetwarzanie danych osobowych w rejestrach publicznych jest zapewnienie, że **odbywa się ono tylko w określonym czasie, a przepisy określają tzw. retencję danych**. Prawidłowe uwzględnienie tego aspektu powinno odnosić się do kategorii, rodzaju i specyfiki danych osobowych oraz celów przetwarzania danych tak, by zapewnić stosowanie **zasad ograniczenia przechowania, legalizmu** oraz **ograniczenia celu**[49]. Dodatkowo w ramach prawidłowo zaplanowanej retencji należy przeanalizować sytuacje, w których ma miejsce bezterminowe przetwarzanie danych w rejestrach, co jest istotne z uwagi na określone w RODO prawo do bycia zapomnianym (art. 17). Należy także przeanalizować cele takiego przetwarzania i ustalić niezbędny zakres danych pamiętając, że dane osobowe archiwalne co do zasady nie powinny być powszechnie dostępne zgodnie z przepisami o archiwach państwowych. Niestety praktyka wskazuje, że zdarzają się sytuacje, gdy w rejestrach są przetwarzane dane nieaktualne i nieprawidłowe.

Istotne jest także zapewnienie prawidłowości danych przetwarzanych w rejestrze publicznym. Organ nadzorczy, analizując model powszechnej dostępności danych osobowych osób fizycznych będących przedsiębiorcami zamieszczonych w Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), dostrzega w tym kontekście poważny problem, gdy adres prowadzonej działalności jest tożsamy z adresem zamieszkania przedsiębiorcy, albo gdy dane byłego przedsiębiorcy dotyczące jego miejsca zamieszkania nadal pozostają przez wiele lat upublicznione, co generuje szereg ryzyk dla prywatności takiej osoby[50]. Jednocześnie jak zwraca się uwagę w orzecznictwie Trybunału Sprawiedliwości także udostępnienie z dzienników urzędowych imienia, nazwiska, podpisu i danych kontaktowych osoby fizycznej reprezentującej osobę prawną stanowi przetwarzanie danych osobowych. Bez znaczenia w tym względzie jest okoliczność, że udostępnienia tego dokonano wyłącznie w celu umożliwienia zidentyfikowania osoby fizycznej upoważnionej do działania w imieniu osoby prawnej [51].

5. Zautomatyzowane podejmowanie decyzji, w tym profilowanie oraz wykorzystanie sztucznej inteligencji a przetwarzanie danych osobowych w rejestrach publicznych.

Przepisy prawa powinny jednoznacznie określać czy w związku z przetwarzaniem danych w rejestrze publicznym dokonywane będzie

[49] Zob. Opinia Prezesa Urzędu Ochrony Danych Osobowych z 24 października 2024 r. do projektu ustawy o zmianie ustawy o narodowym zasobie archiwalnym i archiwach (znak: DOL.401.392.2024).
[50] Zob. Wystąpienie Prezesa Urzędu Ochrony Danych Osobowych do Ministra Finansów i Gospodarki z 4 sierpnia 2025 r. z wnioskiem o podjęcie działań legislacyjnych mających na celu rewizję funkcjonującego obecnie modelu powszechnej dostępności danych osobowych osób fizycznych będących przedsiębiorcami zamieszczonych w Centralnej Ewidencji i Informacji o Działalności Gospodarczej (znak: DPNT.413.32.2025.WL.MP).
[51] Wyrok Trybunału Sprawiedliwości z 3 kwietnia 2025 r., L. H. v Ministerstvo zdravotnictví, C-710/23, EU:C:2025:231.

zautomatyzowane podejmowania decyzji w indywidualnych sprawach, w tym profilowanie osób w rozumieniu art. 4 pkt 4 rozporządzenia 2016/679[52]. Takie działania wymagają stworzenia warunków wymaganych dla takich procesów przepisami rozporządzenia 2016/679[53]. Sam fakt, że w danym rejestrze publicznym w konkretnych celach zgromadzone są i przetwarzane dane osób fizycznych nie uprawnia do wykorzystywania tych danych dla profilowania i tworzenia danych wywnioskowanych, np. w trakcie czynności analitycznych prowadzonych przez administratora lub inny podmiot. Ponadto okoliczność, że dany organ publiczny ma prawo do zautomatyzowanego przetwarzania danych osobowych w określonych w sposób ogólny celach związanych z jego działaniem nie oznacza, że organ ten ma prawo do przetwarzania danych osobowych w rejestrze publicznym bez odrębnej dedykowanej zautomatyzowanemu przetwarzaniu danych osobowych w tym konkretnym rejestrze podstawy prawnej, określającej prawa i obowiązki podmiotu odpowiedzialnego a nie rejestru / systemu jako takiego. W motywie 71 rozporządzenia 2016/679 dodatkowo doprecyzowano, że aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiec m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny lub orientację seksualną, lub przetwarzaniu skutkującemu środkami mającymi taki efekt. Administratorzy rejestrów publicznych powinni zatem stosować automatyczne przetwarzanie danych osobowych jedynie w wyjątkowych i zgodnych z prawem sytuacjach przy poszanowaniu interesów i praw osób, które dane dotyczą.

Także **wykorzystanie narzędzi sztucznej inteligencji** dla przetwarzania danych osobowych w rejestrze publicznym powinno mieć odzwierciedlenie w przepisie prawa. Warto podkreślić, że akt w sprawie sztucznej inteligencji w art. 5 wprowadza katalog zakazanych praktyk w zakresie AI co wyklucza stosowanie tych praktyk. Należy także wziąć również pod uwagę opinię EROD przyjętą 17 grudnia 2024 **w sprawie wykorzystywania danych osobowych do opracowywania i**

[52] Zgodnie z art. 4 pkt 4 rozporządzenia 2016/679 "profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

[53] 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.

wdrażania modeli sztucznej inteligencji[54]. W opinii tej EROD podkreśliła, że administratorzy muszą przeprowadzić trójstopniowy test, aby udowodnić, że uzasadniony interes stanowi odpowiednią podstawę prawną dla przetwarzania danych osobowych w fazach rozwoju i wdrożenia modeli AI.

Oceniając jakie mechanizmy sztucznej inteligencji będą mogły mieć zastosowanie w konkretnym rejestrze publicznym, należy przede wszystkim uwzględnić wprowadzane obecnie do polskiego porządku prawnego rozporządzenie 2024/1689. Jednocześnie podkreślenia wymaga, że wykorzystanie rejestrów publicznych do trenowania algorytmów AI wymaga stworzenia odrębnych przepisów prawa dających na to przyzwolenie. Istotne jest także przeprowadzenie oceny skutków dla ochrony danych, która to czynność nie jest tożsama z dokonaniem oceny wynikającej z art. 27 aktu w sprawie sztucznej inteligencji[55], choć te dwie oceny mogą ze sobą być połączone. Ma to niezwykle istotne znaczenie przy przetwarzaniu danych szczególnych kategorii (art. 9) oraz danych z dotyczących wyroków skazujących i czynów zabronionych (art. 10 rozporządzenia 2016/679)[56].

6. Bezpieczeństwo, prawidłowość, poufność i integralność danych osobowych w trakcie użytkowania rejestrów publicznych, w tym w sytuacjach zagrożenia bezpieczeństwa państwa.

Ustawodawca powinien gwarantować prawidłowość, integralność i poufność przetwarzania danych w rejestrze publicznym, czego wymagają zasady ochrony danych osobowych. W tym celu rejestr publiczny powinien być odpowiednio zaprojektowany zarówno pod kątem technicznym, jak i przede wszystkim podstaw oraz otoczenia prawnego. W kontekście ww. zasad szczególne ważne jest zapewnienie również spełnienia wymagań z zakresu cyberbezpieczeństwa w rozumieniu rozwiązań technologicznych i organizacyjnych wskazanych m.in. w ustawie o krajowym systemie cyberbezpieczeństwa[57]. Przepisami rozporządzenia 2016/679 nałożony został na wykonawców norm szereg obowiązków związanych z przekazywaniem danych osobowych podmiotom przetwarzającym (np. w ramach usługi chmurowej). Tworzenie regulacji zezwalających (wprost lub poprzez interpretację przepisów niejednoznacznych) na (pozaustawowe) powierzenie innemu podmiotowi zadań związanych z przetwarzaniem danych osobowych w kontekście szczególnego znaczenia zapewnieniu bezpieczeństwa informacji w rejestrach

[54] Zob. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

[55] Ocena skutków systemów AI wysokiego ryzyka dla praw podstawowych.

[56] Zob. wystąpienie Prezesa Urzędu Ochrony Danych Osobowych do Ministra Zdrowia i Ministra Nauki i Szkolnictwa Wyższego z 1 września 2025 r. dotyczące problemów związanych ze stosowaniem i wykładnią przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz ustawy Prawo o szkolnictwie wyższym i nauce w kontekście wykorzystywania zasobów danych medycznych, w tym zindywidualizowanych w celach badań naukowych (znak: DPNT.413.39.2025.WL.MKS).

[57] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 ze zm.).

publicznych jest natomiast kontrowersyjne. Niezbędne jest, aby dane były przekazywane tylko do podmiotów gwarantujących spełnienie jedynie takich środków technicznych i organizacyjnych, które są odpowiednie do zagrożeń, ryzyk, technologii, charakteru, zakresu, kontekstu, celów przetwarzania danych w rejestrze publicznym. Konstytucyjna zasada praworządności wymaga by podmioty publiczne działały na podstawie i w granicach wiążących je przepisów prawa. Zatem ewentualne powierzenie przetwarzania danych osobowych powinno zostać poddane szczególnej analizie pod kątem oszacowania wszystkich ryzyk, także w zakresie podstaw prawnych rozwiązań przyjmowanych w zakresie praw i obowiązków podmiotów publicznych. Co do bezpieczeństwa, konieczne jest podjęcie minimum środków wymaganych mocą przepisów rozporządzenia 2016/679 (np. przez pseudonimizację lub szyfrowanie).

Istotnym zagadnieniem jest również **problematyka zapewnienia szczegółowych procedur ochrony danych osobowych w trakcie użytkowania rejestrów publicznych**. Znaczenie rejestrów publicznych i ich specyfika wymagają bowiem, by zasoby te objęte były kompleksowymi procedurami, w tym dotyczącymi ochrony danych osobowych, uwzględniającymi przepisy rozporządzenia 2016/679 a także przepisy prawa krajowego wydane w celu stosowania lub implementacji prawa europejskiego. Dokonywane powinny być również systematyczne przeglądy tych procedur i ich skuteczność. Istotne jest w szczególności stosowanie mechanizmów przewidzianych w art. 25 ust. 1 rozporządzenia 2016/679. Wymagają one bieżącego - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - uwzględniania: stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyk naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikających z przetwarzania, oraz wdrażania odpowiednio do tych sposobów przetwarzania i ryzk: środków technicznych i organizacyjnych, skutecznej realizacji zasad ochrony danych, niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą, tj. na każdym etapie przetwarzania danych, jak i po zakończeniu ich przetwarzania. Wszystkie podmioty korzystające z rejestru publicznego powinny mieć obowiązek uwzględnienia ochrony danych i prywatności na każdym etapie funkcjonowania rejestru, tj. w fazie projektowania (privacy by design), rozwoju, utrzymania i wygaszania. Podmioty prowadzące rejestry są odpowiedzialne za przestrzeganie przepisów wynikających z rozporządzenia 2016/679 oraz muszą być w stanie to wykazać zgodnie z zasadą rozliczalności określoną w art. 5 ust. 2 rozporządzenia 2016/679, dokumentując podejmowane przez siebie czynności mające na celu ochronę danych osobowych**.**

Obecna sytuacja międzynarodowa nakazuje spojrzeć na bezpieczeństwo danych osobowych przetwarzanych w rejestrach publicznych także przez pryzmat sytuacji zagrożenia państwa i bezpieczeństwa narodowego w wielu jego aspektach, które należy potraktować kompleksowo. Rejestry publiczne, w których przetwarzane są dane osobowe zarówno obywateli, jak i innych osób przebywających w Polsce są bowiem kluczowym elementem bezpieczeństwa

państwa. Ochrona tych danych jest więc podyktowana nie tylko zagrożeniami dla prywatności jednostki, ale także istotnymi ryzykami w sferze obronności Polski i Unii Europejskiej. Ryzyka te nie ograniczają się do cyberzagrożeń, ale wiążą się z całym spektrum działań związanych z nielegalnym przetwarzaniem danych osobowych. Przykładowo, działania obcych wywiadów które za pomocą osób z nimi związanych mogą zmierzać do pozyskania nieuprawnionego dostępu do danych osobowych obywateli co może mieć groźne konsekwencję dla bezpieczeństwa państwa. Pozyskanie do współpracy osób na różnym szczeblu struktury administracji publicznej posiadających dostęp do danych osobowych przetwarzanych w rejestrach publicznych czy dokumentów zawierających dane osobowe osób fizycznych może być wykorzystywane przez obce służby m.in. do tworzenia agentom obcego państwa fałszywych tożsamości i życiorysów z wykorzystaniem cudzych danych osobowych (co je uprawdopodabnia). Dostęp do rejestrów publicznych przez agentów obcych państw, a także przestępców jest wiec obarczone szeregiem ryzyk dla bezpieczeństwa państwa. Informacje uzyskane z rejestrów publicznych mogą też służyć m.in. do szantażowania konkretnych osób, ich profilowania na potrzeby działań wywiadowczych, czy nawet dyskredytowania tych osób przed opinią publiczną. Dane sensytywne ujawniające stan zdrowia, poglądy polityczne, seksualność osoby fizycznej, a także informacje o jej karalności mogą mieć olbrzymie znaczenie dla działań wymierzonych w taką osobę, a co za tym idzie umożliwiają wpływ na nią co w zależności od roli jednostki w państwie i w grupach społecznych (społeczeństwie) w wielu przypadkach może rzutować na bezpieczeństwo narodowe. Rola skuteczności i prawidłowość wykorzystywania rejestrów publicznych dla właściwego funkcjonowania społeczeństwa jest więc oczywista. Z tego powodu rejestry te mogą być celem działań hybrydowych mających zakłócić prawidłowe działania instytucji i organów państwowych, a także celem ataków w przypadku wybuchu wojny. Zarówno dokumenty o charakterze strategicznym, jak i ustawodawstwo powinno uwzględniać więc rozwiązania dotyczące bezpieczeństwa państwa związane z ryzykami dla danych osobowych przetwarzanych w rejestrach publicznych (związanymi np. z koniecznością odzyskiwania zasobów rejestrów na wypadek ataków, koniecznością zmiany infrastruktury na której działa dany rejestr w związku z działaniami wojennymi, pozyskania przez obce służby za pośrednictwem zewnętrznych podmiotów obsługujących rejestr informacji o jego zabezpieczeniach itp.).

W kontekście sytuacji zagrożenia bezpieczeństwa państwa należy także ponownie spojrzeć krytycznie na postulowany wielokrotnie w trakcie prac legislacyjnych model powszechnego, niekontrolowanego i nieograniczonego dostępu do przetwarzanych w rejestrach publicznych danych osób pełniących funkcję publiczne. Wątpliwości rodzą również rozwiązania związane z upublicznianiem w Internecie istotnych informacji mogących zidentyfikować osoby fizycznie[58]. Istotne wartości, takie jak przejrzystość życia publicznego czy ułatwienia w dostępie do

[58] Jak miało to przykładowo miejsce w przypadku ujawnienia numerów ksiąg wieczystych na geoportalu.

informacji przydatnych dla osób fizycznych, powinny bowiem zwłaszcza w obecnej sytuacji geopolitycznej podlegać wyważeniu nie tylko z wartościami związanymi z prywatnością jednostki ale także ryzykiem pozyskania i wykorzystania z użyciem nowych technologii zbiorów z danymi osobowymi polskich obywateli i innych osób fizycznych przez obce państwa i organizację przestępcze.

W świetle powyższych argumentów zasadne jest **dokonanie przeglądu funkcjonujących w Polsce rejestrów publicznych w celu zapewnienia przetwarzania zawartych w nich danych, w tym danych osobowych, zgodnie ze standardami ochrony prawa do prywatności wynikającymi z przepisów prawa i orzecznictwa sądów europejskich.**

W sprawozdaniach z działalności Prezesa UODO opublikowanych na stronach Urzędu Ochrony Danych Osobowych na bieżąco zostały wskazane oczekiwania organu nadzorczego odnośnie do konstrukcji przepisów projektów ustaw i projektów informatycznych, na podstawie których są tworzone rejestry publiczne zgłoszone w trakcie prac nad tymi aktami prawnymi i dokumentami[59]. Organ nadzorczy konsekwentnie podtrzymuje swoje stanowisko i postulat, by rejestry publiczne były tworzone przy wykonaniu oceny skutków dla ochrony danych. Aspekt ten był wielokrotnie wskazywany w opiniach legislacyjnych Prezesa UODO, opiniach dotyczących projektów legislacyjnych, jak i w wystąpieniu skierowanym do Przewodniczącego Komitetu Stałego Rady Ministrów[60]. Biorąc pod uwagę nowe wyzwania związane z wykorzystaniem w rejestrach publicznych systemów AI, niezbędne jest także uregulowanie w przepisach ustaw przepisów określających ramy prawne stosowania tych narzędzi w szczególności zgodne z przepisami aktu w sprawie sztucznej inteligencji oraz rozporządzenia 2016/679. Wzgląd na bezpieczeństwo państwa sprawia, że rozwiązania prawne i organizacyjne dla konkretnych rejestrów publicznych powinny być poddane także przeglądowi pod kątem ryzyk i odporności tych rejestrów na zagrożenia związane z działaniami wojennymi i innymi sytuacjami kryzysowymi z punktu widzenia bezpieczeństwa państwa i jego obywateli.

W związku z szeregiem zmian prawnych przytoczonych w wystąpieniu i powierzeniu dodatkowych zadań należy dodatkowo podkreślić, że Prezes Urzędu Ochrony Danych Osobowych ma pełnić rolę nie tylko organu właściwego w sprawie ochrony danych osobowych, ale również w związku z realizacją przepisów Aktu w sprawie zarządzania danymi ma być organem dostępu do danych, gdyż realizacja celów stojąca u podstaw powyższego rozporządzenia ma też wspomóc kształtowanie

[59]Zob. Sprawozdania z działalności Prezesa UODO w roku 2024 https://uodo.gov.pl/pl/487/2279
[60] Wystąpienie Prezesa Urzędu Danych Osobowych do Przewodniczącego Komitetu Stałego Rady Ministrów z 14 lutego 2025 r. (znak: DOL.413.15.2024) z wnioskiem o podjęcie działań legislacyjnych mających na celu uzupełnienie Regulaminu pracy Rady Ministrów w zakresie obowiązku sporządzenia OSR prywatności do projektowanych aktów normatywnych, celem zapewnienia dostosowania ich do przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

gospodarki krajowej i unijnej. Do tego zadania państwo powinno się również przygotować wprowadzając jasne i przejrzyste mechanizmy anonimizacji i pseudonimizacji w ramach przetwarzania danych w rejestrach publicznych, które to są odrębnymi procesami. Nad ryzykiem przywrócenia danych spseudonimizowanych do postaci danych osobowych identyfikujących lub umożliwiających identyfikację osoby fizycznej powinna być zapewniona kontrola wynikająca z przepisów ustaw, a rejestry publiczne podlegać kontroli we wskazanym obszarze.

W świetle przedstawionych argumentów zwracam się do Pana Premiera z uprzejmą prośbą o ustosunkowanie się do niniejszego wystąpienia **w terminie 30 dni od daty jego otrzymania**, zgodnie z dyspozycją art. 52 ust. 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

Do wiadomości:
Pan Maciej Berek
Minister nadzoru nad wdrażaniem polityki rządu

Pani Jolanta Sobierańska-Grenda
Minister Zdrowia

Pan Waldemar Żurek
Minister Sprawiedliwości