PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, **16 marca 2026**

DPNT.413.28.2025

Pan
Marcin Kierwiński
Minister Spraw Wewnętrznych
i Administracji

Ministerstwo Spraw Wewnętrznych i
Administracji

Pan
Waldemar Żurek
Minister Sprawiedliwości
Prokurator Generalny

Szanowni Panowie Ministrowie,

działając na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)[1], **zwracam się z uprzejmą prośbą i wnioskiem o podjęcie pogłębionej analizy i prac legislacyjnych prowadzących do zmiany przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem**

[1] Prezes Urzędu Ochrony Danych Osobowych może występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

przestępczości[2] **w celu zapewnienia prawidłowej implementacji w polskim systemie prawa dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680**[3].

Prezes Urzędu Ochrony Danych Osobowych (dalej jako Prezes UODO) sygnalizował nieprawidłowe implementowanie dyrektywy (UE) 2016/680 już wcześniej, zarówno na etapie opiniowania projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[4], opiniowania projektów innych ustaw[5], jak również w związku z realizowanymi przez Komisję Europejską pracami nad ewaluacją ww. dyrektywy (UE).

Nieprawidłowości w zakresie implementacji dyrektywy 2016/680 zostały w sposób wyraźny ujawnione w toku ewaluacji stosowania tej dyrektywy przeprowadzonych w 2021 r.[6] oraz 2025 r.[7]. Zgodnie z art. 62 ust. 3 dyrektywy, Komisja Europejska zwróciła się do organów ochrony danych utworzonych na podstawie art. 41 dyrektywy o udzielenie informacji niezbędnych do dokonania swojej oceny. W przypadku państw członkowskich, w których funkcjonuje więcej niż jeden organ nadzorczy, Komisja Europejska zobowiązała je do przygotowania jednego, skonsolidowanego wkładu krajowego. Prezes Urzędu zwrócił się do Prokuratora Krajowego, Prokuratorów Okręgowych i Rejonowych, Krajowej Rady Sądownictwa oraz Prezesów Sądów Apelacyjnych i Okręgowych o przekazanie niezbędnych informacji do przygotowania skonsolidowanego wkładu krajowego[8].

Analiza nadesłanych odpowiedzi pokazała, że obecny kształt ustawy z 14 grudnia 2018 r. **nie zapewnia pełnych gwarancji ochrony praw osób**, których dane są przetwarzane, co wskazuje na potrzebę wprowadzenia zmian zapewniających standardy przetwarzania i ochrony danych osobowych. Część sądowych organów nadzorczych wskazuje wprost, że przepisy procedury karnej nie odzwierciedlają w pełni standardów ochrony danych wynikających z dyrektywy (UE) 2016/680. Brakuje w nich gwarancji podstawowych praw osób, których dane dotyczą, takich jak: prawo do informacji, prawo do

---

[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2023 r. poz. 1206), dalej jako ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89, z późn. zm.), dalej jako dyrektywa (UE) 2016/680.

[4] Opinia Prezesa Urzędu Ochrony Danych Osobowych z 18 czerwca 2018 r. (sygn. ZWME.070.1.2018) skierowana do Pani Karoliny Ostrzyniewskiej – ówczesnej Sekretarz Komitetu do Spraw Europejskich RM; opinia Prezesa UODO z 14 sierpnia 2018 r. (sygn. ZSOŚS.11815.2018) skierowana do Pani Małgorzaty Hirszel – ówczesnej Sekretarz Stałego Komitetu Rady Ministrów.

[5] Opinia Prezesa UODO z 5 grudnia 2024 r. do projektu ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw DOL.401.437.2024; opinia Prezesa Urzędu Ochrony Danych Osobowych z 23 stycznia 2025 r. do projektu ustawy o zmianie ustawy - Kodeks postępowania karnego oraz niektórych innych ustaw DPNT.401.2.2025; opinia Prezesa UODO z 25 kwietnia 2023 r. do ustawy o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw DOL.401.150.2023.

[6] https://www.edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-european-commissions-evaluation-data_en

[7] https://www.edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-european-commissions-evaluation-data-0_en

[8] Pisma Prezesa UODO z 8 lipca 2025 r. sygn. DWS.602.1.2025 r.

skargi, prawo dostępu do danych, do ich sprostowania, usunięcia, ograniczenia przetwarzania, a także do wniesienia skargi do organu nadzorczego i skutecznego środka prawnego przed sądem od decyzji tego organu. Wszystkie te mankamenty, a wręcz luki prawne wpływają negatywnie na stosowanie art. 18 dyrektywy(UE) 2016/680, odnoszącego się do praw osób, których dane dotyczą, w postępowaniu przygotowawczym i sądowym w sprawie karnej. Pozostała część sądowych organów nadzorczych w nadesłanych odpowiedziach opowiada się za koniecznością dokonania pilnej nowelizacji ustawy z dnia 14 grudnia 2018 r. w zakresie właściwego wdrożenia przepisów dyrektywy (UE) 2016/680 do polskiego porządku prawnego z uwagi na **brak ich właściwości do stosowania tejże ustawy, co stanowi niewykonanie dyrektywy**.

Potrzebę ponownego zwrócenia uwagi na nieprawidłowości w procesie implementacji dyrektywy (UE) 2016/680 determinuje dodatkowo **decyzja wykonawcza Komisji Europejskiej z 2024 r.** ustanawiająca sprawozdanie z oceny stosowania dorobku Schengen przez Polskę w 2024 r. Jednym z jej zaleceń priorytetowych dla Polski jest wskazany w zaleceniu nr 49 raportu obowiązek zapewnienia pełnej transpozycji dyrektywy (UE) 2016/680 w odniesieniu do przetwarzania danych osobowych wymienionych w art. 3 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz w odniesieniu do danych osobowych przetwarzanych na podstawie dorobku Schengen przez organy wymienione w art. 3 ust. 2 tejże ustawy[9]. Zalecenie to ma charakter systemowy i odnosi się do zapewnienia pełnej zgodności prawa krajowego z wymogami prawa Unii Europejskiej w obszarze przetwarzania danych przez właściwe organy.

Prawidłowe wdrożenie dyrektywy 2016/680 w polskim porządku prawnym będzie miało ogromne znaczenie dla realizacji **strategii na rzecz cyfrowego wymiaru sprawiedliwości na lata 2025–2030**. W Komunikacie Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów[10], podkreślono, że cyfryzacja i wdrażanie sztucznej inteligencji będą miały zasadnicze znaczenie dla zdolności organów publicznych do świadczenia wysokiej jakości usług publicznych, również w dziedzinie wymiaru sprawiedliwości. Celem trwającej obecnie cyfrowej dekady Europy jest udostępnienie wszystkich kluczowych usług publicznych UE w Internecie do 2030 r. Korzystanie z narzędzi cyfrowych w sprawach dotyczących wymiaru sprawiedliwości musi odbywać się z pełnym poszanowaniem praworządności i praw podstawowych zapisanych w Karcie Praw Podstawowych Unii Europejskiej i odpowiednim prawie pochodnym UE[11]. Komisja Europejska zwraca uwagę, że systemy wymiaru sprawiedliwości charakteryzujące się większym stopniem cyfryzacji mogą być narażone na naruszenia ochrony danych osobowych i cyberataki. Chociaż systemy oparte na dokumentacji papierowej mają inne słabe punkty, takie jak ograniczone możliwości udostępniania danych czy trudności z aktualizacją, szczególną uwagę należy

[9] Np. przetwarzanie danych osobowych z Systemu Informacyjnego Schengen (SIS) i Wizowy System Informacyjny (VIS) do celów wymienionych w dorobku SIS i VIS dostępne pod linkiem: https://home-affairs.ec.europa.eu/document/download/aa985c3b-2c11-47e7-99e3-a7459e7c2bc8_en?filename=Schengen%20evaluation%20of%20Poland.pdf

[10] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14517-Strategia-na-rzecz-cyfrowego-wymiaru-sprawiedliwosci-na-lata-2025-2030_pl

[11] Dyrektywa Parlamentu Europejskiego i Rady 2012/13/UE z dnia 22 maja 2012 r. w sprawie prawa do informacji w prawie karnym.

zwrócić na prywatność i bezpieczeństwo danych. Ogólne rozporządzenie o ochronie danych[12] i dyrektywa o ochronie danych w sprawach karnych to podstawowe akty prawne UE, których celem jest ochrona osób fizycznych przed zagrożeniami dla ich praw i wolności, w szczególności przed nieuprawnionym dostępem do danych osobowych, ich utratą, naruszeniem poufności, integralności lub dostępności, realizowana m.in. poprzez stosowanie środków zarządzania ryzykiem oraz mechanizmów zgłaszania incydentów. Unijny akt o cyberbezpieczeństwie również przyczynia się do podniesienia poziomu cyberbezpieczeństwa produktów opartych na technologiach informacyjno-komunikacyjnych w UE, w tym produktów wykorzystywanych w sektorze wymiaru sprawiedliwości.

Za koniecznością ponownego zwrócenia uwagi na potrzebę nowelizacji ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przemawia orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej oraz Europejskiego Trybunału Praw Człowieka, jak również wieloletnia praktyka organu nadzorczego, oraz występujące rozbieżności interpretacyjne między podmiotami zobowiązanymi do stosowaniem dyrektywy 2016/680 (UE).

Poniżej przedstawiam szczegółowe problemy, które powinny być wzięte pod uwagę w analizie i procesie legislacyjnym.

I. Wyłączenie stosowania ustawy.

Prawo do ochrony danych osobowych stanowi jedno z podstawowych praw człowieka gwarantowanych prawem Unii Europejskiej, zarówno w Karcie Praw Podstawowych UE[13] (art. 8), jak i w Traktacie o funkcjonowaniu Unii Europejskiej (art. 16 TFUE[14]). Nie jest to prawo o charakterze bezwzględnym. Jego wykonywanie może podlegać pewnym ograniczeniom, ale musi być zrównoważone z innymi prawami i wolnościami. Zgodnie z motywem 4 rozporządzenia ogólnego o ochronie danych osobowych jego ochrona musi być rozpatrywana w kontekście jego funkcji społecznych i powinna być proporcjonalna do innych praw podstawowych. Niemniej, prawo do ochrony danych osobowych odgrywa szczególnie istotną rolę także w obszarze postępowania karnego, w którym przetwarzanie danych osobowych niesie wysokie ryzyko ingerencji w sferę prywatności jednostki oraz praw podstawowych. Poszanowanie tego prawa wymagane jest przy jednoczesnym zapewnieniu efektywności działań organów odpowiedzialnych za zwalczanie przestępczości. Podczas prowadzonych postępowań gromadzone są nie tylko dane osób podejrzewanych o popełnienie czynu zabronionego, ale również osób trzecich, świadków oraz pokrzywdzonych.

---

[12] 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.).

[13] Dz. Urz. C 202 z 7.6.2016, s. 391-407. Zob. m.in. J. Sobczak, Komentarz do art. 8, w: A. Wróbel (red.), Karta Praw Podstawowych Unii Europejskiej. Komentarz, Warszawa 2020, s. 269-314.

[14] Dz. Urz. C 202 z 7.6.2016, s. 47. Zob. m.in. J. Sobczak, Komentarz do art. 16, w: D. Miąsik, N. Półtorak (red.), A. Wróbel (red. naukowy), Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1-89), Warszawa 2012, s. 300-335.

Celem unijnej dyrektywy 2016/680 oraz całego systemu ochrony danych osobowych jest zapewnienie spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich w sprawach karnych i współpracy policyjnej. Unijny prawodawca przyjął model oparty na rozdzieleniu zakresu stosowania rozporządzenia 2016/679 oraz dyrektywy (UE) 2016/680.

Zakres stosowania ogólnego rozporządzenia o ochronie danych osobowych i dyrektywy (UE) 2016/680 w swoim założeniu jest rozłączny. W art. 2 ust. 2 lit. d rozporządzenia ogólnego wskazano wyraźnie, że nie ma ono zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zakres ten reguluje właśnie dyrektywa (UE) 2016/680, która w swojej istocie ma chronić podstawowe prawa jednostki, zapewniając osobom uczestniczącym w postępowaniach karnych, zarówno podejrzanym, oskarżonym, świadkom czy ofiarom, ochronę ich danych osobowych, w przypadku ich przetwarzania przez organy ścigania lub wymiaru sprawiedliwości w sprawach dotyczących zwalczania szeroko rozumianej przestępczości[15].

Prawodawca w motywie 10 dyrektywy odwołał się do potrzeby przyjęcia szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w dziedzinach wymiaru sprawiedliwości w sprawach karnych i współpracy policyjnej ze względu na ich szczególny charakter. Cele dyrektywy (UE) 2016/680 zostały określone w jej art. 1 ust. 2 jako równoprawne. Po pierwsze, państwa członkowskie zostały zobowiązane do ochrony praw podstawowych i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, a po drugie – do zapewnienia, by wymiana danych osobowych przez właściwe organy w Unii, jeżeli wynika z prawa Unii lub prawa krajowego, nie była ograniczana ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Przepisami dyrektywy (UE) 2016/680 ustanowiono granice ingerencji w prawa człowieka, by osiągnąć równowagę między koniecznością zapewnienia efektywności działalności organom odpowiedzialnym za walkę z przestępczością a prawami jednostki do ochrony prywatności i ochrony danych osobowych. Istotnym założeniem dyrektywy jest również ujednolicenie w całej UE zasad ochrony danych w obszarze ścigania przestępstw, by uniknąć rozbieżności prawnych między państwami członkowskimi[16].

Tymczasem **art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości tę ochronę wyłącza** (konsekwentnie, wyłączenie wskazane jest również w art. 1 pkt 3 tej ustawy kształtującym zakres przedmiotowy regulacji). Zgodnie bowiem z art. 3 pkt 1 tej ustawy, przepisów ustawy nie stosuje się do ochrony danych osobowych: znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie

[15] Motyw 2, 4 i 10 dyrektywy (UE) 2016/680.
[16] Motyw 7 dyrektywy (UE) 2016/680.

ustawy z dnia 6 czerwca 1997 r. - Kodeks karny wykonawczy[17], ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego[18], ustawy z dnia 10 września 1999 r. - Kodeks karny skarbowy[19], ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia[20], ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób[21], ustawy z dnia 28 stycznia 2016 r. - Prawo o prokuraturze[22], ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich[23].

Wyłączenie przyjęte w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości powoduje, że ustawa ta nie obejmuje wszystkich obszarów przetwarzania danych osobowych w celach rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, jakie uwzględnia dyrektywa (UE) 2016/680. Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości istotnie zawęża zatem zakres przedmiotowy oraz podmiotowy regulacji krajowych w porównaniu do tego, jaki został przewidziany w dyrektywie (UE) 2016/680. Zgodnie z art. 2 ust. 1 dyrektywy, ma ona zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów określonych w art. 1 ust 1 tejże dyrektywy, tj. do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Łatwo tym samym zauważyć niezgodność jaka pojawia się pomiędzy normą z art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości a postanowieniami i celem wprowadzenia dyrektywy (UE) 2016/680. Konsekwencją wyłączenia przyjętego przez krajowego ustawodawcę w art. 3 pkt 1 ustawy jest to, że dane osobowe zawarte w aktach prowadzonych spraw oraz dane osobowe przetwarzane w toku czynności lub w urządzeniach ewidencyjnych prowadzonych na podstawie przepisów prawa wynikających z powołanych wyżej ustaw nie podlegają na poziomie krajowym jakimkolwiek przepisom gwarantującym ochronę danych osobowych, niezgodnie z *ratio legis* dyrektywy 2016/680. Tymczasem, jednym z podstawowych celów dyrektywy (UE) 2016/680 jest zapewnienie wysokiego stopnia ochrony danych osobowych, co ma nastąpić m.in. poprzez wzmocnienie praw osób, których dane dotyczą, oraz obowiązków podmiotów, które dane osobowe przetwarzają[24]. Polski ustawodawca przyjął tymczasem kierunek wprost przeciwny i niezgodny z dyrektywą.

Niezwykle istotne jest to, że wyłączenia spod mocy ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przyjęte w jej art. 3 pkt 1 i pkt 2 prowadzą do wyłączenia wszystkich przepisów dotyczących środków zabezpieczających dane osobowe. W konsekwencji ma to istotny wpływ także na bezpieczeństwo danych osobowych – również w kontekście operacyjnym

[17] Dz. U. z 2023 r. poz. 127 oraz z 2022 r. poz. 2600.
[18] Dz. U. z 2022 r. poz. 1375, 1855, 2582 i 2600 oraz z 2023 r. poz. 289 i 535.
[19] Dz. U. z 2023 r. poz. 654.
[20] Dz. U. z 2022 r. poz. 1124.
[21] Dz. U. z 2022 r. poz. 1689.
[22] Dz. U. z 2024 r. poz. 390 ze zm.
[23] Dz. U. poz. 1700 oraz z 2023 r. poz. 289.
[24] Motyw 4 i 7 dyrektywy (UE) 2016/680.

– przetwarzanych w tak istotnych celach jakimi są: zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych, wykonywania kar, ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom. W ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości prawodawca nakłada na administratora i podmiot przetwarzający dane obowiązek stosowania odpowiednich środków technicznych i organizacyjnych, identyfikacje ryzyk naruszenia praw lub wolności osób fizycznych oraz kładzie nacisk na odpowiednie zabezpieczanie danych[25]. Obowiązków tych nie znajdziemy w ustawach o których mowa w art. 3 pkt 1 i 2 powołanej ustawy, szczególnie zaś w Kodeksie postępowania karnego.

Wyłączenia te, błędnie powiązane przez ustawodawcę krajowego z brakiem funkcjonowania zbioru danych w przypadku przetwarzania danych osobowych w urządzeniach ewidencyjnych oraz w systemie teleinformatycznym, są sprzeczne z art. 2 ust. 2 dyrektywy 2016/680 wyznaczającym jej zakres stosowania.

Jednym z przytaczanych przez ustawodawcę polskiego argumentów dla tak szerokiego wyłączenia zastosowanego w omawianej ustawie[26] jest definicja zbioru danych wskazana w art. 3 pkt 6 dyrektywy (UE) 2016/680, którym jest uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie. Nie wdając się w dalszą polemikę czy akta sądowe są zbiorem danych osobowych, czy też nie, należy wskazać że art. 2 ust. 2 dyrektywy (UE) 2016/680 odnosi się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, a takim sposobem jest przecież przetwarzanie danych osobowych w urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych. Zakres ten należy odnieść do trzech użytych w art. 3 pkt 1 ustawy pojęć dotyczących organizacji przetwarzania danych osobowych: **akta spraw**, **urządzenia ewidencyjne** oraz **technika informatyczna**. Cechą każdego urządzenia ewidencyjnego, ze względu na zakres znaczeniowy tego zwrotu, jest porządkowanie danych tak, aby były one dostępne według określonych kryteriów, co spełnia przesłanki definicji zbioru danych z art. 3 pkt 6 dyrektywy (UE) 2016/680. Przykładem takiego systemu może być sądowy system teleinformatyczny, służący m.in. do przechowywania treści zapadłych orzeczeń, zarządzeń oraz ich uzasadnień[27]. W związku z powyższym akta sprawy prowadzonej, np. w oparciu o procedurę karną, są przechowywane przez sąd zarówno w wersji papierowej, jak i z wykorzystaniem technik informatycznych w zakresie danych osobowych znajdujących się w tych aktach[28].

W przypadku wyodrębnienia akt sprawy lub w sytuacji połączenia akt z systemem teleinformatycznym umożliwiającym dostęp do danych osobowych zawartych w takich

---

[25] Art. 32 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
[26] Uzasadnienie do projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości: https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2989
[27] Art. 84 § 1 pkt 7 Regulaminu Urzędowania Sądów Powszechnych.
[28] Opinia Ministra Spraw Zagranicznych o zgodności z prawem Unii Europejskiej projektowanej ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej https://legislacja.rcl.gov.pl/docs//2/12310605/12502724/12502726/dokument355779.PDF

aktach wystarczające dla zaistnienia zbioru jest występowanie jakiegokolwiek kryterium porządkującego akta, które pozwoli na dostęp do danych osobowych określonej osoby[29]. Jeśli akta są połączone z systemem ewidencyjnym zapewniającym dostęp do danych osobowych zawartych w aktach sprawy dotyczących jakiejkolwiek osoby (np. uczestnika postępowania), to takie dane osobowe w aktach stanowią co najmniej część zbioru.

Z kolei art. 18 dyrektywy 2016/680 nie daje podstaw do całościowego wyłączenia stosowania dyrektywy, ponieważ stanowi on jedynie **o możliwości kształtowania realizacji niektórych określonych w dyrektywie praw osób**, których dane dotyczą (uprawnienia wskazane w art. 13, 14 i 16 dyrektywy) zgodnie z przepisami krajowymi w postępowaniu przygotowawczym lub sądowym w sprawie karnej. W szczególności, w art. 18 dyrektywy nie wymieniono żadnego z przepisów dyrektywy dotyczącego bezpieczeństwa danych osobowych. Posłużenie się w art. 18 dyrektywy (UE) 2016/680, tak zresztą jak w jej motywie 20, zwrotem „akta sprawy" świadczy o tym, że wolą prawodawcy, przetwarzanie w nich danych osobowych może mieścić się w zakresie stosowania dyrektywy (UE) 2016/680, ale jedynie punktowo istnieje możliwość wyłączenia lub modyfikacji w prawie krajowym stosowania przepisów dyrektywy w tym względzie.

W dyrektywie (UE) 2016/680 prawodawca nie przewidział więc podstaw do wyłączania stosowania przepisów o bezpieczeństwie danych osobowych w zakresie wskazanym w art. 3 pkt 1 ustawy, w sytuacji, gdy to przetwarzanie następuje w granicach wyznaczonych w art. 2 dyrektywy 2016/680.

Zgodnie z motywem 20 dyrektywy 2016/680 dyrektywa nie powinna stanowić dla państw członkowskich przeszkody w określaniu w krajowym prawie karnym procesowym operacji i procedur przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości, zwłaszcza danych osobowych ujmowanych w orzeczeniach sądowych lub aktach związanych z postępowaniem sądowym.

Celem wyrażonym w motywie 20 jest uniknięcie kolizji między przepisami dyrektywy 2016/680 oraz określanymi w krajowym prawie karnym procesowym „operacjami i procedurami przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości". Motyw ten wskazuje, że przepisy krajowe muszą być precyzyjne i jasne dla osób, których dane są przetwarzane, a ich stosowanie powinno być proporcjonalne i ograniczone do niezbędnego celu. Istotnym problemem w polskim porządku prawnym jest rozproszenie przepisów dotyczących ochrony danych osobowych w sektorze ścigania, umieszczanych fragmentarycznie w ustawach sektorowych czy procedurach, stwarzając niepewność stosowania prawa i poważne trudności interpretacyjne zarówno w zakresie uprawnień, jak i obowiązków dla samych organów nadzorczych.

Z motywu 49 dyrektywy 2016/680 wynika ponadto, że jeżeli dane osobowe przetwarza się w toku postępowania przygotowawczego i sądowego w sprawie karnej, państwa członkowskie powinny mieć możliwość zapewnienia wykonywania prawa do informacji, dostępu lub poprawienia, usunięcia i ograniczenia przetwarzania zgodnie z krajowymi przepisami o postępowaniu sądowym. Jak widać, z przytoczonego motywu nie

[29] Zob. również G. Sibiga, Opinia prawna dotycząca rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy nr 2989), Warszawa 30.11.2018 r. https://orka.sejm.gov.pl/WydBAS.nsf/0/ABD6560FB2845CF4C12583D000292054/$file/8.Grzegorz%20Sibiga.pdf

wynika wprowadzony przez krajowego ustawodawcę obowiązek wyłączenia stosowania omawianych przepisów w tak szerokim zakresie.

W świetle artykułu 18 dyrektywy (UE) oraz jej motywu 20, należy rozważyć przyjęcie w krajowym porządku prawnym nowych przepisów lub uzupełnienie przepisów Kodeksu postępowania karnego oraz pozostałych aktów prawnych, do których ustawodawca odwołał się w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Regulacje takie w sposób jasny i nie budzący wątpliwości określać powinny uprawnienia uczestników procedury karnej zgodnie z wymogami dyrektywy (UE) 2016/680. W obecnym stanie prawnym uprawnienia te mogą być jedynie pośrednio i nie w pełnym zakresie wywodzone z innych przepisów Kodeksu postępowania karnego[30]. Aktualny stan prawny dotyczący przetwarzania danych osobowych w sprawach karnych, choć opiera się na ogólnych zasadach wynikających z rozporządzenia o ochronie danych osobowych oraz ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie zawsze w sposób precyzyjny określa zakres oraz zasady przetwarzania danych osobowych w postępowaniach karnych. Doprecyzowanie tych regulacji pozwoli na zrównoważenie ochrony prywatności z jednoczesnym obowiązkiem skutecznego prowadzenia postępowań przygotowawczych oraz sądowych. Brak takiej regulacji prowadzi do rozbieżności interpretacyjnych, utrudnia zachowanie równowagi między ochroną praw jednostki a skutecznością postępowania karnego. W konsekwencji, nowelizacja przepisów procesowych nie tylko zapewni większą przejrzystość działań organów ścigania, zwiększy poziom zgodności prawa krajowego z przepisami prawa unijnego, ale przede wszystkim wzmocni ochronę praw podstawowych. Stanowić tym samym będzie istotny krok w kierunku zapewnienia spójności i przejrzystości systemu ochrony danych osobowych w sferze postępowania karnego. Wykonawca normy – zwłaszcza podmiot publiczny i w przypadku przepisów służących zachowaniu reżimów prawa karnego – powinien być wyposażony w przejrzyste i wyczerpujące normy tak, aby mógł działać na podstawie i w granicach prawa, czego wymaga także konstytucyjna zasada praworządności (art. 7 Konstytucji RP). Rolą prawodawcy krajowego jest wyposażenie wykonawcy normy w takie przepisy wykonujące cele i przepisy dyrektywy w niewadliwe podstawy prawne celem realizacji tak istotnych celów jak: zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych, wykonywania kar, ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom. Zagadnienia te nie odnoszą się wyłącznie do ochrony interesów jednostki, lecz obejmują również interes ogólny i społeczny. Wprowadzanie i doskonalenie zasad ochrony danych osobowych stanowi bowiem element szerszego systemu odporności państwa, wzmacniającego jego zdolność do reagowania na zagrożenia oraz zapewnienia stabilności porządku publicznego. Spójność i skuteczność tych regulacji wpływa bezpośrednio na poziom zaufania obywateli do

[30] W przypadku np. prawa do sprostowania danych osobowych oraz żądania ich usunięcia jeśli są przetwarzanie niezgodnie z dyrektywą (art. 16 dyrektywy), w odniesieniu do pierwszego z tych uprawnień organ postępowania karnego ma obowiązek sprostować dane, które okażą się nieprawidłowe, co wynika z ciążącego na organach postępowania obowiązku czynienia prawdziwych ustaleń faktycznych (art. 2 § 2 Kpk). Drugie zaś z powyższych uprawnień nie zostało przewidziane w Kpk.

instytucji państwa oraz na efektywność działań organów publicznych, a tym samym na bezpieczeństwo państwa jako całości.

Brak prawidłowej implementacji dyrektywy (UE) 2016/680 w opisanym powyżej zakresie rodzi pytania o pierwszeństwo prawa UE, możliwość bezpośredniego stosowania przepisów dyrektywy (UE) 2016/680 w krajowym systemie prawnym, a co najmniej konieczność dokonywania wykładni prawa krajowego zgodnej z prawem UE. W tym zakresie należy wskazać, że zgodnie z art. 288 TFUE[31] dyrektywa wiąże każde państwo członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawiając jednak organom krajowym swobodę wyboru formy i środków. Ponadto, zgodnie z art. 91 ust. 3 Konstytucji RP, jeżeli wynika to z ratyfikowanej przez RP umowy konstytuującej organizację międzynarodową, prawo przez nią stosowane jest stosowane bezpośrednio, mając pierwszeństwo w przypadku kolizji z ustawami.

II. Nadzór nad przetwarzaniem danych osobowych przez sądy.

Prawodawca nie określił sposobu prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez sądy w sposób zgodny z art. 1 pkt 3 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, co powinien był również uczynić mocą jej przepisów. Materię tę odrębnie reguluje ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych[32] (art. 175dd), która określa właściwość oraz zakres uprawnień organów nadzorczych między innymi w odniesieniu do stosowania przepisów ustawy z dnia 14 grudnia 2018 r.

Mając na względzie wyłączenie stosowania przepisów ustawy dnia 14 grudnia 2018 r. wskazanych w jej art. 3 pkt 1, podkreślić należy, że **taki stan prawny w praktyce skutkuje realnym wyłączeniem polskiego sądownictwa spod norm dotyczących ochrony danych osobowych przewidzianych dyrektywą (UE) 2016/680. Prowadzi to zarazem do braku wykonywania przez niezależny organ nadzorczy** w rozumieniu art. 41–45 dyrektywy (UE) 2016/680 **nadzoru nad przetwarzaniem danych osobowych przez sądy w obszarach objętych materią tej ustawy**.

Przepisy ogólnego rozporządzenia o ochronie danych osobowych oraz dyrektywy (UE) 2016/680 nie definiują pojęcia sądu oraz innego organu wymiaru sprawiedliwości, pozostawiając decyzji państw członkowskich określenie, które organy spełniają kryteria pozwalające na uznanie ich za sąd lub inny organ wymiaru sprawiedliwości, zgodnie z ich porządkami prawnymi. Zgodnie natomiast z art. 175 Konstytucji RP wymiar sprawiedliwości w Polsce sprawują: Sąd Najwyższy, sądy powszechne, sądy administracyjne oraz sądy wojskowe.

Niestety poza wskazaniem, jakie organy są właściwe do sprawowania wymiaru sprawiedliwości, w polskim porządku prawnym brak jest norm wyraźnie wskazujących, czym dokładnie jest „wymiar sprawiedliwości” i gdzie przebiegają granice wyznaczające, które czynności wchodzą w zakres wymiaru sprawiedliwości, a które już nie. Nie należy jednak zapominać, że te aspekty działalności sądów, które nie wchodzą w zakres sprawowania przez nie wymiaru sprawiedliwości również mogą się wiązać z ryzykiem

[31] Traktat o funkcjonowaniu Unii Europejskiej (Dz.U.2004.90.864/2).
[32] Dz. U. z 2024 r. poz. 334.

wystąpienia naruszenia ochrony danych osobowych, a te wymagają już zgłoszenia do Prezesa UODO. Należy przy tym wyjaśnić, że przez postępowanie sądowe rozumie się postępowanie odbywające się przed niezawisłymi i niezależnymi sądami, w oparciu o odpowiednie przepisy prawa cywilnego, karnego czy administracyjnego oraz postępowanie egzekucyjne, postępowanie w sprawach o wykroczenia (każde postępowanie składa się z następujących po sobie ogniw – etapów, tworzących tok procesu – w toku procesu jedynie sąd sprawuje wymiar sprawiedliwości w myśl art. 175 Konstytucji RP).

W normujących działanie sądów ustawach uchwalonych przez polskiego ustawodawcę można odnaleźć doprecyzowania dotyczące nadzoru nad przetwarzaniem danych osobowych przez poszczególne sądy w postępowaniach sądowych[33].

Z motywu 20 rozporządzenia 2016/679 wynika, że **rozporządzenie ma zastosowanie** między innymi **do działań sądów i innych organów wymiaru sprawiedliwości**, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. **Właściwość organów nadzorczych nie powinna dotyczyć wyłącznie przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości** – **tak, by chronić niezawisłość sprawowania wymiaru sprawiedliwości**. Powinna natomiast istnieć możliwość powierzenia nadzoru

[33] Zgodnie z art. 175dd § 1 ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych, nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy, zgodnie z art. 175da i art. 175db, wykonują w zakresie działalności sądu: 1) rejonowego - prezes sądu okręgowego; 2) okręgowego - prezes sądu apelacyjnego; 3) apelacyjnego - Krajowa Rada Sądownictwa. § 2. W ramach nadzoru, o którym mowa w § 1, właściwe organy: 1) rozpatrują skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem; 2) podejmują działania mające na celu upowszechnianie wśród nadzorowanych administratorów i podmiotów przetwarzających wiedzy o obowiązkach wynikających z rozporządzenia 2016/679 oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125 oraz z 2022 r. poz. 1700); 3) współpracują z innymi organami sprawującymi nadzór nad przetwarzaniem danych osobowych w ramach postępowań prowadzonych przez sądy i trybunały oraz z organami nadzorczymi w rozumieniu art. 51 rozporządzenia 2016/679, w tym dzielą się informacjami oraz świadczą wzajemną pomoc, w celu zapewnienia spójnego stosowania rozporządzenia 2016/679 oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. § 3. Organy, o których mowa w § 1, są uprawnione do:
1) nakazywania administratorowi lub podmiotowi przetwarzającemu albo ich przedstawicielom dostarczenia wszelkich informacji potrzebnych do realizacji zadań tego organu; 2) zawiadamiania administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości; 3) uzyskiwania od administratora i podmiotu przetwarzającego dostępu do danych osobowych i informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań; 4) uzyskiwania dostępu do pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych; 5) wydawania ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości; 6) udzielania upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości; 7) wzywania administratora lub podmiotu przetwarzającego do dostosowania przetwarzania danych do przepisów rozporządzenia 2016/679 lub ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. § 4. Do przyjmowania i rozpatrywania skarg związanych z przetwarzaniem danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej stosuje się odpowiednio przepisy działu I rozdziału 5a.

nad takimi operacjami przetwarzania danych **specjalnym organom** w systemie wymiaru sprawiedliwości państwa członkowskiego. Organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim operacjami przetwarzania danych.

W sposób spójny z powyższym została ujęta materia nadzoru nad przetwarzaniem danych osobowych przez sądy w motywie 80 dyrektywy (UE) 2016/680, zgodnie z którym dyrektywa ta ma zastosowanie także do działalności sądów krajowych i innych organów wymiaru sprawiedliwości, niemniej **właściwość organów nadzorczych nie powinna obejmować przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości, tak, by chronić niezawisłość sędziów w wykonywaniu ich zadań sądowych**. Wyjątek ten należy ograniczyć do czynności sądowych w sprawach sądowych i nie powinien on mieć zastosowania do innych czynności, w których sędziowie mogą brać udział zgodnie z prawem państwa członkowskiego. Państwa członkowskie powinny mieć również możliwość przyjęcia, że właściwość organu nadzorczego nie obejmuje przetwarzania danych osobowych przez inne niezależne organy wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości, przykładowo przez prokuraturę. Niemniej przestrzeganie przepisów niniejszej dyrektywy przez sądy i inne niezależne organy wymiaru sprawiedliwości zawsze podlega niezależnej kontroli zgodnie z art. 8 ust. 3 Karty Praw Podstawowych UE. Ponownie prawodawca unijny podkreślił tu, że niezawisłość sędziowska jest jedną z podstawowych wartości, której ochrona uzasadnia nawet powołanie odrębnych organów nadzoru właściwych w zakresie przetwarzania danych osobowych przez sądy w ramach wymiaru sprawiedliwości.

Koncepcja zarysowana w motywie 20 rozporządzenia 2016/679 została wyraźnie ujęta w art. 55 ust. 3 rozporządzenia 2016/679, zgodnie z którym organy nadzorcze nie są właściwe do nadzorowania operacji przetwarzania dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości. Prawodawca unijny konsekwentnie wskazał też w art. 45 ust. 2 dyrektywy 2016/680, że państwa członkowskie zapewniają, by żaden organ nadzorczy nie był właściwy do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku sprawowania przez nie wymiaru sprawiedliwości oraz że państwa członkowskie mogą postanowić, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości.

W Polsce funkcjonuje „kaskadowy” model nadzoru w sądach, zgodnie z którym prezes sądu wyższego szczebla sprawuje kontrolę nad przetwarzaniem danych osobowych w jednostkach niższej instancji. W przypadku sądów gwarancja niezależności sędziowskiej zapewnia pewien poziom autonomii tego nadzoru.

W świetle przepisów ustawy Prawo o ustroju sądów powszechnych (i analogicznie również innych ustaw regulujących funkcjonowanie sądów) na najwyższym szczeblu nadzoru stoi Krajowa Rada Sądownictwa (m.in. w przypadku nadzoru nad działalnością sądu apelacyjnego czy Sądu Najwyższego). Niezależność Krajowej Rady Sądownictwa w obecnym kształcie została jednak wielokrotnie zakwestionowana w ostatnich latach w orzecznictwie Trybunału Sprawiedliwości UE (C-585/18, C-624/18, C-625/18, C-791/19, C-487/19) oraz Europejskiego Trybunału Praw Człowieka (43447/19, 49868/19, 57511/19,

1469/20, 50849/21)[34]. **Ze wskazanych wyroków europejskich Trybunałów wynika, że Krajowa Rada Sądownictwa nie spełnia wymogów niezależności, a to powoduje wątpliwości również w odniesieniu do prawidłowości nadzoru nad przetwarzaniem danych osobowych w polskich sądach.**

Ponadto, w toku mechanizmu ewaluacji stosowania dyrektywy (UE) 2016/680, przeprowadzonej w 2025 r. zgodnie z art. 62 ust. 3 tej dyrektywy, stwierdzono, że znaczna część sądów w Polsce nie identyfikuje obszarów, w których powinna stosować przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Dzieje się tak pomimo, że ustawa Prawo o ustroju sądów powszechnych przyznaje im konkretne kompetencje w tym zakresie (art. 175dd ust. 2 pkt 2, 3 oraz ust. 3 pkt 2, 5, 6 i 7). Organy te są uprawnione m.in. do upowszechniania wiedzy wśród nadzorowanych administratorów i podmiotów przetwarzających o obowiązkach wynikających z ustawy z dnia 14 grudnia 2018 r., współpracy z innymi organami nadzorczymi w celu zapewnienia spójnego stosowania jej przepisów, zawiadamiania administratorów o podejrzeniu jej naruszenia, wydawania ostrzeżeń i upomnień dotyczących możliwości jej naruszenia, a także wzywania do dostosowania przetwarzania danych do jej wymogów.

Z kolei w przypadku sądów, które uznają swoją kompetencję do sprawowania nadzoru w trybie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości w związku z ustawą Prawo o ustroju sądów powszechnych, nadzór ten jest często w praktyce sprawowany przez inspektora ochrony danych. Tymczasem inspektor ochrony danych, o którym mowa w sekcji 3 rozdziału IV dyrektywy 2016/680, nie jest organem nadzoru, lecz wykonuje obowiązki po stronie administratora lub podmiotu przetwarzającego[35]. Jest to zatem instytucja odrębna od niezależnego organu nadzorczego, o którym mowa w rozdziale VI dyrektywy[36]. Takie rozwiązanie prowadzi do wewnętrznego konfliktu interesów i stoi w sprzeczności z przepisami art. 41 - 45 dyrektywy (UE) 2016/680, które wymagają, aby nadzór nad przetwarzaniem danych był sprawowany przez organ wyposażony w odpowiednie uprawnienia i gwarancje niezależności. **W konsekwencji przyjęty model nadzoru w sądach polskich nie zapewnia realizacji celu dyrektywy w zakresie zapewnienia skutecznego i niezależnego nadzoru nad przetwarzaniem danych osobowych.**

Choć z art. 45 dyrektywy (UE) 2016/680 wynika, że państwa członkowskie mają zapewnić, by każdy organ nadzorczy był właściwy do wypełniania przeznaczonych mu zadań i wykonywania uprawnień powierzonych mu zgodnie z dyrektywą na terytorium

---

[34] W orzecznictwie TSUE (m.in. wyrok z 19 listopada 2019 r. w sprawie C-585/18, C-624/18, C-625/18 – A.K. i in. oraz wyrok z 15 lipca 2021 r. w sprawie C-791/19 Komisja przeciwko Polsce) jednoznacznie stwierdzono, że sposób powoływania sędziów przez Krajową Radę Sądownictwa po 2018 r. narusza wymogi niezależności i bezstronności wynikające z art. 19 ust. 1 Traktatu o Unii Europejskiej oraz art. 47 Karty praw podstawowych UE. Podobnie Europejski Trybunał Praw Człowieka w Strasburgu (m.in. wyrok w sprawie Reczkowicz przeciwko Polsce, skarga nr 43447/19, z 22 lipca 2021 r.) uznał, że Izba Dyscyplinarna Sądu Najwyższego, utworzona z udziałem nowej KRS, nie jest „sądem ustanowionym ustawą" w rozumieniu art. 6 ust. 1 Europejskiej Konwencji Praw Człowieka.

[35] Zgodnie z art. 32 ust. 1 dyrektywy (UE) 2016/680 Państwa członkowskie zapewniają, by administrator wyznaczył inspektora ochrony danych. Państwa członkowskie mogą zwolnić z tego obowiązku sądy i inne niezawisłe organy sądowe w ramach sprawowania przez te organy wymiaru sprawiedliwości.

[36] Szerzej o zagadnieniu dotyczącym inspektora ochrony danych osobowych w punkcie VIII niniejszego pisma.

swego państwa członkowskiego, to część zadań i uprawnień przewidzianych w art. 46 - 49 tej dyrektywy przysługuje wyłącznie Prezesowi UODO, a nie pozostałym organom właściwym dla sądów i prokuratur.

Dotyczy to upowszechniania w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk (art. 46 ust. 1 b)), doradzania, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie ustawowych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem (art. 46 ust. 1 c)), udzielanie osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących jej na mocy dyrektywy, a w stosownym przypadku współpracowania w tym celu z organami nadzorczymi innych państw członkowskich(art. 46 ust. 1 e)), pełnienia funkcji konsultacyjnych, o których mowa w art. 28 dyrektywy, co do operacji przetwarzania (art. 46 ust. 1 k)) oraz brania udziału w pracach Europejskiej Rady Ochrony Danych (art. 46 ust. 1 pkt l)).

Organy nadzorcze właściwe dla sądów nie posiadają uprawnień doradczych pozwalających przedstawić administratorowi zalecenia zgodnie z procedurą uprzednich konsultacji oraz by z własnej inicjatywy lub na wniosek mógł wydawać opinie skierowane do parlamentu narodowego, rządu lub, zgodnie z jego prawem krajowym, innych instytucji i organów oraz do społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych (art. 47 ust. 3). Z ustawy Prawo o ustroju sądów powszechnych nie wynika również mechanizm zgłaszania naruszeń ochrony danych (art. 48), ani obowiązek sporządzania rocznego sprawozdania ze swojej działalności (art. 49).

Brak wyposażenia organów nadzorczych właściwych dla sądów w pełnię kompetencji prowadzi do braku jednolitego standardu nadzoru i może ograniczać ochronę praw jednostek w zakresie przetwarzania danych w wymiarze sprawiedliwości, co nie jest pożądane i zapewnia skutecznej ochrony praw podstawowych.

Potwierdzają to również opinie części sądowych organów nadzorczych przedstawione w toku mechanizmu ewaluacji stosowania tej dyrektywy prowadzonym w 2025 r. Wskazano w nich, że obowiązujące przepisy procedury karnej nie odzwierciedlają w pełni standardów ochrony danych wynikających z prawa Unii. Brakuje w nich podstawowych gwarancji praw osób, których dane dotyczą – takich jak prawo do informacji, wniesienia skargi, dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawa do skutecznego środka prawnego przed sądem w przypadku decyzji organu nadzorczego.

Oznacza to również nieskuteczne wdrożenie art. 18 dyrektywy (UE) 2016/680 dotyczącego praw osób w postępowaniu przygotowawczym i sądowym w sprawie karnej, a w praktyce ograniczenie możliwości egzekwowania praw osób, których dane dotyczą, w postępowaniach prowadzonych przez organy wymiaru sprawiedliwości i organy ścigania.

Konkludując tę część wystąpienia, wskazać należy, że nadzór nad prawidłowym przetwarzaniem danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości, by chronić niezawisłość sprawowania wymiaru sprawiedliwości, powinien być powierzony wyłącznie specjalnym organom w systemie wymiaru sprawiedliwości

danego państwa członkowskiego, a więc nie organom nadzorczym, o których mowa w art. 51 rozporządzenia 2016/679, ale również nie organom nadzorczym usytuowanym w systemie sądownictwa. Doprecyzowanie przepisów krajowych oraz opracowanie jednolitych wytycznych interpretacyjnych w tym zakresie mogłoby przyczynić się do zwiększenia przejrzystości nadzoru oraz zapewnienia spójności stosowania przepisów o ochronie danych osobowych w szczególności w kontekście powołania niezależnego organu nadzorczego – innego niż Prezes UODO, który jest niezależnym organem publicznym odpowiedzialnym za monitorowanie stosowania rozporządzenia 2016/679 w celu ochrony podstawowych praw i wolności osób fizycznych, m. in. w związku z przetwarzaniem danych osobowych (art. 51 ust. 1 ww. rozporządzenia) oraz za monitorowanie stosowania dyrektywy 2016/680 dla ochrony tych praw i wolności (art. 41 ust. 1 ww. dyrektywy), znajdującym się poza strukturami władzy sądowniczej, czyli poza systemem wymiaru sprawiedliwości.

W związku z realizowanymi przez Komisję Europejską pracami nad ewaluacją dyrektywy (UE) 2016/680, o czym wspomniano we wstępie, organ nadzorczy jest zobowiązany do przedstawienia ww. organowi UE informacji o stopniu wdrożenia przepisów dyrektywy do polskiego porządku prawnego. Zgodnie z nadesłanymi odpowiedziami pozostałych organów ochrony danych funkcjonujących w Polsce na przekazany przez Prezesa UODO kwestionariusz, wskazać należy ze analiza nadesłanych odpowiedzi potwierdza, że wyłączenie podmiotowe i przedmiotowe określone w art. 1 pkt 3 oraz art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości powoduje, że znaczna część sądów w Polsce nie identyfikuje obszarów dla których ma stosować przepisy ustawy. Jednocześnie wyłączony został nadzór nad sądami w obszarze regulacji ustawy na mocy art. 1 pkt 3. W konsekwencji wszystkie obszary, w których sądy wykonują swoje zadania w zakresie regulacji ustawy – tj. w zakresie zapobiegania i zwalczania przestępczości – wyłączone zostały spod jej zastosowania. **Obszary te pozostają wyłączone z zakresu zastosowania przepisów rozporządzenia ogólnego o ochronie danych osobowych na mocy przepisu art. 2 ust. 2 pkt lit. d rozporządzenia 2016/679. W konsekwencji, jedynymi przepisami regulującymi sposób przetwarzania danych w procesach objętych materią ustawy, są przepisy właściwych procedur (kodeksów, ustaw), które nie uwzględniają wymogów ochrony danych osobowych na poziomie wymaganych dyrektywą (UE) 2016/680.**

Na konieczność tych zmian wskazuje zatem nie tylko Prezes Urzędu Ochrony Danych Osobowych. W toku ewaluacji stosowania dyrektywy (UE) 2016/680, o której mowa w art. 62 ust. 3 tej dyrektywy, część organów nadzorczych właściwych dla sądów, która zwróciła się do Prezesa UODO, wskazuje na pilną potrzebę nowelizacji krajowych przepisów wdrażających dyrektywę (UE) 2016/680 w celu pełnego i jednoznacznego dostosowania ich do jej wymogów – w szczególności w odniesieniu do sądów powszechnych. Sygnalizowane przez te organy problemy potwierdzają systemowy charakter nieprawidłowości oraz konieczność podjęcia działań legislacyjnych w celu zapewnienia zgodności krajowego systemu nadzoru z prawem Unii Europejskiej.

III. Nadzór nad przetwarzaniem danych osobowych przez prokuraturę.

Kolejnym problemem – wywołującym zastrzeżenia co do interpretacji przepisów rozporządzenia 2016/679 oraz dyrektywy (UE) 2016/680, jak również implementującej ją ustawy – są uregulowania dotyczące nadzoru nad przetwarzaniem danych osobowych przez prokuraturę.

Organ właściwy w sprawie ochrony danych osobowych konsekwentnie, już od zainicjowania prac legislacyjnych dotyczących ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (por. pkt II powyżej), a następnie na etapie procesu legislacyjnego, opiniując projekt ustawy o zmianie ustawy - Kodeks postępowania cywilnego, ustawy - Prawo o ustroju sądów powszechnych, ustawy - Kodeks postępowania karnego oraz niektórych innych ustaw, wskazywał na konieczność zmian lub doprecyzowania przepisów w zakresie nadzoru nad przetwarzaniem przez powszechne jednostki prokuratury danych osobowych[37].

W motywie 20 zdanie pierwsze rozporządzenia 2016/679 oraz w motywie 80 zdanie pierwsze dyrektywy (UE) 2016/680 podkreślono, że odpowiednio: rozporządzenie i dyrektywa mają zastosowanie między innymi do działań sądów i innych organów wymiaru sprawiedliwości.

Mocą art. 45 ust. 2 zdanie drugie dyrektywy (UE) 2016/680 prawodawca upoważnił państwa członkowskie, by ustanowić inny niż organ nadzorczy w rozumieniu art. 41 dyrektywy 2016/680 (w Rzeczypospolitej Polskiej – Prezes Urzędu Ochrony Danych Osobowych zgodnie z art. 34 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych) do nadzorowania operacji przetwarzania dokonywanych przez inne niż sądy niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości. Choć więc w motywie 80 zdanie trzecie *in fine* dyrektywy 2016/680 prawodawca unijny przewidział możliwość, by za niezależny organ wymiaru sprawiedliwości uznać prokuraturę, to podyktowane to było różnymi modelami funkcjonowania prokuratury w poszczególnych państwach członkowskich. Dlatego w powoływanym wyżej motywie 80 zdanie trzecie *in fine* dyrektywy 2016/680 prawodawca unijny poprzestał na sformułowaniu „[…] **przykładowo przez** prokuraturę", pozostawiając uregulowaniom państw członkowskich i orzecznictwu sądowemu ocenę, czy uwzględniając całokształt przepisów i norm kompetencyjnych w danym państwie członkowskim prokuratura spełnia wymagania niezbędne do uznania za niezależny organ wymiaru sprawiedliwości.

Przenosząc te rozważania na grunt polskiego ustawodawstwa przypomnieć należy, że wyłączność w zakresie sprawowania wymiaru sprawiedliwości w Rzeczypospolitej Polskiej należy do sądów: Sądu Najwyższego, sądów powszechnych, sądów administracyjnych i sądów wojskowych (art. 10 ust. 2 i art. 175 ust. 1 Konstytucji RP). **Jednostki organizacyjne prokuratury nie mogą zostać uznane za niezależne organy wymiaru sprawiedliwości także ze względu na model funkcjonowania prokuratury w Rzeczypospolitej Polskiej** – hierarchiczne podporządkowanie, a nie niezależność[38]. Na

[37] Opinia Prezesa Urzędu Ochrony Danych osobowych z 25 kwietnia 2023 r. (sygn. DOL.401.150.2023) skierowana do Marcina Warchoła, Sekretarza Stanu w Ministerstwie Sprawiedliwości. Także opinia Prezesa Urzędu Ochrony Danych Osobowych z 5 grudnia 2024 r.(sygn. DOL.401.437.2024).
[38] Art. 7 § 2–4, art. 13 § 1 i 3, art. 18 § 2, art. 28, art. 29 i art. 34 ustawy Prawo o prokuraturze.

konieczność posiadania przymiotu niezależności dla uznania danego podmiotu za organ wymiaru sprawiedliwości wskazał zaś tymczasem jednoznacznie Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 27 maja 2019 r. w połączonych sprawach **C-508/18** i **C-82/19** w sprawie wydawania europejskiego nakazu aresztowania[39].

Nie należy również zapominać o treści art. 191a § 1a ustawy Prawo o prokuraturze, wskazującego na sposób ochrony danych osobowych w prokuraturze w ramach realizacji zadań określonych w art. 2 ustawy tej ustawy. Nadzór nad ochroną danych sprawują wyłącznie powszechne jednostki organizacyjne prokuratury, a nie organ niezależny. Zgodnie bowiem z tym przepisem w zakresie danych osobowych przetwarzanych przez powszechne jednostki organizacyjne prokuratury w ramach realizacji zadań określonych w art. 2, obowiązki, uprawnienia i zadania organu nadzorczego przewidziane w art. 5 ust. 1 pkt 1 i 5-8, art. 6, art. 7, art. 8 ust. 1 i 2, art. 10, art. 11, art. 35 ust. 6, art. 36 ust. 6 i art. 50 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości są wykonywane przez organy nadzoru, o których mowa w § 1, zaś obowiązki, uprawnienia i zadania, przewidziane w art. 38 ust. 1 i 3-5, art. 44 ust. 1 i 8, art. 45 ust. 5 oraz art. 47 ust. 1 pkt 6 tej ustawy przez organ nadzoru, o którym mowa w § 1 pkt 3. Zamiast decyzji administracyjnej, o której mowa w art. 8 ust. 2 ustawy powołanej w zdaniu pierwszym, organ nadzoru, o którym mowa w § 1, wydaje polecenie służbowe. Oznacza to, że nadzór nad przetwarzaniem danych osobowych do celów, o których mowa w art. 1 dyrektywy (UE) 2016/680, sprawowany jest w ramach tej samej struktury organizacyjnej, w której odbywa się przetwarzanie. O ile przepisy art. 191a § 1a ustawy Prawo o prokuraturze wprowadzają mechanizm nadzoru, to czynią to wyłącznie w strukturach powszechnych jednostek organizacyjnych prokuratury, nie zaś w postaci niezależnego organu nadzorczego.

Model ten pozostaje w sprzeczności z art. 41 ust. 1 dyrektywy, wymagający zapewnienia nadzoru przez organ w pełni niezależny.

W odniesieniu do organów nadzorczych właściwych dla prokuratury, wskazanych w art. 191a ustawy Prawo o prokuraturze, wnioski organu nadzorczego w toku mechanizmu ewaluacji stosowania dyrektywy (UE) 2016/680 przeprowadzonego w 2025 r. wskazują na brak wśród tych organów nadzorczych posiadania przez nie pełni właściwości, zadań i uprawnień określonych w art. 45–49 dyrektywy (UE) 2016/680, podobnie jak ma to miejsce w przypadku organów sądowych. Co więcej, w przypadku niektórych prokuratur, funkcję organu nadzorczego, o którym mowa w rozdziale VI dyrektywy, również powierzono inspektorom ochrony danych działającym w strukturach prokuratur, co pozostaje w oczywistej sprzeczności z wymogiem niezależności organu nadzorczego oraz pozycji inspektora ochrony danych osobowych w organizacji. Taki model nie wynika z przepisów prawa, lecz z praktyki organizacyjnej przyjętej przez kierownictwa jednostek, co prowadzi do rażącego konfliktu interesów i jest niezgodne z art. 33, 34, 42, 46 i 47 dyrektywy (UE) 2016/680.

Skoro zatem, zarówno w świetle przepisów konstytucyjnych, regulacji ustawy Prawo o prokuraturze, jak i ugruntowanego orzecznictwa sądów europejskich prokuratura w Rzeczypospolitej Polskiej nie może być uznana za niezależny organ wymiaru

[39] Wyrok TSUE z 27.05.2019 r., C-508/18, MINISTER FOR JUSTICE AND EQUALITY v. OG I PI., LEX nr 2671250.

sprawiedliwości, to **wskazanie kompetencji nadzorczych organów prokuratury nad przetwarzaniem przez powszechne jednostki prokuratury danych osobowych** (art. 191a ustawy Prawo o prokuraturze) **pogłębia istniejący stan niezgodności przepisów tej ustawy z unormowaniami dyrektywy (UE) 2016/680** dotyczącymi konieczności zapewnienia sprawowania nadzoru nad przetwarzaniem danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar przez niezależny organ nadzorczy (art. 41 ust. 1 dyrektywy 2016/680).

Dlatego Prezes UODO, kierując się wytycznymi zawartymi w art. 41 ust. 3 dyrektywy 2016/680, **postuluje rozpoczęcie prac legislacyjnych i uchylenie art. 191a ustawy Prawo o prokuraturze. Dzięki temu nadzór nad przetwarzaniem danych osobowych przez powszechne jednostki prokuratury do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar obejmie niezależny organ nadzorczy** (Prezes Urzędu Ochrony Danych Osobowych – art. 34 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych), **co zapewni właściwą implementację postanowień dyrektywy (UE) 2016/680.**

Jako zmianę wynikową w stosunku do wskazanej wyżej, organ właściwy w sprawie ochrony danych osobowych widzi potrzebę usunięcia z art. 1 pkt 3 ustawy krajowej sformułowania „prokuraturę". Tylko w ten sposób można osiągnąć zapewnienie konieczności respektowania – przy realizacji materii objętej tą dyrektywą – praw podstawowych i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych[40].

IV. Naruszenia ochrony danych osobowych przetwarzanych przez sądy i prokuraturę[41].

Kompetencje związane z egzekwowaniem przepisów dotyczących ochrony danych osobowych przez sądy zostały przyznane sądowym organom nadzorczym. Przepisami art. 55 ust. 3 rozporządzenia 2016/679 oraz art. 45 ust. 2 dyrektywy (UE) 2016/680 wyłączone są kompetencje organów nadzorczych do nadzorowania operacji przetwarzania dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości. W

[40] W myśl art. 1 ust. 2 lit a) dyrektywy 2016/680 – „Zgodnie z niniejszą dyrektywą państwa członkowskie: a) chronią prawa podstawowe i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych."

[41] Zgodnie z definicją zawartą w art. 4 pkt 12 rozporządzenia 2016/679 oraz w art. 3 pkt 11 dyrektywy 2016/680.

myśl art. 175db ustawy Prawo o ustroju sądów powszechnych[42] administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są sądy, zaś z art. 175dd § 1 ustawy Prawo o ustroju sądów powszechnych wynika, że nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy, zgodnie z art. 175da i art. 175db, wykonują w zakresie działalności sądu: rejonowego – prezes sądu okręgowego; okręgowego – prezes sądu apelacyjnego; apelacyjnego – Krajowa Rada Sądownictwa. Wśród zadań organów nadzorczych określonych w art. 175dd § 2 ustawy Prawo o ustroju sądów powszechnych ustawodawca nie wymienił przyjmowania zgłoszeń czy oceny naruszeń ochrony danych osobowych, a także kompetencji do przeprowadzania kontroli. Zgodnie z treścią wyroku Naczelnego Sądu Administracyjnego z 14 listopada 2025 r. (sygn. akt: III OSK 250/25) „ustawodawca konsekwentnie wyłącza właściwość Prezesa Urzędu Ochrony Danych Osobowych jako organu nadzorczego w obszarze czynności podejmowanych przez sądy - jako Administratorów – „*w ramach sprawowania wymiaru sprawiedliwości*". Regulacje te są systemowo i celowościowo skorelowane z treścią art. 55 ust. 3 RODO. Niezależnie zatem od tego, że zgodnie z ugruntowanym stanowiskiem doktryny i orzecznictwa, wykluczone jest jakiekolwiek domniemywanie treści norm kompetencyjnych, a w konsekwencji podstaw i zakresu kompetencji organów państwa, to (…) ustawodawca powiązał kompetencje organów wymienionych w art. 175dd § 1 p.u.s.p. (prezesa sądu okręgowego, prezesa sądu apelacyjnego i Krajowej Rady Sądownictwa) z obowiązkiem gwarantowania przez te organy wymagań RODO. Nie można zatem podzielić stanowiska (…), że jedynie nadzór sprawowany przez ten organ gwarantuje właściwy poziom ochrony danych osobowych i wypełnianie wymogów wynikających z prawa UE i art. 9 Konstytucji RP".

Niezależnie od orzekania, sądy wykonują również działalność administracyjną. Jej istota sprowadza się do zapewnienia odpowiednich warunków technicznych i organizacyjnych dla wykonywania przez sąd powierzonych mu zadań z zakresu sprawowania wymiaru sprawiedliwości i ochrony prawnej. Zgodnie z art. 8 pkt 1 i 2 ustawy Prawo o ustroju sądów powszechnych, działalność administracyjna sądów polega na zapewnieniu odpowiednich warunków techniczno-organizacyjnych oraz majątkowych funkcjonowania sądu i wykonywania przez sąd zadań, o których mowa w art. 1 § 2 i 3 tejże ustawy (na podstawie art. 31a § 1 ww. ustawy, czynności te należą do kompetencji dyrektora sądu) oraz zapewnieniu właściwego toku wewnętrznego urzędowania sądu, bezpośrednio związanego z wykonywaniem przez sąd zadań, o których mowa w art. 1 § 2 i 3 (na podstawie art. 22 § 1 ww. ustawy, czynności te należą do prezesa sądu).

Przetwarzanie danych osobowych przez sądy związane ze sprawowaniem wymiaru sprawiedliwości rozstrzygane są poza nadzorem, który – zgodnie z ustawą o ochronie

[42] Z art. 175db § 2 Prawa o ustroju sądów powszechnych wynika, że w ramach nadzoru, o którym mowa w § 1, właściwe organy: 1) rozpatrują skargi osób, których dane osobowe są przetwarzane niezgodnie z prawem; 2) podejmują działania mające na celu upowszechnianie wśród nadzorowanych administratorów i podmiotów przetwarzających wiedzy o obowiązkach wynikających z RODO, 3) współpracują z innymi organami sprawującymi nadzór nad przetwarzaniem danych osobowych w ramach postępowań prowadzonych przez sądy i trybunały oraz z organami nadzorczymi w rozumieniu art. 51 rozporządzenia 2016/679, w tym dzielą się informacjami oraz świadczą wzajemną pomoc, w celu zapewnienia spójnego stosowania rozporządzenia 2016/679 oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – sprawowany jest przez Prezesa UODO (art. 44 ust. 1 zdanie pierwsze tej ustawy stanowi, że w przypadku naruszenia ochrony danych osobowych, administrator, bez zbędnej zwłoki, nie później jednak niż w ciągu 72 godzin po stwierdzeniu naruszenia, zgłasza naruszenie Prezesowi Urzędu).

Realizacja powyższych kompetencji nie ma wpływu na niezawisłość sądu, co jest szczególnie istotne ze względu na zasadę wyrażoną m.in. w art. 55 ust. 3 rozporządzenia 2016/679. Ocena tego, czy dane zdarzenie jest naruszeniem, jak również, czy jest incydentem związanym bezpośrednio ze sprawowaniem wymiaru sprawiedliwości, a tym samym niepodlegającym obowiązkowi notyfikacji do Prezesa UODO, należy w pierwszej kolejności do odpowiednich organów wymiaru sprawiedliwości. Problemem praktycznym jaki wyłania się w tej materii jest trudność w określeniu granicy sprawowania wymiaru sprawiedliwości w odniesieniu do przetwarzania danych osobowych w sądach oraz ewentualnych naruszeń nie mieszczących się w tej sferze.

Inaczej wygląda zgłaszanie naruszeń oraz wykonywanie uprawnień kontrolnych przez prokuraturę. W art. 1 pkt 3 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości stanowi się, że ustawa określa sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez właściwe organy w celach, o których mowa w pkt 1, **z wyłączeniem danych osobowych przetwarzanych przez prokuraturę** i sądy, a z treści art. 3 pkt 1 tejże ustawy wynika, że przepisów tej ustawy nie stosuje się do ochrony danych osobowych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, m. in prowadzonych na podstawie ustawy Prawo o prokuraturze.

Gdyby przyjąć brak właściwości Prezesa UODO w zakresie przyjmowania zgłoszeń naruszeń oraz przeprowadzania kontroli, to prokuratura pozostałaby poza jakimkolwiek nadzorem w tym zakresie. **Wyłączenia ze wskazanej ustawy w przypadku prokuratury, a także pozostałych podmiotów działających na podstawie ustaw** wskazanych w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, to jest: Policji, Straży Granicznej, Służby Więziennej, straży miejskich/gminnych, Straży Leśnej, Państwowej oraz Społecznej Straży Rybackiej (słowem wobec wszystkich organów realizujących cele, o których mowa w art. 1 pkt 1 ustawy z 14 grudnia 2018 r.) **są jedynie rezultatem nieprawidłowej krajowej implementacji dyrektywy (UE) 2016/680.**

Uprawnienia niezależnego organu nadzorczego do przeprowadzania kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych organu nadzorczego, jak i kompetencje w zakresie odbierania zgłoszeń o naruszeniach ochrony danych osobowych, są niezwykle istotne dla skutecznej ochrony praw osób, których dane są przetwarzane, jak i dla zapobiegania naruszeniom. **Konsekwencją braku zmian wyżej przytoczonych przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości jest przede wszystkim niezgłaszanie organowi nadzorczemu naruszeń dotyczących bezpieczeństwa przetwarzanych danych przez administratorów.** Dane osobowe określone w art. 3 pkt 1 ustawy z 14 grudnia 2018 r., w tym te zawarte w aktach spraw i urządzeniach,

dotyczących spraw prowadzonych przez prokuratorów, są przecież w polskim prawie wyłączone spod nadzoru niezależnego organu ochrony danych.

Analizując przyjęty w Polsce model przetwarzania danych osobowych dla prowadzenia postępowania karnego – w kontekście prawa konstytucyjnego, prawa międzynarodowego, prawa Unii Europejskiej, a także orzecznictwa sądów międzynarodowych – należy wskazać na brak konkretnych środków ochrony praw i wolności osób, których dane dotyczą. **Model ten pozbawia osoby, których dane są przetwarzane przysługujących im gwarancji w zakresie ochrony danych osobowych, a także nie uwzględnia poszanowania ich prawa do prywatności**. Co więcej, wyłączenie działań prokuratury spod mocy ustawy wskazuje na fakt braku respektowania zasad odnoszących się do przetwarzania danych osobowych. W rezultacie wnioskować można by, że prokuratury nie wiążą zasady dotyczące przetwarzania danych osobowych: zasada legalizmu, minimalizacji danych, ograniczenia celu. Praktyka organu nadzorczego pokazuje, że prokuratura w niektórych przypadkach przetwarza dane w sposób nieproporcjonalny do celu ścigania lub zapobiegania przestępstwom, tym samym nie respektując obowiązków administratora oraz podstawowych praw podmiotów danych[43]. Doskonałym tego przykładem jest wyrok Europejskiego Trybunału Praw Człowieka (ETPC) z 13 listopada 2025 r. w sprawie *A.G-Ś przeciwko Polsce*. Skarga rozpatrzona przez ETPC dotyczyła ujawnienia przez Narodowy Fundusz Zdrowia dokumentacji medycznej skarżącej będącej świadkiem w postępowaniu przygotowawczym (dochodzeniu) prowadzonym przez prokuraturę, dotyczącym jej męża, oskarżonego o udział w zorganizowanej grupie przestępczej. Akta śledztwa, w tym dokumentacja medyczna skarżącej zawierająca dane o jej stanie zdrowia, zostały udostępnione stronom tego postępowania oraz w innych postępowaniach.

Brak regulacji wskazujących organy uprawnione do realizacji kompetencji kontrolnych w związku z naruszeniami ochrony danych osobowych, a mających status niezależnych organów nadzorczych, nie powinien mieć miejsca. Prezes Urzędu Ochrony Danych Osobowych w kontekście analizy działań naprawczych dotyczących wykonania tego wyroku[44] zaakcentował nie tylko konsekwencje braku niezależnego organu nadzorczego w strukturze organów prokuratury, ale również podkreślił, że przepisy ustawy Kodeks postępowania karnego nie zawierają w istocie żadnych rozwiązań dedykowanych ochronie danych osobowych i prywatności uczestników postępowań. Przy obecnej konstrukcji art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości i przy braku przepisów szczególnych w Kodeksie postępowania karnego, **dane osobowe**

[43] Jednym z takich przykładów jest naruszenie bezpieczeństwa danych przez Prokuraturę Regionalną w Szczecinie, polegające na zatrzymaniu całej dokumentacji medycznej zawierającej dane wrażliwe pacjentek leczonych w jednej z praktyk lekarskich (a nie wyłącznie jednej pacjentki). Prezes UODO pismem z 10 marca 2024 r. zwrócił się do Prokuratora Krajowego o zwrócenie uwagi kierownikom podległych Prokuratorowi Krajowemu powszechnych jednostek organizacyjnych prokuratury na niedopuszczalność przetwarzania bez podstawy prawnej danych osobowych, w szczególności danych podlegających wzmożonej ochronie, w tym danych o stanie zdrowia. Wystąpienie dotyczyło czynności przeprowadzonych przez funkcjonariuszy Delegatury Centralnego Biura Antykorupcyjnego w Szczecinie w wykonaniu postanowienia prokuratora o żądaniu wydania rzeczy i przeszukaniu w postępowaniu przygotowawczym prowadzonym przez Prokuraturę Regionalną w Szczecinie (sygn. I Ds. 31.2020).

[44] Pismo Prezesa UODO z 2 stycznia 2026 r. skierowane do Pełnomocnika Ministra Spraw Wewnętrznych i Administracji do spraw Współpracy Międzynarodowej.

pozostające w treści akt spraw (a także akt czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych) **nie podlegają żadnym przepisom gwarantującym ochronę danych osobowych** (odnosi się to również innych aktów prawnych objętych przedmiotowym wyłączeniem).

Trybunał Sprawiedliwości UE w licznych orzeczeniach niejednokrotnie wskazywał na konieczność zapewnienia w prawie krajowym gwarancji w postaci kontroli niezależnego organu, mającego status osoby trzeciej w stosunku do organu przetwarzającego dane osobowe. Doskonałym przykładem jest m. in. wyrok TSUE z 30 kwietnia 2024 r. w sprawie C-470/21 La Quadrature du Net, w którym Trybunał wyraźnie stwierdził, że: „sąd lub organ zajmujący się kontrolą musi być w stanie zapewnić właściwą równowagę pomiędzy z jednej strony interesami związanymi z potrzebami dochodzenia w ramach zwalczania przestępczości, a z drugiej strony prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych osób, których dane są udostępniane. W demokratycznym państwie prawa zasadność pozyskania danych powinna być poddana kontroli sądu lub niezależnego organu administracyjnego.”. Kontrola przeprowadzana przez te podmioty byłaby też zgodna z zasadą pogłębiania zaufania obywateli do państwa, gdyż eliminowałaby ryzyko nieproporcjonalnej ingerencji w prawa podstawowe, jak też gwarantowałaby pewność stosowania prawa (na co wskazywał TSUE w wyroku z 8 kwietnia 2014 r. w sprawach połączonych Digital Rights Ireland Ltd (C-293/12) i Kärntner Landesregierung (C-594/12).

V. Nadzór nad wielkoskalowymi systemami informacyjnymi UE.

Prezes UODO od wielu lat jest aktywnym członkiem Komitetu Skoordynowanego Nadzoru w zakresie nadzoru nad wielkoskalowymi systemami informacyjnymi Unii Europejskiej. Systemy te służą państwom członkowskim UE do wspólnego zarządzania granicami, migracją, bezpieczeństwem i wymiarem sprawiedliwości. Państwa członkowskie, korzystając z krajowych punktów dostępowych, przetwarzają dane dla potrzeb infrastruktury unijnej służącej interesowi wspólnemu. Wielkoskalowe systemy informacyjne UE nie mają charakteru krajowego. Są częścią wspólnej infrastruktury Unii, opierającej swe funkcjonowanie na wzajemnym zaufaniu państw członkowskich. Dane w tych systemach stanowią wspólny zasób Unii Europejskiej, dlatego przetwarzanie danych osobowych i nadzór nad ich przetwarzaniem powinien być zapewniony na poziomie odpowiadającym standardom unijnym. Jest to zarówno kwestia zaufania między państwami członkowskimi, jak i warunek sprawnego i bezpiecznego działania całej infrastruktury informacyjnej UE oraz organów poszczególnych państw członkowskich opierających swoje działania o dane i informacje zgormadzone w tych systemach.

Systemy te, w tym SIS[45], VIS[46], EES[47], ETIAS[48], ECRIS-TCN[49] oraz Eurodac stanowią część wspólnej infrastruktury Unii Europejskiej, w której dane osobowe stanowią wspólny zasób państw członkowskich Unii Europejskiej. Prawo UE nakłada na uczestniczące w ich obsłudze organy krajowe obowiązek stosowania wysokich standardów ochrony danych, w tym dyrektywy (UE) 2016/680 jako podstawy przetwarzania danych osobowych w celach związanych z zapewnieniem porządku publicznego, bezpieczeństwa i wymiaru sprawiedliwości (np. art. 66 ust. 2 rozporządzenia (UE) 2018/1862[50] w sprawie SIS, art. 36a ust. 3 rozporządzenia 767/2008[51] w sprawie VIS, art. 49 ust. 3 rozporządzenia 2017/2226[52] w sprawie EES czy art. 56 ust. 3 rozporządzenia 2018/1240[53] w sprawie ETIAS). Europejski standard przewiduje nie tylko gwarancję praw jednostki, ale również istnienie niezależnego organu nadzorczego posiadającego pełnię uprawnień do przyjmowania zgłoszeń naruszeń, rozpatrywania skarg i przeprowadzania kontroli zgodnie z międzynarodowymi standardami audytu w systemach uczestniczących w przetwarzaniu danych dla wspólnego celu. Niezależność organu nadzorczego jest kluczowa dla zapewnienia spójności, bezpieczeństwa i wzajemnego zaufania między państwami członkowskimi.

Ponadto, wielkoskalowe systemy informacyjne Unii Europejskiej podlegają mechanizmowi skoordynowanego nadzoru zgodnie z art. 62 rozporządzenia 2018/1725. Europejski Inspektor Ochrony Danych (EIOD) oraz krajowe organy nadzorcze – każdy w zakresie swoich kompetencji – mają obowiązek współdziałać w ramach mechanizmu skoordynowanego nadzoru (art. 62 rozporządzenia 2018/1725[54]), aby zapewnić spójny, skuteczny i niezależny nadzór nad przetwarzaniem danych w wielkoskalowych systemach

[45] System Informacji Schengen (ang. Schengen Information System (SIS)).
[46] Wizowy System Informacyjny (ang. Visa Information System (VIS)).
[47] System wjazdu/wyjazdu (ang. Entry/Exit System (EES)).
[48] Unijny system informacji o podróży oraz zezwoleń na podróż (ang. European Travel Information and Authorisation System (ETIAS)).
[49] Europejski system przekazywania informacji z rejestrów karnych – informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich (ang. European Criminal Records Information System - Third Country Nationals (ECRIS-TCN)).
[50] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE.
[51]Rozporządzenie Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany informacji pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, wiz długoterminowych i dokumentów pobytowych.
[52] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011.
[53] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226.
[54] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

informacyjnych i jednostkami organizacyjnymi Unii Europejskiej. Dla realizacji tej współpracy organy prowadzą wymianę informacji, wspierają się wzajemnie w audytach i inspekcjach, analizują trudności w interpretacji prawa oraz propagują wiedzę o prawach do ochrony danych.

W Polsce dostęp do tych systemów posiadają m.in. Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, a także sądy i prokuratura. Jednakże, krajowy model nadzoru, przyjęty w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz w ustawach sektorowych, nie zapewnia pełnej zgodności z wymogami UE.

Przewidziane wyłączenia gwarancji ochrony danych osobowych w art. 1 pkt 3 oraz art. 3 ustawy z dnia 14 grudnia 2018 r. **mają zatem szerokie i poważne konsekwencje nie tylko dla krajowego, lecz także dla unijnego systemu ochrony danych osobowych w odniesieniu do funkcjonowania wielkoskalowych systemów informacyjnych Unii Europejskiej oraz dla utrzymania unijnego porządku prawnego w ogólności.** Wyłączenia te prowadzą zatem do przetwarzania danych osobowych przez krajowe podmioty i organy, przy realizacji wspólnej infrastruktury Unii Europejskiej, danych nie podlegającego żadnemu nadzorowi ani gwarancjom przewidzianym przez prawo Unii. Oznacza to, że Polska konsekwentnie nie realizuje obowiązków wynikających z unijnych rozporządzeń sektorowych. **Wyłączenia stosowania przepisów ochrony danych wobec prokuratury, sądów i organów wymienionych w art. 3 pkt 2 ustawy z 14 grudnia 2018 r. powodują, że osoby fizyczne nie mają zapewnionej pełnej możliwości egzekwowania swoich praw w zakresie ochrony danych względem tych podmiotów.**

Brak pełnego stosowania dyrektywy (UE) 2016/680 oraz brak skutecznego nadzoru krajowego nad tym przetwarzaniem podważa spójność i bezpieczeństwo całego systemu – w tym systemów centralnych, unijnych – powodując ryzyko błędów, nieuprawnionych zmian danych i naruszeń integralności informacji o znaczeniu transgranicznym, potencjalnie także dezinformacji. Takie naruszenia mogą wprost wpływać na bezpieczeństwo obywateli, funkcjonowanie i korzystanie ze wspólnych rejestrów UE. W szerszej perspektywie osłabia to bezpieczeństwo Unii Europejskiej jako całości oraz zaufanie do jej zdolności do ochrony danych przetwarzanych w ramach współpracy policyjnej i sądowej. Systemy centralne UE, oparte na zasadzie wzajemnego zaufania między państwami członkowskimi, funkcjonują prawidłowo wyłącznie przy założeniu jednolitego i skutecznego stosowania standardów ochrony danych oraz istnienia realnego, niezależnego nadzoru krajowego.

W konsekwencji brak udziału niezależnego organu nadzorczego posiadającego pełnię uprawnień wynikających z art. 46 i art. 47 dyrektywy (UE) 2016/680 skutkuje nie tylko luką w krajowym systemie nadzoru, lecz także niespójnością z unijnym mechanizmem skoordynowanego nadzoru, utrudniającą współpracę z EIOD i ograniczającą udział Polski w pracach Komitetu Skoordynowanego Nadzoru.

Zasada niezależności organów ochrony danych, o których mowa w art. 42 dyrektywy (UE) 2016/680, stanowi fundament skutecznego nadzoru. **Niedopuszczalne jest, aby w mechanizmie skoordynowanego nadzoru uczestniczyły podmioty, które pełnią jednocześnie funkcję organu nadzorczego i organu nadzorowanego.** Taka

sytuacja prowadzi do konfliktu interesów i ogranicza możliwość niezależnego podejmowania decyzji.

W polskim porządku prawnym – z uwagi na wskazane wyłączenia stosowania przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – Prezes Urzędu Ochrony Danych Osobowych jako członek Komitetu Skoordynowanego Nadzoru nie posiada pełnych uprawnień jako organ nadzorczy. Przyjęty przez polskiego prawodawcę hierarchiczny model organów nadzorczych odpowiednio w sądach i prokuraturze przy obecnym systemie nadzoru powodują, że nie istnieje żaden niezależny organ nadzorczy, posiadający pełnię uprawnień, o których mowa w dyrektywie (UE) 2016/680. W skoordynowanym nadzorze nie uczestniczy zatem żaden niezależny organ ochrony danych dysponujący pełnią uprawnień wynikających z tejże dyrektywy. Polska uczestniczy w mechanizmie skoordynowanego nadzoru w sposób połowiczny – ogranicza to skuteczność i spójność tego nadzoru.

Zapewnienie ochrony danych osobowych przetwarzanych w celach ochrony porządku publicznego oraz skutecznego i niezależnego nadzoru nad ich przetwarzaniem w wielkoskalowych systemach informacyjnych Unii Europejskiej jest warunkiem nie tylko ochrony praw jednostek i spójności unijnego systemu ochrony danych, lecz także pełnego i wiarygodnego wykonywania przez Polskę zobowiązań wynikających z członkostwa w Unii Europejskiej oraz utrzymania jej pozycji jako wiarygodnego uczestnika wspólnej przestrzeni bezpieczeństwa, wolności i sprawiedliwości.

W związku z powyższym Prezes Urzędu Ochrony Danych Osobowych postuluje **wprowadzenie zmian legislacyjnych umożliwiających pełną realizację mechanizmu skoordynowanego nadzoru przewidzianego w prawie Unii Europejskiej**. Zmiany te powinny zapewnić, aby przetwarzanie danych osobowych w ramach wielkoskalowych systemów informacyjnych UE w Polsce podlegało nadzorowi niezależnego organu nadzorczego wyposażonego w pełnię kompetencji wynikających z dyrektywy (UE) 2016/680, w tym w szczególności uprawnienie do przeprowadzania kontroli we wszystkich podmiotach uczestniczących w obsłudze tych systemów. Usunięcie wskazanych wcześniej ograniczeń krajowego modelu nadzoru jest niezbędne, aby zapewnić pełną zgodność z prawem Unii oraz umożliwić skuteczny udział Polski w mechanizmie skoordynowanego nadzoru nad wielkoskalowymi systemami informacyjnymi UE.

VI. Sankcje.

Zgodnie z art. 57 dyrektywy (UE) 2016/680 państwa członkowskie mają obowiązek **przyjęcia przepisów określających sankcje za naruszenie przepisów wdrażających dyrektywę** oraz **zapewnienia ich skutecznego wykonania**. Sankcje te powinny być skuteczne, proporcjonalne i odstraszające.

Tymczasem ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości nie wyposaża Prezesa Urzędu Ochrony Danych Osobowych w żadne instrumenty sankcyjne o takim charakterze. Przepisy dyrektywy (UE) 2016/680 nie są w tym zakresie wykonywane.

W postępowaniach dotyczących naruszeń przepisów tej ustawy Prezes Urzędu Ochrony Danych Osobowych nie może nakładać administracyjnych kar pieniężnych, a zatem nie dysponuje wystarczającym środkiem o charakterze prewencyjnym czy odstraszającym.

W przypadku stwierdzenia naruszenia, które zostało następnie usunięte, organ, w przeciwieństwie do sytuacji przewidzianej w rozporządzeniu (UE) 2016/679, nie może ani udzielić upomnienia, ani nałożyć kary pieniężnej. Brak takiej możliwości ogranicza katalog dostępnych środków reakcji i pozbawia postępowanie waloru prewencyjnego oraz wychowawczego.

Upomnienie, przewidziane w rozporządzeniu (UE) 2016/679 jako środek umożliwiający zareagowanie na naruszenie, które już usunięto, nie zostało przewidziane w ustawie z 14 grudnia 2018 r. Z perspektywy praktyki nadzorczej jego brak znacząco ogranicza skuteczność działań organu ochrony danych, ponieważ uniemożliwia formalne zwrócenie uwagi administratorowi lub podmiotowi przetwarzającemu na stwierdzone nieprawidłowości.

Prezes Urzędu Ochrony Danych Osobowych jest jedynym organem nadzorczym w systemie krajowym, który nie posiada uprawnienia do udzielenia upomnienia, w odróżnieniu od organów nadzorczych właściwych dla sądów i prokuratur.

Choć dyrektywa (UE) 2016/680 pozostawia państwom członkowskim swobodę w doborze środków sankcyjnych, to obecne rozwiązania krajowe nie zapewniają żadnych realnych instrumentów egzekwowania prawa, przez co implementacja art. 57 dyrektywy (UE) 2016/680 jest nieskuteczna i pozbawiona efektu użytecznego (effet utile).

Taki stan rzeczy osłabia system ochrony danych w obszarze bezpieczeństwa i wymiaru sprawiedliwości oraz narusza zobowiązania Polski jako państwa członkowskiego Unii Europejskiej.

VII. Zasady przetwarzania danych.

Zasady przetwarzania danych osobowych zostały określone w art. 4 dyrektywy (UE) 2016/680 i są zbliżone do zasad wynikających z ogólnego rozporządzenia o ochronie danych osobowych, lecz dostosowane do specyfiki działań organów ścigania.

Ustawodawca krajowy jako naczelną zasadę przetwarzania danych uznał zasadę legalności wskazaną w art. 13 ustawy z 14 grudnia 2018 r. i umieścił ją w rozdziale 3 tejże ustawy zatytułowanym „Zasady dotyczące przetwarzania danych osobowych”. Pozostałe zasady dotyczące przetwarzania danych osobowych zostały umieszczone w rozdziale dotyczącym obowiązków administratora, co w założeniu miało skutkować zwiększeniem skuteczności ich przestrzegania oraz gwarancją ich prawidłowej realizacji przez poszczególnych administratorów.

Zasady przetwarzania danych poprzez ich określenie na poziomie normatywnym stanowią nadrzędne normy w stosunku do pozostałych przepisów o kluczowym znaczeniu dla całej regulacji. Zasady przetwarzania danych są elementem zapewniającym spójność ochrony danych w związku z ich przetwarzaniem przez właściwe organy do celów zapobiegania, przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar. Określają one sposób wykładni

poszczególnych przepisów w razie wątpliwości interpretacyjnej. Dlatego też zasadom przetwarzania danych osobowych przypisuje się funkcję regulacyjną, ochronną, systematyzującą, określającą w jaki sposób dane mają być zbierane, wykorzystywane i przechowywane – przetwarzane – aby zapewnić ich bezpieczeństwo oraz poszanowanie prywatności osób, których dane dotyczą.

Z założenia zasady wprost komunikują prawa i obowiązki podmiotów je przetwarzających. Są nadrzędne wobec obowiązków w przypadku zaistnienia konfliktu. Respektowanie zasad dotyczących przetwarzania danych osobowych, kierowanie się nimi przy ważeniu *ratio legis*, interesów wykonawców norm, ale i praw i wolności podmiotów danych jest wymagane przy tworzeniu szczególnych regulacji krajowych.

Taki – jak w art. 13 ustawy z 14 grudnia 2018 r. – **model przyjęty przez ustawodawcę i umiejscowienie zasad dotyczących przetwarzania danych osobowych w części obejmującej obowiązki administratora stanowi o umniejszeniu ich roli i funkcji.** Prowadzi do mechanicznego stosowania przepisów, zmniejsza przejrzystość dla podmiotów danych, a w konsekwencji pod wątpliwość poddaje respektowanie praw osób których dane dotyczą, szczególnie w kontekście wyłączenia wskazanego w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

VIII. Zadania inspektora ochrony danych (IOD).

W toku prac legislacyjnych w zakresie objętym niniejszym wystąpieniem warto byłoby przeanalizować także **regulacje odnoszące się do inspektorów ochrony danych (IOD)**.

Prezes Urzędu Ochrony Danych Osobowych konsekwentnie, tj. od ponad 3 lat w kierowanych do Ministerstwa Spraw Wewnętrznych i Administracji wystąpieniach podnosił konieczność podjęcia prac nad nowelizacją przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości w zakresie odnoszącym się do inspektora ochrony danych. W wystąpieniach z 19 lipca 2022 r. i 13 września 2025 r.[55] Prezes UODO wskazał, że w przepisach ww. ustawy w sposób niezgodny z dyrektywą (UE) 2016/680 ukształtowano zadania inspektora ochrony danych oraz nieprecyzyjnie określono obowiązek przesyłania zawiadomień dotyczących IOD, powodując w tym zakresie istotne problemy w stosowaniu tych przepisów przez podmioty zobowiązane do ich przestrzegania.

Prezes Urzędu Ochrony Danych Osobowych zwrócił uwagę na błąd w konstrukcji art. 38 ust. 6 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, który stanowi, że realizację obowiązków, o których mowa w ust. 1- 4 tego artykułu, administrator lub podmiot przetwarzający może powierzyć inspektorowi ochrony danych[56]. Prezes UODO sygnalizował również, że z przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości wynika obowiązek administratora poinformowania Prezesa Urzędu Ochrony Danych Osobowych o każdej zmianie

[55] Prowadzone pod sygnaturą DOL.413.11.2022.
[56] Wystąpienie Prezesa UODO z 7 lutego 2022 r. sygn. DOL.413.4.2022.

dotyczącej inspektora ochrony danych, przepisy te nie uwzględniają zaś konieczności poinformowania o każdej zmianie dotyczącej administratora (art. 46 ust. 10). Zmian wymaga także art. 37 ust. 3 ustawy, zgodnie z którym przeprowadzenie oceny skutków dla ochrony danych administrator może powierzyć inspektorowi ochrony danych, co nie jest rozwiązaniem prawidłowym i wymaga zmiany, gdyż przepisy dyrektywy nie dopuszczają możliwości scedowania takiego obowiązku przez administratora na jakikolwiek inny podmiot. Roli administratora nie może pełnić inspektor ochrony danych.

Pismem z 13 września 2025 r. (sygnatura DOL.413.11.2022) Prezes UODO po raz kolejny wystąpił do Ministra Spraw Wewnętrznych i Administracji o podjęcie prac legislacyjnych w zakresie wprowadzenia zmian do ustawy z dnia 14 grudnia 2018 r. odnoszących się do inspektora ochrony danych, w celu zapewnienia prawidłowej implementacji dyrektywy (UE) 2016/680. Jednym z poruszonych w tym wystąpieniu zagadnień jest rola jaką pełni IOD w świetle dyrektywy 2016/680. Jego zadaniem jest wspieranie administratora w przestrzeganiu i właściwym stosowaniu przepisów o ochronie danych osobowych. Zadaniem IOD nie jest natomiast wyręczanie administratora w realizacji jego zadań, tj. przeprowadzenie oceny skutków dla ochrony danych oraz występowanie z wnioskiem o uprzednie konsultacje. Doskonale ten problem obrazuje również ewaluacja dotycząca dyrektywy (UE) 2016/680 przeprowadzona w 2025 r. W nadesłanych do Urzędu Ochrony Danych Osobowych kwestionariuszach kierowanych do organów nadzorczych, w znacznej części przypadków odpowiedzi udzielane były przez Inspektora Ochrony Danych Osobowych, który w miejsce administratora analizował i wypełniał dedykowany administratorom danych kwestionariusz.

Istotne także są wcześniej ujęte uwagi dotyczące IOD, wskazane w pkt II niniejszego wystąpienia.

IX. Dostęp pośredni wynikający z art. 17 dyrektywy (UE) 2016/680.

Przepisami dyrektywy (UE) 2016/680 ustanowiono granice ingerencji w prawa człowieka, by osiągnąć równowagę między koniecznością zapewnienia efektywności działalności organom odpowiedzialnym za walkę z przestępczością a prawami jednostki do ochrony prywatności i ochrony danych osobowych.

Mechanizm pośredniego dostępu jest ściśle powiązany z art. 8 ust. 3 KPP, który stanowi, że przestrzeganie zasad ochrony danych osobowych podlega kontroli niezależnego organu. Potwierdza to również Trybunał Sprawiedliwości UE, wskazując w swoim orzecznictwie, że wykonywanie przez organ nadzorczy zadań w ramach art. 17 dyrektywy (UE) 2016/680 musi odbywać się w warunkach pełnej niezależności, a wydawane decyzje mają charakter wiążący i podlegają kontroli sądowej[57].

Instytucja pośredniego dostępu stanowi swoistą przeciwwagę dla przewidzianych w prawie ograniczeń praw podmiotowych wskazanych w dyrektywie[58]. Prawodawca unijny dostrzegł tym samym konieczność wprowadzenia mechanizmu umożliwiającego dostęp do informacji na temat przetwarzania danych osobowych, obejmującego m.in. treść danych,

[57] Wyrok Trybunału z 16.11.2023 r. w sprawie C-333/22 Ligue des droits humains ASBL i BA przeciwko Organe de contrôle de l'information policière, EU:C:2023:874.
[58] Art. 13 ust. 3, art. 15 ust. 3, art. 16 ust. 4.

ich źródła oraz podstawę prawną przetwarzania. Instytucja pośredniego dostępu do danych, zagwarantowana w art. 17 dyrektywy (UE) 2016/680, jest gwarancją realizacji prawa do informacji, prawa do sprostowania lub usunięcia danych czy prawa dostępu nie bezpośrednio (jak na gruncie rozporządzenia 2016/679), lecz również za pośrednictwem niezależnego organu nadzorczego. Zagadnienie dotyczące **praw podmiotu danych wykonywanych za pośrednictwem organu nadzorczego** jest przedmiotem pogłębionej analizy zarówno Prezesa Urzędu Ochrony Danych Osobowych, jak i działań na forum europejskich innych organów ochrony danych i instytucji UE.

W ocenie Prezesa UODO brak implementowania tego przepisu prawa unijnego w prawie polskim, tj. w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, budzi zasadnicze wątpliwości. Prezes UODO w toku prac w 2025 r. nad ewaluacją dyrektywy (UE) 2016/680 oraz prac nad projektem wytycznych Europejskiej Rady Ochrony Danych (dalej jako EROD) w sprawie prawa dostępu zgłaszał uwagi w tym przedmiocie. Zaakcentował, że prawo podmiotu danych do wykonywania jego praw za pośrednictwem organu nadzorczego – wynikające z art. 17 dyrektywy (UE) 2016/680 – oraz prawo do wniesienia skargi do organu nadzorczego w na podstawie art. 52 tej dyrektywy (art. 50 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości) – to odrębne prawa, których nie należy utożsamiać. Prezes UODO od początku wskazywał, że jest to odrębny instrument, który powinien być realizowany za pośrednictwem innych procedur. Artykuł 17 ust. 1-3 dyrektywy 2016/680 przewiduje mechanizm, w którym w przypadku ograniczenia prawa jednostki dostępu do dotyczących jej danych osoba ta może wykonywać swoje uprawnienia za pośrednictwem „właściwego organu nadzorczego”[59]. Skarga, o której mowa w art. 50 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, ma inny charakter niż uprawnienie wynikające z art. 17 dyrektywy 2016/680. Zgodnie z art. 50 ust. 1 powołanej ustawy uprawnienie do złożenia skargi przysługuje wówczas, gdy dane osobowe danego podmiotu są przetwarzane niezgodnie z prawem.

Prezes UODO prowadził w tej materii również korespondencję z Rzecznikiem Praw Obywatelskich, który podzielił opinię co do braku implementacji art. 17 dyrektywy (UE) 2016/680 w prawie krajowym (w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości)[60], co jest sprzeczne nie tylko z orzecznictwem Trybunału Sprawiedliwości UE (TSUE), ale również ze zobowiązaniami wynikającymi z Karty Praw Podstawowych UE.

Problem prawidłowej implementacji dyrektywy (UE) 2016/680 do polskiego porządku prawnego mimo starań Prezesa UODO, o czym była już mowa na wstępie niniejszego pisma[61] w sposób szczególny uwidoczniła prowadzona w 2025 r. ewaluacja stosowania dyrektywy (UE) 2016/680 przez państwa członkowskie UE. Strona polska w odniesieniu do prawa z art. 17 dyrektywy (UE) 2016/680 zgłosiła brak wdrożenia do ustawodawstwa krajowego tego przepisu.

---

[59] Dostępu do informacji, sprawdzania ich prawidłowości oraz nadzoru nad procesem ich przetwarzania.
[60] Pismo Prezesa UODO z 14 sierpnia 2025 r., sygn. DPNT.051.11.2025.
[61] Zob. przypis 4, 5 i 53.

Problem prawa dostępu do danych realizowanego pośrednio przez organ nadzorczy na rzecz podmiotu danych był także przedmiotem analizy podczas oceny przeprowadzonej w 2024 r. w zakresie stosowania przez Rzeczpospolitą Polską dorobku Schengen. Komisja Europejska wraz z ekspertami państw członkowskich **stwierdziła brak zapewnienia pośredniego dostępu do danych w systemach SIS i VIS** za pośrednictwem Prezesa Urzędu Ochrony Danych Osobowych w przypadkach odmowy realizacji praw osób, których dane dotyczą.

W konsekwencji Polska została zobowiązana (zalecenie priorytetowe) do zapewnienia, aby osoby, których dane dotyczą, mogły wykonywać swoje prawa: dostępu, sprostowania i usunięcia danych osobowych w Systemie Informacyjnym Schengen za pośrednictwem Prezesa Urzędu Ochrony Danych Osobowych w przypadku odmowy realizacji tych praw przez właściwy organ – zgodnie z art. 53 ust. 3 rozporządzenia (UE) 2018/1861[62], art. 67 ust. 3 rozporządzenia (UE) 2018/1862 oraz art. 19 rozporządzenia (UE) 2018/1860[63], a także w Wizowym Systemie Informacyjnym — zgodnie z art. 38 ust. 7 rozporządzenia (UE) 767/2008.

Państwa członkowskie powinny zapewnić jednostce możliwość zwrócenia się do organu nadzorczego o kontrolę legalności przetwarzania, a także zapewnić skuteczny środek ochrony prawnej w razie odmowy realizacji praw dostępu, sprostowania czy usunięcia danych przez administratora – odnosi się do tego jednoznacznie motyw 48 preambuły dyrektywy (UE) 2016/680.

Stanowisko Prezesa UODO odnośnie do wykonywania przez organ nadzorczy uprawnień w ramach art. 17 dyrektywy (UE) 2016/680 jest zgodne z prezentowanym przez Trybunał Sprawiedliwości UE, który w wyroku z 16 listopada 2023 r. w sprawie C-333/22 stwierdził, że: „Przepisy te [art. 46 ust. 1 lit. g) i art. 47 ust. 1 i 2 dyrektywy 2016/680] należy interpretować w świetle wyrażonego w art. 8 ust. 3 karty [KPP] wymogu, zgodnie z którym przestrzeganie określonych w ust. 1 i 2 tego artykułu zasad dotyczących prawa każdej osoby do ochrony danych osobowych powinno »podlega[ć] kontroli niezależnego organu«, a w szczególności wyrażonego w art. 8 ust. 2 zdanie drugie karty wymogu, zgodnie z którym »[k]ażdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania«. Jak bowiem potwierdza to orzecznictwo, ustanowienie niezależnego organu nadzorczego ma na celu zapewnienie skuteczności i wiarygodności kontroli przestrzegania przepisów w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i powinno być interpretowane w świetle tego celu […]” (teza 47 wyroku). „W związku z tym, gdy taki organ nadzorczy działa w celu zapewnienia wykonywania praw osoby, której dane dotyczą, na podstawie art. 17 dyrektywy 2016/680, jego zadanie wpisuje się w pełni w dokonane w prawie pierwotnym Unii określenie jego roli, ponieważ określenie to pociąga za sobą w szczególności kontrolę przestrzegania prawa dostępu przysługującego osobie, której dane dotyczą, oraz jej prawa

[62] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006, Dz. Urz. L 312 z 7.12.2018, s. 14.

[63] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich.

do sprostowania. Wynika z tego, że przy wykonywaniu tego szczególnego zadania, podobnie jak w ramach wszelkich innych zadań, organ nadzorczy powinien być w stanie wykonywać uprawnienia powierzone mu na mocy art. 47 tej dyrektywy, działając w pełni niezależnie – zgodnie z kartą i jak to stanowi motyw 75 wspomnianej dyrektywy" (teza 48 wyroku). Jak można zatem zauważyć, opierając się na dyspozycji art. 46 ust. 1 lit. g) w zw. z art. 17 dyrektywy 2016/680, Trybunał Sprawiedliwości Unii Europejskiej rozumie uprawnienia organu nadzorczego szeroko, jako obejmujące kontrolę przestrzegania przepisów o ochronie danych osobowych, nie zaś jedynie kontrolę prawa dostępu do zebranych danych i prawa do dokonania ich sprostowania.

Analiza art. 17 dyrektywy (UE) 2016/680 w kontekście wskazanego wyżej wyroku TSUE w sprawie C-333/22 prowadzi do wniosku, że wskazanym przepisem dyrektywy (UE) 2016/680 prawodawca zobowiązuje organ nadzorczy do tego, by poinformował osobę, której dane dotyczą, po pierwsze: o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub przeglądów przetwarzania jej danych osobowych oraz, po drugie: o przysługującym tej osobie prawie do wniesienia środka prawnego do sądu w sytuacji, gdy taka informacja nie pozwala na kontrolę sądową działania organu nadzorczego i dokonanych przez niego ocen, przy uwzględnieniu przetwarzanych danych i obowiązków administratora. Tym samym art. 17 dyrektywy 2016/680 ustanawia szczególny mechanizm realizacji praw jednostki w sektorze organów zajmujących się zwalczaniem przestępczości. Zgodnie z jej ust. 1 państwa członkowskie zapewniają, aby osoba, której dane dotyczą, mogła wykonywać prawa przysługujące jej na mocy art. 13 i 16 za pośrednictwem właściwego organu nadzorczego, jeżeli prawa te zostały ograniczone przez administratora na podstawie art. 13 ust. 3, art. 15 ust. 3 lub art. 16 ust. 4. Mocą art. 17 ust. 2 dyrektywy 2016/680 nałożony został na administratora obowiązek informacyjny: musi on powiadomić osobę, której dane dotyczą, że jej prawa mogą być wykonywane za pośrednictwem organu nadzorczego. Obowiązek ten jest niezmiernie istotny z uwagi na fakt, iż w praktyce jednostki często nie wiedzą o samym fakcie przetwarzania ich danych – zwłaszcza na etapie przygotowawczym postępowania karnego – a więc także o ograniczeniu przysługujących im praw. Celem tej regulacji jest zatem zapewnienie jednostce dodatkowej gwarancji jej praw, równoważące ograniczenia w sytuacji, gdy administrator – najczęściej organ ścigania – odwołuje się do przesłanek ograniczenia praw przewidzianych w tej dyrektywie, w szczególności w sytuacjach objętych tajemnicą postępowania przygotowawczego lub śledztwa bądź też ze względu na konieczność zapewnienia bezpieczeństwa publicznego.

Nie wdając się w zagadnienia implementacji tego przepisu w poszczególnych państwach członkowskich[64], wskazać należy, że brak podstawy ustawowej w Polsce oznacza, że mechanizm pośredniego dostępu nie istnieje obecnie w ogóle. **Ustawodawca w ustawie z dnia 14 grudnia 2018 r.** o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości **nie przewidział żadnych**

[64] Przykładowo: we Francji problemem pozostaje ograniczony dostęp organu nadzorczego (Commission Nationale de l'Informatique et des Libertés; CNIL) do policyjnych baz danych – organ nadzorczy często nie ma możliwości realnej oceny niezbędności i proporcjonalności operacji przetwarzania, co powoduje, że informacja zwrotna przekazywana jednostce ma charakter czysto deklaratywny („kontrolę przeprowadzono"). W Niemczech z kolei na przeszkodzie skuteczności stoją rozproszone regulacje federalne i krajowe oraz szerokie klauzule poufności, które sprowadzają weryfikację organów nadzorczych do minimum formalnego.

przepisów odpowiadających art. 17 dyrektywy 2016/680. Artykuł 17 dyrektywy (UE) 2016/680 nakłada na państwa członkowskie obowiązek ustanowienia odpowiednich regulacji prawnych umożliwiających realizację tego prawa. W tym zakresie należy przypomnieć, że zgodnie z art. 288 TFUE dyrektywa wiąże każde państwo członkowskie, do którego jest kierowana w odniesieniu do rezultatu, który ma być osiągnięty, pozostawiając jednak organom krajowym swobodę wyboru formy i środków.

W rezultacie regulacje przyjęte w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości nie zapewniają transpozycji art. 17 dyrektywy (UE) 2016/680, co pozbawia jednostkę możliwości wystąpienia do Prezesa UODO – który zgodnie z art. 34 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych jest organem nadzorczym w rozumieniu dyrektywy (UE) 2016/680 – z wnioskiem o zweryfikowanie legalności przetwarzania jej danych w razie odmowy informacji, sprostowania czy usunięcia danych przez organy ścigania. Realnie rzecz biorąc kompetencje Prezesa UODO skupiają się przede wszystkim na obszarze objętym ogólnym rozporządzeniem o ochronie danych, natomiast w zakresie przetwarzania danych w celach zapobiegania i zwalczania przestępczości jego rola została znacząco ograniczona chociażby z uwagi na wyłączenia, o których mowa w art. 3 powołanej ustawy. Skutkuje to nie tylko naruszeniem zobowiązań wynikających z prawa Unii Europejskiej, lecz również osłabia konstytucyjne gwarancje ochrony danych osobowych wskazane w art. 51 Konstytucji RP.

Niezbędne jest zatem przeprowadzenie pogłębionych analiz opisanego problemu i podjęcie działań legislacyjnych zmierzających do nowelizacji ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości poprzez wprowadzenie przepisów implementujących art. 17 dyrektywy (UE) 2016/680 oraz jednoznaczne określenie kompetencji Prezesa UODO w zakresie realizacji prawa pośredniego dostępu. Wpłynie to nie tylko na usunięcie stanu niezgodności z dyrektywą oraz Kartą Praw Podstawowych UE, lecz także zapewni osobom fizycznym odpowiedni poziom ochrony odpowiadający standardom unijnym i międzynarodowym.

Niewątpliwie podjęcie działań legislacyjnych w obszarze wyżej opisanych wątpliwości przyczyni się do zapewnienia zgodności przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z przepisami dyrektywy, co ma istotne znaczenie z punktu widzenia zapewnienia jej pełnej implementacji w prawie krajowym. Brak prawidłowej implementacji dyrektywy 2016/680 to jednak nie tylko zagadnienie formalno-prawne. Brak ten jest realnym **zagrożeniem dla praw osób, których dane dotyczą, ich prywatności oraz skuteczności działania organów państwa odpowiedzialnych za bezpieczeństwo publiczne.** Opisane powyżej luki przepisów krajowych regulujących przetwarzanie danych osobowych przez organy ścigania i inne właściwe organy prowadzą do **osłabienia standardów ochrony praw jednostki**. W szczególności istotną lukę stanowi brak skutecznych mechanizmów kontroli nad procesem przetwarzania danych, w tym realnego dostępu do informacji o przetwarzaniu danych, możliwości ich sprostowania lub usunięcia, a także efektywnych środków ochrony prawnej. Z perspektywy bezpieczeństwa publicznego i interesu państwa brak pełnej implementacji dyrektywy stanowi również istotne zagrożenie dla **efektywnej**

współpracy międzynarodowej, w szczególności w ramach Unii Europejskiej. Luki w tym zakresie prowadzą do fragmentaryzacji poziomu ochrony, a co więcej osłabiają skuteczność wspólnych polityk UE w obszarze bezpieczeństwa, zwalczania przestępczości i ochrony granic.

Mając na uwadze powyższe, uprzejmie proszę Panów Ministrów o odniesienie się do tego wystąpienia na piśmie, **w terminie 30 dni** od daty jego otrzymania.

W przypadku podjęcia prac legislacyjnych w związku z przedstawionym powyżej zagadnieniami Prezes UODO deklaruje swoje wsparcie eksperckie celem wypracowania rozwiązań uwzględniających przepisy o ochronie danych osobowych.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

Do wiadomości:

Pan
Radosław Sikorski
Wiceprezes Rady Ministrów
Minister Spraw Zagranicznych

Pan
dr hab. Marcin Wiącek
Rzecznik Praw Obywatelskich