



Warszawa, dnia 23 września 2026 r.

OPINIA

Komisji Kodyfikacyjnej Ustroju Sądownictwa i Prokuratury dotycząca wniosku Prezesa Urzędu Ochrony Danych Osobowych 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 przestępczości¹ w celu zapewnienia prawidłowej implementacji w polskim systemie prawa dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680²

I. Wprowadzenie

W dniu 2 czerwca 2026 r. do Komisji Kodyfikacyjnej Ustroju Sądownictwa i Prokuratury³ wpłynęło przekazane przez Ministra Sprawiedliwości wystąpienie Prezesa Urzędu Ochrony Danych Osobowych⁴ z dnia 16 marca 2026 r.⁵, adresowane również do Ministra Spraw Wewnętrznych i Administracji z wnioskiem o podjęcie pogłębionej analizy i prac legislacyjnych prowadzących do zmiany przepisów UDODO w celu zapewnienia prawidłowej implementacji w polskim systemie prawa Dyrektywy w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającej decyzję ramową Rady 2008/977/WSiSW⁶.

Przekazując powyższe wystąpienie, Minister Sprawiedliwości zwrócił się do Komisji o wydanie opinii w kontekście uwag podniesionych przez PUODO co do potrzeby zainicjowania i podjęcia prac w zakresie postulowanej przez PUODO zmiany UDODO, a ewentualnie także innych wymienionych w przedmiotowym piśmie aktów prawnych, w celu zagwarantowania pełnej i prawidłowej implementacji Dyrektywy.

¹ T.j. Dz. U. z 2023 r., poz. 1206, dalej: UDODO.

² 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, Dz. Urz. UE L 119 z 04.05.2016, tzw. „dyrektywa o ochronie danych w sprawach karnych” lub „dyrektywa policyjna”, dalej: Dyrektywa.

³ Dalej: Komisja.

⁴ Dalej: PUODO.

⁵ DPNT.413.28.2025, dalej: wystąpienie.

⁶ Decyzja ramowa z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U.UE.L.2008.350.60.

II. Charakter uwag zgłoszonych przez PUODO

1. Uwagi o charakterze systemowym

W treści wystąpienia PUODO dominujący charakter miały uwagi o charakterze systemowym, odnoszące się do przyjętej w 2018 r. koncepcji wdrożenia Dyrektywy do polskiego systemu prawnego w przepisach UDODO.

Zdaniem PUODO, w toku procesu legislacyjnego, a w szczególności podczas prowadzonych konsultacji, sygnalizował on nieprawidłowości związane z niewłaściwą implementacją, a następnie informował o nich w trakcie obowiązywania UDODO, jednak nie spotkało się to z odpowiednią reakcją ustawodawcy. Tymczasem jego zastrzeżenia były uzasadnione, co znalazło swoje potwierdzenie w procesie ewaluacji Dyrektywy⁷. Obowiązujący kształt UDODO nie zapewnia pełnych gwarancji ochrony praw osób, których dane są przetwarzane, a przepisy procedury karnej nie odzwierciedlają w pełni standardów ochrony danych wynikających z Dyrektywy.

Zdaniem PUODO konieczne jest pełne dostosowanie polskiego prawa do wymogów Dyrektywy, albowiem dotychczasowe regulacje:

- nie zapewniają pełnej ochrony danych osobowych w postępowaniach karnych;
- nie gwarantują skutecznego i niezależnego nadzoru nad sądami i prokuraturą z uwagi na brak niezależnego systemu (organu nadzoru);
- nie zapewniają osobom, których dane są przetwarzane, praw wymaganych przez prawo UE (art. 18 Dyrektywy) w postępowaniu przygotowawczym i sądowym w zakresie spraw karnych.

Formułując szczegółowe zarzuty, PUODO wskazał przede wszystkim na brzmienie art. 3 pkt 1 UDODO zawierającego wyłączenie spoza zakresu ochrony ustawy i implementowanej Dyrektywy przetwarzania danych osobowych znajdujących się w aktach spraw lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie:

- ustawy z dnia 6 czerwca 1997 r. - Kodeks karny wykonawczy⁸,
- ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego⁹,

⁷ 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.

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.

⁸ T.j. Dz. U. z 2025 r., poz. 911, dalej: k.k.w.

⁹ T.j. Dz. U. z 2026 r., poz. 490, dalej: k.p.k.

- ustawy z dnia 10 września 1999 r. - Kodeks karny skarbowy¹⁰,
- ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia¹¹,
- ustawy z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób¹²,
- ustawy z dnia 28 stycznia 2016 r. - Prawo o prokuraturze¹³,
- ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich¹⁴.

W rezultacie zakres możliwej kontroli powołanego organu uległ istotnemu zawężeniu i to pomimo tego, że Dyrektywa w sposób jednoznaczny określa zakres stosowania jej przepisów do przetwarzania danych osobowych przez właściwe organy 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, a zgodnie z art. 2 ust 2 należy ją stosować do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Według PUODO istnieje poważna niezgodność systemowa pomiędzy celem wprowadzenia Dyrektywy, a regulacją art. 3 UDODO.

Przyjęte założenie, że dane osobowe zawarte w aktach prowadzonych spraw oraz dane osobowe przetwarzane w toku czynności lub w urządzeniach ewidencyjnych prowadzonych w oparciu o przepisy prawa wynikające z ustaw wymienionych w art. 3 pkt 1 UDODO są chronione na podstawie tych przepisów, nie gwarantuje ochrony zgodnej z ratio legis Dyrektywy.

W ocenie PUODO art. 18 Dyrektywy nie daje podstaw do całościowego wyłączenia jej stosowania¹⁵. W Dyrektywie prawodawca nie przewidział podstaw do wyłączania stosowania przepisów o bezpieczeństwie danych osobowych w zakresie wskazanym w art. 3 pkt 1 UDODO. Tymczasem w świetle artykułu 18 Dyrektywy oraz jej motywu 20¹⁶, które stanowią podstawę do sformułowania wyłączenia, należy na nowo rozważyć przyjęcie w krajowym porządku prawnym innych przepisów lub uzupełnienie przepisów k.p.k. oraz pozostałych aktów prawnych, do których ustawodawca odwołał się w art. 3 pkt 1 UDODO, w celu zapewnienia stosownych gwarancji wynikających z Dyrektywy. Regulacje takie

¹⁰ T.j. Dz. U. z 2025 r., poz. 633, dalej: k.k.s.

¹¹ T.j. Dz. U. z 2025 r., poz. 860, dalej: k.p.o.w.

¹² T.j. Dz. U. z 2022 r., poz. 1689.

¹³ T.j. Dz. U. z 2026 r., poz. 810, dalej: UPOP.

¹⁴ T.j. Dz. U. z 2026 r., poz. 163.

¹⁵ Art. 18 Dyrektywy stanowi, że państwa członkowskie mogą zapewnić, by wykonywanie praw, o których mowa w art. 13, 14 i 16, odbywało się zgodnie z prawem państwa członkowskiego, jeżeli dane osobowe znajdują się w orzeczeniu sądu, protokole lub aktach sprawy przetwarzanych w toku postępowania przygotowawczego lub sądowego w sprawie karnej.

¹⁶ Według motywu (20) 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 karnym.

w sposób jasny i niebudzący wątpliwości określać powinny uprawnienia uczestników procedury karnej zgodnie z wymogami Dyrektywy. W obecnym stanie prawnym uprawnienia te mogą być jedynie pośrednio i nie w pełnym zakresie wywodzone z innych przepisów k.p.k., w sytuacji, gdy przetwarzanie to następuje w granicach wyznaczonych w art. 2 Dyrektywy.

PUODO zakwestionował podstawę merytoryczną wyłączenia określonego w art. 3 pkt 1 UDODO, która opierała się na interpretacji definicji „zbioru danych”¹⁷, szczególnie w aspekcie istniejących i rozwijanych systemów teleinformatycznych. W przypadku wyodrębnienia akt sprawy lub w sytuacji połączenia akt z systemem teleinformatycznym umożliwiającym dostęp do danych osobowych zawartych w takich aktach wystarczające dla zaistnienia zbioru jest występowanie jakiegokolwiek kryterium porządkującego akta, które pozwoli na dostęp do danych osobowych określonej osoby. Jeśli akta są połączone z systemem ewidencyjnym zapewniającym dostęp do danych osobowych zawartych w aktach sprawy dotyczących jakiegokolwiek osoby (np. uczestnika postępowania), to takie dane osobowe w aktach stanowią co najmniej część zbioru.

2. Nadzór nad przetwarzaniem danych osobowych przez sądy

PUODO zwrócił uwagę na brak zgodnego z Dyrektywą uregulowania zagadnień związanych z nadzorem nad przetwarzaniem danych w ustawie z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych¹⁸. Przepis art. 175dd tej ustawy, który określa właściwość oraz zakres uprawnień organów nadzorczych w tym zakresie, w istocie wyłącza polskie sądownictwo spod norm dotyczących ochrony danych osobowych przewidzianych Dyrektywą. Obecnie nadzór ten sprawowany jest głównie przez organy funkcjonujące wewnątrz struktury sądownictwa. W wystąpieniu wskazano, że:

- model nie spełnia w pełni wymogu niezależnego nadzoru w rozumieniu art. 41–45 Dyrektywy,
- organy nadzorcze sądów nie posiadają wszystkich kompetencji przewidzianych przez prawo UE,
- sądy w praktyce nie stosują przepisów UDODO lub nie identyfikują obszarów, w których powinny je stosować,

Jak podniósł PUODO, 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 w sprawach sądowych i nie powinien on mieć zastosowania do innych czynności, w których sędziowie mogą brać udział zgodnie z prawem państwa członkowskiego.

¹⁷ Art. 3 pkt 6 Dyrektywy przewiduje, że „zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

¹⁸ Dz.U. z 2024 r. poz. 334, dalej jako PUSP.

Szczególne zastrzeżenia wzbudził brak wyposażenia organów nadzorczych właściwych dla sądów w pełni kompetencji, co prowadzi do braku jednolitego standardu nadzoru i może ograniczać ochronę praw jednostek w zakresie przetwarzania danych w wymiarze sprawiedliwości. Nie jest to pożądane i nie zapewnia skutecznej ochrony praw podstawowych. W tym aspekcie PUODO zasugerował stworzenie organu specjalnego, jednak nie przedstawił propozycji konkretnych rozwiązań.

W konkluzji podkreślono, że na mocy art. 1 pkt 3 UDODO wyłączony został nadzór nad sądami. 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 RODO na mocy art. 2 ust. 2 pkt lit. d tego rozporządzenia. W konsekwencji, jedynymi przepisami regulującymi sposób przetwarzania danych w procesach objętych materią UDODO są przepisy właściwych procedur (kodeksów, ustaw), które nie uwzględniają wymogów ochrony danych osobowych na poziomie wymaganym przez Dyrektywę.

W związku z tym PUODO zasugerował utworzenie w ramach sądownictwa (wymiaru sprawiedliwości) niezależnego organu, który realizowałby czynności nadzorcze nad przetwarzaniem danych osobowych i chroniłby indywidualne prawa jednostki.

3. Nadzór nad przetwarzaniem danych osobowych przez prokuraturę

PUODO zakwestionował także możliwość sprawowania przez organy prokuratury nadzoru nad ochroną danych osobowych pomimo tego, że na podstawie art. 45 ust. 2 zd. drugiej Dyrektywy prawodawca europejski upoważnił państwa członkowskie do ewentualnego ustanowienia innego, niż organ w rozumieniu art. 41 Dyrektywy, organu nadzoru nad operacjami przetwarzania danych osobowych, dokonywanymi przez inne niż sądy niezależne organy wymiaru sprawiedliwości. W tym kontekście PUODO zakwestionował wyrażone w motywie 80 zdanie trzecie *in fine* Dyrektywy stanowisko prawodawcy unijnego, upoważniające państwa członkowskie do 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.

PUODO wskazał, że prokuratura i jej jednostki organizacyjne nie mogą zostać uznane za niezależne organy wymiaru sprawiedliwości ze względu na model funkcjonowania prokuratury w Rzeczypospolitej Polskiej, w tym hierarchiczne podporządkowanie i realny (faktyczny) brak niezależności.

Stosownie do art. 191a § 1 UPOP nadzór nad przetwarzaniem danych osobowych w ramach realizacji zadań określonych w art. 2 tej ustawy sprawują kierownicy jednostek wyższego szczebla. Prokuratura nie jest organem niezależnym w rozumieniu Dyrektywy. W zakresie danych osobowych

przetwarzanych przez powszechne jednostki organizacyjne prokuratury w ramach realizacji zadań określonych w art. 2 UPOP, 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 UDODO, związane z zapobieganiem i zwalczaniem przestępczości, są wykonywane przez organy nadzoru, o których mowa w art. 191a § 1 UPOP, 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 UPOP – przez organ nadzoru, jakim jest Prokurator Krajowy. Zamiast decyzji administracyjnej, o której mowa w art. 8 ust. 2 UDODO organ nadzoru w zakresie przetwarzania danych osobowych wydaje polecenie służbowe. Oznacza to, że sprawowanie nadzoru nad przetwarzaniem tych danych do celów, o których mowa w art. 1 Dyrektywy, jest realizowane w ramach tej samej struktury organizacyjnej, w której odbywa się przetwarzanie.

Zdaniem PUODO zasadnicze zastrzeżenia dotyczą sprawowania nadzoru nad ochroną danych w prokuraturze, która nie jest organem niezależnym, co nie spełnia wymogu określonego w Dyrektywie. W związku z tym PUODO postuluje:

- uchylenie przepisów powierzających nadzór organom prokuratury,
- przekazanie nadzoru niezależnemu organowi, co w konkretnej sytuacji sprowadza się do przekazania nadzoru PUODO.

III. Stan prawny i przebieg procesu ewaluacji

1. Rys historyczny

W związku z wejściem w życie RODO oraz Dyrektywy Rzeczpospolita Polska została zobowiązana do przyjęcia i opublikowania do dnia 6 maja 2018 r. przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania Dyrektywy. UDODO, mająca w założeniu ustawodawcy wdrożyć do polskiego porządku prawnego Dyrektywę, została uchwalona już po wskazanym terminie, co było związane z tym, że dopiero w dniu 30 października 2018 r. wpłynął do Sejmu RP rządowy projekt ustawy¹⁹.

Na etapie prac nad projektem pojawiały się uwagi co do prawidłowości zakresu implementacji Dyrektywy w związku z opinią Ministra Spraw Zagranicznych i podniesionym zarzutem niezgodności art. 3 pkt 1 projektu ustawy z art. 2 ust. 2 w zw. z art. 3 pkt 6 Dyrektywy oraz art. 3 pkt 2 projektu ustawy z art. 2 ust. 3 lit. a Dyrektywy, szczególnie w zakresie Centralnego Biura Antykorupcyjnego. Biuro Analiz Sejmowych wydając opinię z dnia 28 listopada 2018 r. uznało powyższe zarzuty za trafne.

Jednocześnie Biuro Analiz Sejmowych w dalszej części opinii wskazało m.in., że: *w myśl art. 1 pkt 3 projektu ustawy ma ona określać sposób prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez właściwe organy w celach, o których mowa w pkt 1, z wyłączeniem danych osobowych*

¹⁹<https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?id=35EDF804B677502AC125833E00510EA0>.

przetwarzanych przez prokuraturę i sądy. W ocenie skutków regulacji zawartej w uzasadnieniu do projektu ustawy wyłączenie z jej zakresu danych osobowych przetwarzanych przez prokuraturę uzasadniono, przywołując motyw 80 preambuły Dyrektywy. W motywie tym określono m.in., że „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. W świetle przytoczonego postanowienia wątpliwości budzi możliwość uznania prokuratury za „niezależny organ wymiaru sprawiedliwości” w rozumieniu Dyrektywy. W myśl art. 175 ust. 1 Konstytucji RP wymiar sprawiedliwości w Rzeczypospolitej Polskiej sprawują Sąd Najwyższy, sądy powszechne, sądy administracyjne oraz sądy wojskowe. Zgodnie z art. 2 UPOP prokuratura wykonuje zadania w zakresie ścigania przestępstw oraz stoi na straży praworządności, natomiast przymiot niezależności został w tej ustawie przypisany (w pewnym zakresie) prokuratorom, a nie instytucji.

W konsekwencji wskazano, że może to prowadzić do przyjęcia, iż art. 1 pkt 3 projektu ustawy w zakresie, w którym dotyczy prokuratury, pozostaje niezgodny z Dyrektywą²⁰.

Pomimo istniejących zastrzeżeń, także na etapie prac w Senacie RP ustawa została uchwalona bez zmian, a zatem ustawodawca podtrzymał stanowisko zawarte w uzasadnieniu projektu, że wskazane podstawy prawne, o których mowa w przytoczonej opinii, dają podstawy do tak daleko idących wyłączeń przedmiotowych i podmiotowych w zakresie stosowania ustawy.

Warto w tym miejscu przedstawić szczegółową argumentację z uzasadnienia projektu (druk 2989) w którym projektodawca przedstawiał motywy tej decyzji: (...) *Definicja zbioru danych, zawarta w art. 3 pkt 6 dyrektywy, jest tożsama z definicją zawartą uprzednio w art. 2 lit c. dyrektywy 95/46/WE oraz art. 7 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – co oznacza, że do zbioru danych w dalszym ciągu mają zastosowanie koncepcje wypracowane przez doktrynę i orzecznictwo pod rządami poprzedniej dyrektywy. W świetle doktryny i orzecznictwa, zbiór danych, zdefiniowany w art. 3 pkt 6 dyrektywy, powinien zatem spełniać następujące kryteria:*

- 1) musi to być zestaw danych osobowych;*
- 2) dane osobowe w tym zbiorze muszą być uporządkowane w taki sposób, aby można było odszukać żadaną informację bez potrzeby przeszukiwania całego zbioru;*
- 3) dane muszą być uporządkowane według co najmniej dwóch określonych kryteriów, przy czym kryteria te powinny się odnosić do osób fizycznych, a więc zbiór ma być uporządkowany w taki sposób, aby można było odszukać dane osobowe bez potrzeby przeszukiwania całego zbioru.*

²⁰<https://orka.sejm.gov.pl/rexdomk8.nsf/0/E2F8769F9A45643AC125834E002F27B8/%24File/i2765-18.docx>.

Oznacza to, że dyrektywy nie stosuje się do akt, takich jak akta postępowania karnego. Akta są wyłączone spod definicji zbioru danych osobowych z trzech powodów:

- 1) nie są zbiorem danych osobowych, ponieważ gromadzi się różnego rodzaju informacje i materiały dowodowe, na podstawie których organ prowadzący postępowanie i wydający rozstrzygnięcie kształtuje swoje stanowisko co do faktu popełnienia czynu zabronionego, sprawcy tego czynu oraz odpowiedzialności karnej;
- 2) nie są uporządkowane w rozumieniu dyrektywy, ponieważ ani nie stanowią one jednorodnego zestawu, ani nie można w nich wyszukać według określonych kryteriów danych osobowych zawartych w materiale dowodowym;
- 3) kryteria porządkujące akta nie dotyczą danych osobowych, gdyż te, według których organizowane są akta, odnoszą się nie do danych osobowych, ale do kolejności przeprowadzania dowodów lub wątków postępowania dotyczących zwykle odrębnych czynów zabronionych,
- 4) kryteria porządkujące akta nie dotyczą danych osobowych.

Dane zawarte w zbiorze muszą być danymi o charakterze osobowym. Tymczasem w aktach spraw i czynności prowadzonych na podstawie ustaw wskazanych w art. 3 pkt 1 gromadzi się różnego rodzaju informacje i materiały dowodowe, na podstawie których organ prowadzący postępowanie i wydający rozstrzygnięcie kształtuje swoje stanowisko co do faktu popełnienia czynu zabronionego, sprawcy tego czynu oraz odpowiedzialności karnej. Gromadzone i dokumentowane w aktach spraw i czynności dowody nie tworzą zbioru danych. Sam fakt, że dokument, pośród innych informacji, zawiera między innymi dane osobowe nie sprawia, że dokument taki staje się zestawem danych osobowych, a tym bardziej zbiorem danych. Trybunał Sprawiedliwości w wyroku z dnia 17 lipca 2014 r. w połączonych sprawach C 141/12 i C 372/12 wskazał, że dokumenty, w których zawarte są dane osobowe, na przykład dotycząca danej osoby analiza prawna, nie nabierają przez to charakteru „danych osobowych” w rozumieniu prawa unijnego. Nie stanowią zatem danych osobowych, ani tym bardziej zestawu takich danych, dokumenty wchodzące w skład akt, np. protokół przesłuchania czy wyrok z uzasadnieniem. Co za tym idzie, zbiór gromadzący takie dokumenty nie jest zbiorem danych osobowych”.

Stanowisko to zostało poddane krytyce w literaturze. M. Kusak oraz P. Wiliński podkreślają, że wskazana interpretacja (...) jest niezgodna zarówno z orzecznictwem TSUE, jak i wprowadza niezasadne rozwarstwienie pojęcia zbioru danych w kontekście akt sądowych, pomimo identycznej definicji tego terminu na gruncie RODO, dyrektywy 2016/680 oraz ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości²¹.

²¹ M.Kusak, P.Wiliński, *Ustawa krajowa* [w:] M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020, s. 29-30.

Autorzy podzielają pogląd dotyczący możliwości bezpośredniego stosowania Dyrektywy do przetwarzania danych osobowych ujętych w aktach postępowania karnego, a nawet skierowania w tym zakresie pytania prejudycjalnego. Wskazują także na wadliwe podmiotowe (a nie przedmiotowe) wyłączenie w art. 3 pkt 2 UODO danych przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego. Nie negując możliwości i zasadności takiego wyłączenia wskazują na użycie pojęcia bezpieczeństwa narodowego, które nie jest jednoznacznie definiowane oraz podnoszą, że instytucje te wykonują także zadania, przy których przetwarzają dane, a taki sposób sformułowania przepisu budzi wątpliwości co do zakresu wyłączenia danych spod regulacji.

2. Ewaluacja

W 2021 r. European Data Protection Board (EDPB) przygotowała formalny wkład do ewaluacji prowadzonej przez Komisję Europejską. EDPB podkreśliła, że państwa członkowskie dopiero zakończyły lub kończyły proces implementacji Dyrektywy, dlatego było jeszcze za wcześnie na ocenę jej skuteczności. Jednocześnie zwrócono uwagę na potrzebę zapewnienia pełnej zgodności krajowych ustaw implementacyjnych z Dyrektywą oraz na utrzymujące się różnice między państwami członkowskimi.

EDPB nie opublikowała w 2021 r. odrębnej krytyki polskiej ustawy i wskazywała ogólnie, że występują problemy z pełną i jednolitą transpozycją Dyrektywy w państwach członkowskich, zalecając dalsze monitorowanie krajowych rozwiązań przed wyciąganiem ostatecznych wniosków.

W dniu 25 lipca 2022 r. Komisja Europejska przedstawiła pierwszy raport ewaluacyjny, zgodnie z art. 62 ust. 1 Dyrektywy²². Przeanalizowano w nim poziom transpozycji Dyrektywy w państwach członkowskich UE, np. w odniesieniu do zakresu działań wymiaru sprawiedliwości, zarządzeń i uprawnień organów nadzorujących ochronę danych, środków odwoławczych i praw osób, których dane dotyczą. Wskazano, że Dyrektywa została zasadniczo implementowana w sposób zadowalający, niemniej jednak zidentyfikowano kilka problemów.

W ocenie Komisji Dyrektywa zaowocowała wyższym poziomem świadomości i uwagi na temat ochrony danych osobowych przez właściwe organy krajowe, zwłaszcza w odniesieniu do bezpieczeństwa ich przetwarzania. Odnosząc się do dalszych działań, w sprawozdaniu wezwano między innymi państwa członkowskie do zapewnienia pełnej i prawidłowej transpozycji Dyrektywy, a także zwrócenia uwagi na kompetencje organów nadzorujących ochronę danych osobowych. Powinny one otrzymać wystarczające zasoby do wykonywania swoich zadań w zakresie ochrony danych osobowych, posiadać

²² <https://www.edpb.europa.eu/documents/other-policy-document/contribution-of-the-edpb-to-the-european-commissions-evaluation-of>.

uprawnienia określone w Dyrektywie oraz uczestniczyć w procesie konsultacji projektów aktów prawnych i środków administracyjnych. Państwa członkowskie powinny również kontynuować działania mające na celu zapewnienie właściwym organom szkoleń dotyczących wymogów ochrony danych, w tym w odniesieniu do nowych technologii.

W zakresie odnoszącym się do Dyrektywy w sprawozdaniu wskazano, że zakres organów przetwarzających dane osobowe może być szeroki i państwo może go kształtować, nadając konkretnym podmiotom szczególne uprawnienia (pod warunkiem, że w określonym celu).

W sprawozdaniu wskazano, że *jeżeli chodzi o zakres podmiotowy, przetwarzanie danych wchodzi w zakres dyrektywy o ochronie danych w sprawach karnych, jeżeli, po pierwsze, zajmuje się nim właściwy organ, a po drugie, gdy dane osobowe przetwarza się w celach zgodnych z tą dyrektywą (np. zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom). Zdaniem Komisji „właściwe organy”, w rozumieniu dyrektywy o ochronie danych w sprawach karnych, to organy państwa lub podmioty prywatne, którym prawo nadaje szczególne uprawnienia wykraczające poza uprawnienia wynikające ze zwykłych przepisów obowiązujących w stosunkach z innymi osobami fizycznymi lub z możliwości stosowania przymusu. Organy te są właściwymi organami zgodnie z dyrektywą o ochronie danych w sprawach karnych, jeżeli (nawet wyłącznie sporadycznie lub w odosobnionych przypadkach) przetwarzają dane w celu zapobiegania przestępstwom, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar (w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom). Oznacza to na przykład, że przetwarzanie danych osobowych przez takie organy do celów innych niż dyrektywa o ochronie danych w sprawach karnych (np. do celów związanych z zasobami kadrowymi lub innych celów administracyjnych, takich jak przetwarzanie danych osobowych przez jednostki analityki finansowej) w ramach dorobku prawnego UE w zakresie przeciwdziałania praniu pieniędzy jest objęte zakresem stosowania RODO, a nie dyrektywy o ochronie danych w sprawach karnych²³.*

Odnosnie do zarządzania organami nadzorującymi ochronę danych podniesiono, że wszystkie państwa członkowskie z wyjątkiem dwóch (Belgii i Szwecji) powierzyły egzekwowanie przepisów dyrektywy o ochronie danych w sprawach karnych organowi nadzorczemu odpowiedzialnemu również za egzekwowanie RODO. Belgia powierzyła nadzór nad policją do celów dyrektywy o ochronie danych w sprawach karnych innemu organowi nadzorczemu.

²³ https://www.edpb.europa.eu/documents/other-policy-document/contribution-of-the-edpb-to-the-european-commissions-evaluation-of_pl.

W Szwecji nadzór nad niektórymi właściwymi organami, w tym policją, sprawują wspólnie organ nadzorczy właściwy ds. RODO oraz inny organ nadzorczy. Co więcej, zgodnie z dyrektywą o ochronie danych w sprawach karnych żaden organ nadzorujący ochronę danych nie jest właściwy do nadzorowania sądów w ramach sprawowania przez nie wymiaru sprawiedliwości. Jeśli chodzi o przepisy dyrektywy o ochronie danych w sprawach karnych dotyczące niezależności organów nadzorujących ochronę danych, wszystkie państwa członkowskie przewidziały w swoich przepisach transponujących, że podczas wykonywania swoich zadań organy nadzorujące ochronę danych działają w sposób niezależny, a członkowie tych organów muszą być wolni od wszelkich wpływów zewnętrznych i nie przyjmować od nikogo poleceń. Nadzór nad zgodnością z przepisami wykonywany przez organy nadzorujące ochronę danych ma kluczowe znaczenie i został zagwarantowany w art. 8 ust. 3 Karty praw podstawowych. W dyrektywie o ochronie danych w sprawach karnych nakłada się na państwa członkowskie obowiązek zapewnienia, by każdy organ nadzorujący ochronę danych posiadał skuteczne uprawnienia w zakresie prowadzenia postępowań, uprawnienia naprawcze oraz uprawnienia doradcze. To warunek wstępny właściwego egzekwowania przepisów o ochronie danych, a tym samym osiągnięcia celu dyrektywy o ochronie danych w sprawach karnych, jakim jest wysoki stopień ochrony praw podstawowych, w szczególności prawa do ochrony danych osobowych oraz zapewnienie swobodnego przepływu danych w UE. (...). Wszystkie państwa członkowskie przyznały swoim organom uprawnienia w zakresie prowadzenia postępowań określone w dyrektywie o ochronie danych w sprawach karnych, a większość państw członkowskich nadała im również inne uprawnienia (np. do prowadzenia audytów, uzyskiwania dostępu do pomieszczeń, wykonywania kopii danych oraz konfiskowania przedmiotów (...))²⁴.

Z kolei w dokumencie Parlamentu Europejskiego z 2021 r. (*Assessment of the implementation of the Law Enforcement Directive*²⁵) w kontekście Polski zwrócono uwagę, że w odróżnieniu od innych państw (Belgia, Czechy, Finlandia, Francja, czy też Węgry), które przyjęły przepisy o ochronie danych do operacji przetwarzania prowadzonych przez organy, takie jak służby wywiadowcze, w celu ochrony bezpieczeństwa narodowego, Polska wykluczyła całkowicie zastosowanie unijnych przepisów o ochronie danych do szerokiego zakresu działań, nawet tych, które nie mają nic wspólnego z bezpieczeństwem narodowym lub tych, które wchodziłyby w zakres bezpieczeństwa publicznego i tym samym powinny podlegać transpozycji Dyrektywy. W szczególności polska transpozycja Dyrektywy nie ma zastosowania do danych osobowych przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego, co może być uznane za zbyt szerokie wyłączenie. Generalnie nie sformułowano

²⁴ Jw.

²⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0530-> Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies PE 740.209 - December 2022,

daleko idących rekomendacji, wskazując w sposób ogólny na konieczność przestrzegania zapisów Dyrektywy, ścisłą jej wykładnię i właściwe umocowanie organów nadzoru.

W latach 2024–2025 Komisja rozpoczęła drugą ewaluację Dyrektywy. W styczniu 2026 r. EDPB poinformowała o przekazaniu Komisji obszernego raportu obejmującego jej funkcjonowanie w okresie od stycznia 2022 r. do sierpnia 2025 r. Raport ten miał stanowić podstawę drugiego oficjalnego przeglądu Komisji, który zgodnie z Dyrektywą ma zostać przedstawiony Parlamentowi Europejskiemu i Radzie w czerwcu 2026 roku.

W kontekście analizy dostępnych źródeł można jedynie stwierdzić, że do 2026 r. Komisja Europejska, EDPB i Parlament Europejski nie opublikowały dokumentu wskazującego wprost, iż art. 3 pkt 1 UDODO narusza Dyrektywę. Instytucje UE formułowały natomiast bardziej ogólne zastrzeżenia dotyczące nadmiernej różnorodności implementacji, ograniczeń praw jednostki oraz wyjątków krajowych, które potencjalnie mogą obejmować również rozwiązanie przyjęte w Polsce.

Z kolei w zaleceniu nr 49 zawartym w decyzji wykonawczej Komisji Europejskiej z 2024 r. ustanawiającej sprawozdanie z oceny stosowania dorobku Schengen przez Polskę w 2024 r. zawarto zalecenie o charakterze priorytetowym²⁶. Z jego treści wynika, że Polska powinna zapewnić pełną transpozycję Dyrektywy w odniesieniu do przetwarzania danych osobowych objętych art. 3 ust. 1 UDODO oraz zapewnić transpozycję Dyrektywy również wobec danych przetwarzanych na podstawie dorobku Schengen przez organy wymienione w art. 3 ust. 2 UDODO, w szczególności danych z Schengen Information System oraz Visa Information System.

W kontekście przedstawionych stanowisk można dojść do wniosku, że w przypadku Polski sformułowane zostały przez organy europejskie pewne zastrzeżenia odnoszące się do niewłaściwej implementacji Dyrektywy również w zakresie brzmienia art. 3 pkt 1 UDODO. Nadmienić jednak należy, że instytucje UE do tej pory wypowiadały się raczej na poziomie ogólnych standardów implementacji Dyrektywy (poza wspomnianym zaleceniem nr 49).

W dniu 8 lipca 2026 r. Komisja Europejska wszczęła postępowanie naruszeniowe wobec Polski kierując stosowne wystąpienie do Ministra Spraw Zagranicznych. Komisja Europejska wskazała w nim, że zawarte w art. 3 ust. 1 UDODO wyłączenie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości prowadzi do nadmiernego ograniczenia zakresu stosowania przepisów implementujących Dyrektywę. Wyłączenie obejmuje bowiem niemal wszystkie podstawowe akty prawne regulujące postępowanie karne, działalność prokuratury, sądów oraz innych organów ścigania, co w praktyce pozbawia ochrony znaczną część danych osobowych przetwarzanych w ramach zapobiegania i zwalczania przestępczości. W konsekwencji dane

²⁶Schengen evaluation of Poland. Executive summary and recommendations - https://home-affairs.ec.europa.eu/document/download/aa985c3b-2c11-47e7-99e3a7459e7c2bc8_en?filename=Schengen%20evaluation%20of%20Poland.pdf, s. 10.

osobowe zawarte w aktach spraw, rejestrach oraz innych zbiorach prowadzonych na podstawie tych przepisów nie podlegają ochronie przewidzianej w ustawie implementującej Dyrektywę. Dotyczy to między innymi danych przetwarzanych przez prokuratorów podczas prowadzenia postępowań przygotowawczych, także spraw rozpoznawanych przez sądy karne, w tym danych zawartych w protokołach, aktach spraw oraz materiałach związanych z przesłuchaniami uczestników postępowania. Dyrektywa wyraźnie obejmuje swoim zakresem przetwarzanie danych przez organy ścigania i sądy, o czym świadczą zarówno jej przepisy, jak i motywy preambuły. Jednocześnie wskazano, że przepisy krajowe regulujące postępowania karne nie zawierają kompleksowych regulacji dotyczących ochrony danych osobowych, które mogłyby zastąpić rozwiązania wynikające z dyrektywy.

Komisja Europejska zakwestionowała brzmienie wprowadzonych regulacji, które stanowią podstawę wyłączenia akt spraw i danych w urządzeniach ewidencyjnych podkreślając, że przepisy obejmują również akta tworzone i przetwarzane z wykorzystaniem technik informatycznych, a więc także dane przetwarzane w sposób zautomatyzowany. Podkreślono, że nawet akta prowadzone wyłącznie w formie papierowej mogą stanowić zbiór danych, jeżeli są uporządkowane w sposób umożliwiający łatwe wyszukiwanie informacji. Na poparcie tej tezy przywołano orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, w szczególności wyrok w sprawie Endemol Shine przeciwko Finlandii²⁷, w którym ustalono, że dane zawarte w rejestrach sądowych stanowią zbiór danych niezależnie od tego, czy są przechowywane elektronicznie, czy w aktach papierowych.

W rezultacie Komisja Europejska doszła do wniosku, że przepisy wyłączające stosowanie ustawy do szerokiego zakresu sposobów przetwarzania danych przez sądy i organy ścigania są niezgodne z art. 2 Dyrektywy²⁸. Wyłączenie to narusza obowiązek zapewnienia ochrony danych osobowych przetwarzanych przez właściwe organy w ramach zapobiegania i zwalczania przestępczości oraz wykonywania wymiaru sprawiedliwości w sprawach karnych.

W swoim wystąpieniu Komisja Europejska podniosła także szereg innych zarzutów, które sprowadzały się do niewłaściwej implementacji określonych Dyrektywą rozwiązań przewidzianych w:

- 1) art. 9 ust. 3 i 4 Dyrektywy, zobowiązujących państwa członkowskie do zapewnienia, aby organ przekazujący dane osobowe informował odbiorcę o wszelkich szczególnych warunkach ich przetwarzania oraz o obowiązku ich przestrzegania, a także nakładających na odbiorców z innych państw członkowskich UE oraz na właściwe organy i agencje UE bardziej rygorystyczne warunki przetwarzania niż te, które obowiązują przy krajowym przekazywaniu danych. W tym aspekcie art. 21 ust. 6 UDODO nie zapewnia właściwej realizacji Dyrektywy, albowiem reguluje wyłącznie

²⁷ Wyrok TSUE z dnia 7 marca 2024 r., C-740/22, LEX nr 3691186.

²⁸ Zgodnie z art. 2 ust. 2 Dyrektywy ma ona zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

obowiązek informowania odbiorcy o szczególnych warunkach przetwarzania danych i nie zawiera zakazu stosowania odmiennych lub dyskryminujących warunków wobec odbiorców z innych państw członkowskich oraz instytucji UE;

- 2) art. 10 Dyrektywy określającym warunki przetwarzania szczególnych kategorii danych osobowych (danych wrażliwych). Ich przetwarzanie jest dopuszczalne wyłącznie wtedy, gdy jest bezwzględnie niezbędne, objęte odpowiednimi zabezpieczeniami praw i wolności osoby, której dane dotyczą, oraz spełnia jedną z przesłanek określonych w Dyrektywie, takich jak wyraźna podstawa prawna, ochrona żywotnych interesów osoby lub przetwarzanie danych w sposób oczywisty upublicznionych przez tę osobę; wymóg bezwzględnej niezbędności stanowi wzmocnienie zasady minimalizacji danych i zapewnia wyższy poziom ochrony przy przetwarzaniu danych przez organy ścigania. W ocenie Komisji Europejskiej UDODO nie wdraża tych wymogów w pełnym zakresie; art. 14 ust. 2 ustawy nie uzależnia przetwarzania danych wrażliwych od przesłanki bezwzględnej niezbędności, ani nie wymaga stosowania odpowiednich zabezpieczeń chroniących prawa i wolności osób, których dane dotyczą. Ponadto polskie przepisy przewidują szersze podstawy przetwarzania danych niż Dyrektywa, dopuszczając przetwarzanie danych w celu ochrony życia, zdrowia lub interesów osoby, podczas gdy Dyrektywa ogranicza tę możliwość wyłącznie do ochrony żywotnych interesów;
- 3) art. 13 ust. 3, art. 15 oraz art. 16 ust. 4 Dyrektywy, dopuszczających ograniczenie prawa do informacji, dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania wyłącznie wtedy, gdy jest to niezbędne i proporcjonalne w demokratycznym społeczeństwie oraz służy ochronie ściśle określonych wartości, takich jak prawidłowy przebieg postępowań, zapobieganie i ściganie przestępstw, bezpieczeństwo publiczne, bezpieczeństwo narodowe lub prawa i wolności innych osób. Komisja Europejska uznała, że polskie przepisy nie zapewniają pełnej zgodności z tymi wymaganiami. Art. 26 UDODO wprawdzie wskazuje przesłanki ograniczenia praw osób, których dane dotyczą, jednak nie uzależnia ich stosowania od spełnienia wymogu niezbędności i proporcjonalności. Brak tego zastrzeżenia stwarza ryzyko arbitralnego ograniczania praw jednostki. Ponadto ustawa wprowadza dodatkową przesłankę odmowy udzielenia informacji lub dostępu do danych, odnoszącą się do ujawnienia informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych. Zdaniem Komisji rozwiązanie to wykracza poza katalog wyjątków dopuszczonych przez Dyrektywę, ponieważ pozwala na automatyczne ograniczenie praw osób, których dane dotyczą, niezależnie od tego, czy ujawnienie informacji rzeczywiście zagraża prowadzonym postępowaniom, bezpieczeństwu publicznemu lub innym chronionym wartościom. Komisja wskazała również, że polska ustawa nie nakłada obowiązku informowania osoby, której dane dotyczą,

- o przyczynach odmowy sprostowania, usunięcia danych lub ograniczenia ich przetwarzania, a obowiązek taki przewidziano jedynie w odniesieniu do odmowy prawa dostępu, co nie odpowiada wymogom Dyrektywy;
- 4) art. 17 Dyrektywy, ustanawiającym uprawnienie osoby, której dane dotyczą, do pośredniego wykonywania swoich praw za pośrednictwem organu nadzorczego w sytuacjach, gdy bezpośredni dostęp do tych praw został ograniczony. Administrator ma obowiązek poinformować osobę o takiej możliwości, natomiast organ nadzorczy powinien zweryfikować zgodność przetwarzania z prawem, poinformować o wynikach kontroli oraz o prawie do wniesienia środka zaskarżenia do sądu. Mechanizm ten stanowi dodatkową gwarancję ochrony praw jednostki i funkcjonuje niezależnie od prawa do wniesienia skargi do organu nadzorczego, co potwierdził Trybunał Sprawiedliwości Unii Europejskiej w sprawie *Ligue des droits humains ASBL*. Komisja Europejska uznała, że polskie przepisy nie zapewniają realizacji tego mechanizmu. UDODO przyznaje wprowadzić osobom, których dane dotyczą, prawo do wniesienia skargi do organu nadzorczego oraz zobowiązuje administratora do informowania o tej możliwości, a także określa zadania organu nadzorczego związane z kontrolą przestrzegania przepisów. Nie przewiduje jednak odrębnej procedury umożliwiającej organowi nadzorczemu wykonywanie roli pośrednika w realizacji praw osoby, której dane dotyczą;
- 5) art. 25 ust. 1 Dyrektywy, który zobowiązuje administratorów do prowadzenia ewidencji operacji przetwarzania danych w zautomatyzowanych systemach, obejmującej m.in. informacje pozwalające ustalić datę, godzinę, tożsamość osoby dokonującej operacji, odbiorców danych oraz zasadność przeglądania i ujawniania danych osobowych; wymogi te mają umożliwić skuteczną kontrolę legalności przetwarzania, zapobiegać nadużyciom oraz ułatwiać audyty prowadzone przez organy nadzorcze. Komisja Europejska uznała, że UDODO nie wdraża tych wymogów w pełnym zakresie. Art. 36 ust. 3 ustawy nakazuje wprowadzić rejestrowanie daty i godziny operacji oraz – w miarę możliwości – tożsamości osoby przeglądającej lub ujawniającej dane i odbiorców danych, jednak nie wymaga ewidencjonowania informacji pozwalających ustalić zasadność dostępu lub ujawnienia danych w zautomatyzowanych systemach przetwarzania;
- 6) art. 34 Dyrektywy, który reguluje zadania inspektora ochrony danych, obejmujące przede wszystkim informowanie i doradzanie administratorowi oraz jego pracownikom w zakresie obowiązków wynikających z przepisów o ochronie danych, monitorowanie ich przestrzegania oraz udzielanie porad dotyczących oceny skutków dla ochrony danych. Natomiast obowiązki przeprowadzania oceny skutków dla ochrony danych oraz prowadzenia uprzednich konsultacji z organem nadzorczym spoczywają na administratorze danych, zgodnie z art. 27 i 28 Dyrektywy. Komisja Europejska uznała, że UDODO nieprawidłowo implementuje te przepisy.

Art. 37 ust. 3 oraz art. 38 ust. 6 UODO dopuszczają bowiem powierzenie inspektorowi ochrony danych obowiązku przeprowadzenia oceny skutków dla ochrony danych oraz obowiązku prowadzenia uprzednich konsultacji z organem nadzorczym; zdaniem Komisji rozwiązanie to jest niezgodne z Dyrektywą, ponieważ prowadzi do przeniesienia na inspektora obowiązków należących do administratora danych. Taki podział ról osłabia niezależną funkcję doradczą i kontrolną inspektora ochrony danych, który powinien monitorować wykonywanie obowiązków administratora, a nie wykonywać je w jego imieniu;

- 7) art. 45 Dyrektywy, który określa zakres właściwości organów nadzorczych w zakresie ochrony danych osobowych. Dyrektywa wyłącza spod nadzoru jedynie przetwarzanie danych przez sądy w zakresie sprawowania wymiaru sprawiedliwości, a państwa członkowskie mogą rozszerzyć to wyłączenie na inne niezależne organy wymiaru sprawiedliwości wykonujące funkcje orzecznicze. Komisja Europejska uznała, że UDODO wykracza poza dopuszczalne wyjątki. Art. 1 pkt 3 ustawy całkowicie wyłącza spod nadzoru przetwarzanie danych osobowych przez prokuraturę oraz obejmuje wyłączeniem całą działalność sądów, a nie tylko przetwarzanie danych w związku ze sprawowaniem wymiaru sprawiedliwości; tak szerokie wyłączenie nie znajduje oparcia w art. 45 ust. 2 Dyrektywy.

W podsumowaniu Komisja uznała, że Polska uchybiła obowiązkom wynikającym z Dyrektywy, nieprawidłowo implementując szereg jej przepisów, w szczególności art. 2, 9 ust. 4, 10, 13 ust. 3, 15, 16 ust. 4, 17 w związku z art. 46 ust. 1 lit. g), 25, 34 w związku z art. 27 i 28 oraz 45. Na podstawie art. 258 Traktatu o Funkcjonowaniu Unii Europejskiej²⁹ Komisja wezwała Rzeczpospolitą Polską do przedstawienia stanowiska w terminie dwóch miesięcy od otrzymania pisma.

Z perspektywy całego uzasadnienia ostatni zarzut ma charakter ustrojowy. Komisja uznała, że polskie przepisy całkowicie wyłączają prokuraturę spod nadzoru niezależnego organu ochrony danych oraz zbyt szeroko wyłączają spod tego nadzoru sądy, podczas gdy Dyrektywa dopuszcza wyłączenie jedynie czynności przetwarzania danych przez sądy w toku sprawowania wymiaru sprawiedliwości. To jeden z najistotniejszych zarzutów dotyczących systemu nadzoru nad przetwarzaniem danych osobowych w Polsce.

IV. Stanowisko w zakresie uwag PUODO

1. Zakres wyłączenia określony w art. 3 UDODO

Nie budzi wątpliwości, że Dyrektywa tworząc określone ramy ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy

²⁹ Traktat o funkcjonowaniu Unii Europejskiej zawarty pierwotnie w Rzymie 25 marca 1957 r., Dz.U. z 2004 r., Nr 90, poz. 864/2; Dz. Urz. UE serii C z 2010 r., Nr 83.

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, przekazała państwom członkowskim możliwość ukształtowania (także poprzez sformułowanie wyższych zabezpieczeń niż przewidziane w Dyrektywie), określonych zasad przetwarzania danych osobowych przez właściwe organy. Art. 2 ust. 2 Dyrektywy zawiera natomiast przepisy dotyczące zakresu zastosowania do:

- przetwarzania danych osobowych przez właściwe organy do celów określonych w art. 1 ust. 1;
- przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Istotne z punktu widzenia Dyrektywy pozostaje zatem to, że w przypadku przetwarzania danych osobowych przez właściwe organy 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, państwa członkowskie mają możliwość odrębnego ukształtowania zasad ochrony danych osobowych, aniżeli ma to miejsce w ramach RODO, jednak przy zastosowaniu standardów i wymogów zawartych w Dyrektywie.

Zgodnie z motywem 20 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. W tym kontekście, mając na względzie przepisy RODO oraz Dyrektywy, w UDODO określono jej zastosowanie do danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, a zatem z szeroko pojętymi działaniami związanymi z zapewnieniem bezpieczeństwa państwa.

W ramach tych podstaw na mocy art. 3 ust. 1 i 2 UDODO wyłączono z zakresu normatywnego ustawy, a co za tym idzie, także wymagań Dyrektywy przetwarzanie danych osobowych:

- znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie k.k.w., k.p.k., k.k.s., k.p.o.w., ustawy z 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz.U. z 2022 poz. 1689), UPOP, oraz ustawy z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich (Dz. U. poz. 1700 oraz z 2023 r. poz. 289);

- przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

Wyłączenie z art. 3 pkt 1 UDODO oparte zostało na kryterium przedmiotowym, które dotyczy sposobu (miejsca) przetwarzania danych rozumianego jako akta spraw oraz powiązanych z nimi urządzeń ewidencyjnych, w tym także tych, które są tworzone przy wykorzystaniu systemów teleinformatycznych. Takie podejście odwoływało się do swoistej wykładni pojęcia zbioru danych, które w odniesieniu do akt spraw jako zbioru dokumentów papierowych znajdowało merytoryczne uzasadnienie, jednak w odniesieniu do danych gromadzonych w urządzeniach ewidencyjnych w systemach informatycznych stawało się zawodne. Tymczasem art. 2 ust. 2 Dyrektywy dotyczy stosowania ustawy do przetwarzania danych osobowych w „zbiorach” mających charakter informatyczny (według Dyrektywy zautomatyzowany), co szczególnie w dobie powszechnej cyfryzacji zyskuje na znaczeniu. W związku z tym podnoszony jest zarzut niewłaściwej wykładni pojęcia „zbioru danych”, które legło u podstaw daleko idącego wyłączenia. Nie budzi bowiem wątpliwości, iż generalnie urządzenia ewidencyjne stanowią zbiór danych i spełniają kryteria definicji zawartej w art. 3 ust 6 Dyrektywy, gdzie wskazano, że: *„zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie*. Analogiczną definicję przyjęto w art. 4 pkt 17 UDODO. Opiera się ona na określonych elementach, które definiują to pojęcie przez pryzmat „uporządkowanego zestawu” (czyli nieprzypadkowej masy danych) i ich „dostępności według określonych kryteriów”, która daje możliwość ich wyszukiwania, odnajdywania i generowania.

O ile można zaakceptować pogląd, że akta postępowania karnego nie są zbiorem danych osobowych, skoro gromadzi się w nich przede wszystkim informacje dotyczące określonego zdarzenia, na podstawie których organ prowadzący postępowanie i wydający rozstrzygnięcie kształtuje swoje stanowisko co do faktu popełnienia czynu zabronionego, sprawcy tego czynu oraz odpowiedzialności karnej, o tyle inaczej sytuacja kształtuje się w przypadku urządzeń ewidencyjnych. Sam fakt, że dokument, pośród innych informacji, zawiera między innymi dane osobowe nie sprawia, iż staje się on zestawem, danych osobowych, a tym bardziej zbiorem danych. Trybunał Sprawiedliwości w ww. wyroku z dnia 17 lipca 2014 r. w sprawach C-141/12 i C-372/12 wskazał, że dokumenty, w których zawarte są dane osobowe, na przykład dotyczące danej osoby, nie nabierają przez to charakteru „danych osobowych” w rozumieniu prawa unijnego. Nie stanowią zatem danych osobowych, ani tym bardziej zestawu takich danych, dokumenty wchodzące w skład akt, np. protokół przesłuchania czy wyrok z uzasadnieniem. Należy wszakże podkreślić, iż rozwój systemów informatycznych oraz wprowadzanie akt elektronicznych nie pozostają bez wpływu na stanowisko w tym zakresie. Na osobowe kryterium wyszukiwania jako warunek

uznania zbioru za zbiór danych osobowych wskazywały również polskie sądy administracyjne, np. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 16 marca 2007 r. (II SA/Wa 2110/06). Uporządkowanie (struktura) zbioru może odnosić się albo do indywidualnych osób (oznaczonych np. nazwiskiem lub numerem identyfikacyjnym), albo do kryteriów grupowych stosowanych do większej liczby osób (np. wiek, wykonywana praca, prawo do określonych przywilejów, członkostwo w organizacjach). Akta sprawy karnej nie są zorganizowane według kryteriów dotyczących osób fizycznych. Kryteria, według których organizowane są akta, odnoszą się nie do danych osobowych, a do kolejności przeprowadzania dowodów lub wątków postępowania dotyczących zwykle odrębnych czynów zabronionych. Kryteria te nie pozwalają na wyszukiwanie danych osobowych, które są rozproszone po całym materiale dowodowym.

W tym kontekście problematyczną pozostaje kwestia przetwarzania danych w urządzeniach ewidencyjnych, która w określonych procedurach (wskazanych ustawach) również została wyłączona z zakresu regulacji wynikających z Dyrektywy. Zarzut podniesiony w tym zakresie przez PUODO znajduje merytoryczne uzasadnienie, gdyż dokonując tak szerokiego wyłączenia, nie zagwarantowano pełnej transpozycji przepisów przyznających określone prawa w zakresie ochrony przetwarzanych danych osobowych.

Zgodnie z art. 18 Dyrektywy, państwa członkowskie mogą zapewnić, by wykonywanie praw, o których mowa w art. 13, 14 i 16 Dyrektywy, odbywało się zgodnie z prawem państwa członkowskiego, jeżeli dane osobowe znajdują się w orzeczeniu sądu, protokole lub aktach sprawy przetwarzanych w toku postępowania przygotowawczego lub sądowego w sprawie karnej. Implementację art. 18 Dyrektywy stanowi w tym zakresie art. 27 UDODO. Zgodnie z tym przepisem, w odniesieniu do danych osobowych zgromadzonych w postępowaniach, prowadzonych na podstawie ustaw wskazanych w art. 3 pkt 1, prawa osób, których dane dotyczą, są wykonywane wyłącznie na podstawie i w zakresie przewidzianym przez przepisy regulujące te postępowania.

Treść motywu 44 Dyrektywy wskazuje wprost na możliwość przyjmowania przez państwa członkowskie aktów prawnych pozwalających opóźnić, ograniczyć lub pominąć informowanie osób, których dane dotyczą, lub ograniczyć, w całości lub w części, dostęp tych osób do ich własnych danych osobowych w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem niezbędnym i proporcjonalnym w celu uniemożliwienia zakłócania czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych, czynności procesowych, zapobiegania przestępczości lub wykrywania i ścigania czynów zabronionych. Niemniej jednak kwestia ta winna być uregulowana w taki sposób, aby nie wyłączać ochrony praw osób, których dane są przetwarzane w zakresie określonym w art. 1 Dyrektywy.

Informacje zawarte w aktach prowadzonych spraw, szczególnie na etapie postępowania przygotowawczego, objęte są tajemnicą postępowania, a część przepisów proceduralnych (np. art. 148a i art. 156 k.p.k.) w sposób istotny chroni

przetwarzane dane osobowe. W tym aspekcie trudno zarzucić brak implementacji Dyrektywy, której istota sprowadzała się do umożliwienia państwom członkowskim dostosowania jej zapisów do systemu krajowego. Problem właściwej implementacji powinien być jednak rozstrzygany na kilku płaszczyznach.

Mając na względzie postanowienia Dyrektywy, należy podkreślić, że:

- 1) nie ma wymogów, aby kwestię nadzoru nad przetwarzaniem danych osobowych w sprawach określonych w art. 1 Dyrektywy sprawował centralny organ utworzony na gruncie przepisów RODO. W tym aspekcie dążenie PUODO do objęcia nadzorem akt prokuratorskich oraz informatycznych urzędów ewidencyjnych jest przejawem dążenia do rozszerzenia zakresu jego kompetencji w oparciu o preferowaną wykładnię przepisów RODO oraz Dyrektywy. Nie oznacza to, iż określone państwa w systemach prawnych nie przyjęły podobnego rozwiązania (np. we Francji uprawnienia tego rodzaju posiada centralny organ - Commission nationale de l'informatique et des libertés (CNIL)), jednak z bardzo ograniczonymi uprawnieniami³⁰. W UDODO przyjęto w tym zakresie inne podejście poprzez istotne wykorzystanie klauzul ograniczających uprawnienia osób, których dane podlegają przetwarzaniu. Dodać należy, iż Komisja Europejska nie formułowała w tym zakresie zarzutów, co oczywiście nie oznacza, iż dotychczasowe rozwiązania dotyczące nadzoru nie mogą budzić zastrzeżeń,
- 2) akta spraw wyłączonych przedmiotowo w oparciu o art. 3 pkt 1 UDODO nie obejmują jedynie akt postępowania karnego, ale także akta postępowań o wykroczenie prowadzonych przez policję, czy też postępowań z zakresu ustawy o wspieraniu i resocjalizacji nieletnich prowadzonych przez sądy rodzinne. W tym stanie rzeczy wyłączenie, o którym mowa w art. 3 pkt 1 UDODO częściowo wynika z interpretacji pojęcia „zbioru dokumentów”, a ponadto z zastosowania precyzyjnie określonej w RODO i Dyrektywie możliwości wyłączenia działalności sądownictwa powszechnego w zakresie sprawowania wymiaru sprawiedliwości. Nie budzi wątpliwości, że prowadzenie akt spraw na podstawie wskazanych przepisów w zdecydowanej większości mieści się w działaniach z zakresu sprawowania wymiaru sprawiedliwości,
- 3) akta spraw karnych (postępowania przygotowawczego, postępowania w sprawach o wykroczenia), które stanowią w swej istocie potencjalną podstawę rozpoznania sprawy przez sądy w ramach sprawowania wymiaru sprawiedliwości, podlegają wyłączeniu. Trudno w tej mierze wyobrazić sobie zaakceptowanie swoistego dychotomicznego podejścia do akt postępowania karnego, z wyodrębnieniem fazy postępowania przygotowawczego i jurysdykcyjnego, w zakresie innych reguł

³⁰ CNIL nie jest właściwa do kontrolowania operacji przetwarzania danych dokonywanych przez sądy i prokuraturę podczas wykonywania ich funkcji jurysdykcyjnych. CNIL może kontrolować systemy informatyczne i bazy danych wykorzystywane przez policję, żandarmerię lub inne właściwe organy w celach zapobiegania przestępczości, prowadzenia dochodzeń i wykonywania kar.

przetwarzania danych osobowych i nadzoru nad tymi samymi informacjami. Powyższe uzasadnia podjęcie prac nad stworzeniem formuły „niezależnego organu” nadzoru nad przetwarzaniem danych osobowych w postępowaniu karnym, a także, mając na uwadze motyw 20 Dyrektywy, do odrębnego określenia w ustawie procesowej „procedur i operacji przetwarzania danych osobowych ujmowanych w orzeczeniach sądowych lub aktach związanych z postępowaniem karnym”. Dotyczy to nie tylko sądów, ale także innych organów wymiaru sprawiedliwości.

Rozważenia wymaga, czy istnieje możliwość stworzenia takich regulacji, które skutkowałyby możliwością przekazania na gruncie prawa polskiego nadzoru nad częścią spraw, o których mowa w art. 3 pkt 1 UDODO, niezależnemu organowi przy uwzględnieniu rozwijających się baz i systemów elektronicznych, a w najbliższym czasie także akt elektronicznych. W tym aspekcie należy uznać za uzasadniony zarzut sformułowany przez PUODO odnoszący się do niezastosowania art. 2 ust 2 Dyrektywy w zakresie braku podstaw do wyłączenia systemów elektronicznych. Jednakowoż należy wziąć pod uwagę, że systemy elektroniczne już istniejące i tworzone zawierają nie tylko odrębne informacje o sprawie w ramach urządzeń ewidencyjnych, ale także mogą obejmować odwzorowanie akt sprawy oraz dokumenty procesowe wytwarzane w ramach sprawowania wymiaru sprawiedliwości, czy też realizowania funkcji śledczej, które samodzielnie nie tworzą zbioru danych.

Należy wobec tego stwierdzić, że ustawodawca powinien rozważyć, czy istnieje możliwość takiego ukształtowania przepisów, aby dokonać odpowiedniej korekty art. 3 ust. 1 UDODO w zakresie przyznania osobom, których dane są przetwarzane, określonych uprawnień w obszarach wskazanych przez Komisję Europejską w wystąpieniu z dnia 8 lipca 2026 r., z uwzględnieniem konieczności zachowania odpowiedniego balansu pomiędzy wykonywaniem funkcji związanych z zapewnieniem bezpieczeństwa publicznego, a ochroną praw i wolności innych osób (art. 13 ust. 3 i art. 15 ust. 3 Dyrektywy). Można przyjąć, że te okoliczności miał na uwadze ustawodawca europejski, formułując art. 18 Dyrektywy przyznający szerokie uprawnienia w zakresie kształtowania regulacji przez państwo członkowskie.

W obecnym stanie prawnym można oczywiście rozważać, czy ochrona w poszczególnych ustawach objętych art. 3 pkt 1 UDODO pozostaje w zgodzie z ideą Dyrektywy i czy ustawy te zawierają przepisy chroniące w odpowiedni sposób i na odpowiednim poziomie prawa jednostek, uwzględniając zarówno aspekt akt postępowań, jak i danych zawartych w informatycznych urządzeniach ewidencyjnych. Przepisy ustaw określonych w art. 3 pkt 1 UDODO obejmują bowiem pewne regulacje gwarantujące ochronę danych zawartych w aktach postępowań, jednak w kontekście formułowanych uwag przez Komisję Europejską nie dają rękojmi takiej ochrony, jaka wynika z Dyrektywy. W tym układzie należałoby rozważyć, czy istnieje możliwość wprowadzenia do tych ustaw dodatkowych gwarancji odpowiadających regulacjom art. 13, 14 oraz 16 Dyrektywy przyznających daleko idące uprawnienia osobom, których dane są

przetwarzane w zakresie prawa do informacji, usunięcia lub sprostowania danych osobowych bez naruszenia skuteczności działań podejmowanych m.in. w celu zapewnienia zwalczania przestępczości.

2. Organy nadzoru w sądownictwie

W kontekście zarzutów dotyczących funkcji z zakresu nadzoru należy zwrócić uwagę, iż w RODO w motywie 20 zawarto wskazanie, że właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości po to, by chronić niezawisłość sprawowania tego wymiaru. Powyższy kierunek interpretacji przepisów został też przedstawiony w motywie 80 Dyrektywy, gdzie wskazano, że ma ona zastosowanie do sądów, jednak właściwość organów nadzorczych (niezależnych) nie może obejmować kwestii związanych ze sprawowaniem wymiaru sprawiedliwości. Motyw ten potwierdza zatem, 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. Państwa członkowskie mogą postanowić, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych także przez inne niż sądy niezależne organy wymiaru sprawiedliwości w ramach podejmowania przez nie czynności z zakresu sprawowania tego wymiaru.

W takim przypadku:

- właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości - tak by chronić niezawisłość sprawowania wymiaru sprawiedliwości,
- powinna istnieć możliwość powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego,
- organy te powinny w szczególności zapewnić przestrzeganie przepisów RODO, zwiększać w wymiarze sprawiedliwości wiedzę o obowiązkach wynikających z tego rozporządzenia oraz rozpatrywać skargi związane z operacjami przetwarzania danych.

Kwestię tę przesądza w sposób jednoznaczny art. 55 ust. 3 RODO, który wskazuje, że organy nadzorcze nie są właściwe do nadzorowania operacji przetwarzania danych osobowych dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości.

Nie budzi zatem wątpliwości, iż w kontekście obowiązujących regulacji dotyczących nadzoru czynności obejmujące wymiar sprawiedliwości są wyłączone z zakresu normatywnego RODO. Z tego powodu problematyka ta została uregulowana w sposób odrębny i kompleksowy w przypadku sądów powszechnych (art. 175dd PUSP), co znajduje także zastosowanie w odniesieniu do sądów wojskowych, (art. 6b-6c ustawy z dnia 21 sierpnia 1997 r. Prawo

o ustroju sądów wojskowych³¹), sądów administracyjnych, w tym Naczelnego Sądu Administracyjnego (art. 12b ustawy z dnia 25 lipca 2002 r. Prawo o ustroju sądów administracyjnych³²) oraz Sądu Najwyższego (art. 97a ustawy z dnia 8 grudnia 2017 r. o Sądzie Najwyższym³³).

PUODO w wystąpieniu w tym zakresie podnosi kwestię braku niezależności organów sądowych, o której mowa w art. 51-52 RODO, jak również wskazuje zbyt szeroką interpretację pojęcia wymiaru sprawiedliwości w odniesieniu do przetwarzanych danych. Zdaniem tego organu pojęcie sprawowania wymiaru sprawiedliwości w kontekście ram ochrony danych osobowych ustanowionych przez RODO należy rozumieć wąsko.

Zgodnie ze stanowiskiem Trybunału Konstytucyjnego zawartym w wyroku z dnia 1 grudnia 2008 r.³⁴ *wymiar sprawiedliwości stanowi działalność państwa polegającą na sądzeniu, czyli wiążącym rozstrzyganiu sporów o prawo, w których przynajmniej jedną ze stron jest jednostka lub inny podmiot podobny* (zob. L. Garlicki, Polskie prawo konstytucyjne. Zarys wykładu, Warszawa 2006, s. 342; Z. Czeszejko-Sochacki, O wymiarze sprawiedliwości w świetle Konstytucji, międzynarodowych standardów i praktyki, "Państwo i Prawo" z. 9/1999, s. 3; S. Włodyka, Ustrój organów ochrony prawnej, Warszawa 1968, s. 16). Tymczasem orzecznictwo administracyjne, co prawda w jednostkowym orzeczeniu, opowiada się w kontekście ochrony danych osobowych za szerokim rozumieniem tego pojęcia. W wyroku NSA z dnia 14 listopada 2025 r., stwierdzono mianowicie, że (...) *jako czynności podejmowane przez sądy w ramach sprawowania wymiaru sprawiedliwości" rozumieć należy cały cykl działań (czynności) sędziego w ramach prowadzonego postępowania sądowego, które zmierzają do wydania orzeczenia końcowego w sprawie, tj. zarówno czynności o charakterze orzecznym, jak i te o charakterze przygotowawczym, czy kontrolnym. Nie tylko bowiem samo wydanie orzeczenia, ale wszystkie poprzedzające wydanie orzeczenia czynności, zmierzające do jego wydania i podejmowane w tym celu, winny być objęte ochroną, należeć do sfery niezawisłości sędziowskiej i tym samym winny być kwalifikowane jako podejmowane w ramach sprawowania wymiaru sprawiedliwości. Wszystkie te czynności sądu, nawet jeśli nie stanowią wyrokowania, są bowiem czynnościami służącymi tej funkcji i pełnią rolę przygotowawczą bądź wykonawczą do wyrokowania. Choć w ramach pełnionych funkcji administracyjnych sędzia podlega nadzorowi ze strony Prezesa sądu, Przewodniczącego wydziału oraz Ministra Sprawiedliwości, to tylko w zakresie organizacyjnym, bez możliwości wydawania sędziom poleceń odnośnie do merytorycznego załatwienia sprawy. Każda decyzja sądu, również ta związana z wysyłką korespondencji sądowej, to czynność sądowa, związana ze stosowaniem prawa procesowego, bowiem jurysdykcyjna działalność sądu nie ogranicza się jedynie do czynności orzecznich związanych z wydawaniem*

³¹ Dz.U. z 2024 r. poz. 1614.

³² Dz.U. z 2026 r. poz. 143.

³³ Dz.U. z 2024 poz. 622.

³⁴ P 54/07, OTK-A 2008/10/171, LEX nr 465092.

*orzeczeniem, ale obejmuje także czynności związane z gromadzeniem materiału procesowego i zewnętrznym prowadzeniem procesu*³⁵. Uwagi te wskazują, że stanowisko PUODO zmierzające do zawężenia pojęcia wymiaru sprawiedliwości w kontekście wyłączenia spod ogólnych zasad nadzoru nie musi być uważane za w pełni uzasadnione.

Zagadnieniem wymagającym analizy jest natomiast kwestia zmiany formuły nadzoru, który obecnie sprawowany jest przez prezesów sądów okręgowych i apelacyjnych, a także Krajową Radę Sądownictwa (KRS). W wystąpieniu PUODO wskazano na konieczność powołania „wewnętrznego” organu nadzorczego (specjalnego), który miałby wykonywać funkcje przewidziane w RODO. Nie przedstawiono jednak żadnej klarownej koncepcji utworzenia i umocowania tego organu. PUODO, podkreślając konieczność zmiany przepisów i strukturalnego przyznania kompetencji nadzorczych w PUSP (i analogicznie również w innych ustawach regulujących funkcjonowanie pozostałych rodzajów sądów) organowi specjalnemu, odwołał się do argumentów, które akurat w tym aspekcie nie mają pierwszorzędного znaczenia. PUODO wskazał bowiem na niekonstytucyjność składu funkcjonującej do 12 maja 2026 r. Krajowej Rady Sądownictwa (będącej organem nadzorczym w przypadku sądu apelacyjnego i Sądu Najwyższego) i przywołał orzecznictwo Trybunału Sprawiedliwości UE (w sprawach C-585/18, C-624/18, C-625/18, C-791/19, C-487/19) oraz Europejskiego Trybunału Praw Człowieka (w sprawach ze skarg nr 43447/19, 49868/19, 57511/19, 1469/20, 50849/21). W wystąpieniu uznano, że Rada nie spełnia wymogów niezależności w rozumieniu ustrojowym, co ma uzasadniać wnioski, że nie może wykonywać prawidłowo nadzoru nad przetwarzaniem danych osobowych w polskich sądach.

Na wstępie należy zamieścić uwagę o charakterze porządkującym. Zgodnie z art. 186 i 187 Konstytucji RP, Krajowa Rada Sądownictwa jest organem niezależnym. Modelowo więc może spełniać funkcje przewidziane dla organu pełniącego funkcje nadzorcze nad przetwarzaniem danych osobowych w ramach sprawowania przez sądy wymiaru sprawiedliwości. Wskazywane przez PUODO jej wady wynikające ze sposobu ukształtowania, na które zwracano uwagę w orzecznictwie europejskim i krajowym, nie mogą dyskwalifikować tego organu w zakresie posiadania kompetencji nadzorczych. Na konstruowany w taki sposób zarzut braku niezależności może być narażony każdy organ, który jest w pewien sposób kształtowany przez zwykłego ustawodawcę. W tym przypadku KRS ma tę przewagę nad jakimkolwiek organem utworzonym przez zwykłego ustawodawcę, że posiada stabilne gwarancje niezależności zakotwiczone w Konstytucji RP. Odrębną kwestią jest natomiast to, że w wystąpieniu PUODO zwraca się uwagę na sposób ukształtowania KRS. Zauważając brak zmian w stanie prawnym od czasu wydania powołanych orzeczeń przez trybunały europejskie, nie można pominąć, że wybór większości członków KRS będących sędziami nastąpił w zupełnie innych okolicznościach. Sejm uwzględnił bowiem w tym zakresie opinię

³⁵ III OSK 250/25. LEX nr 3964332.

samych sędziów i wybrał na członków KRS osoby cieszące się znacznym poparciem środowiska. Wpłynęło to na podwyższenie stopnia faktycznej niezależności KRS. Z tych względów nie można podzielić odmiennej argumentacji przytoczonej w wystąpieniu PUODO.

Natomiast na podzielenie zasługują uwagi PUODO dotyczące ryzyka nieefektywności obecnego „kaskadowego” systemu nadzoru istniejącego w sądach.

Administratorem danych osobowych w zakresie wskazanym przez ustawę są sądy (art. 175db PUSP), a Prezesi tychże sądów są ich organami (art. 22 PUSP). Z kolei zgodnie z art. 175dd PUSP nadzór nad przetwarzaniem tych danych sprawują prezesi sądów wyższego rzędu nad sądami niższego rzędu, za wyjątkiem sądu apelacyjnego, gdzie nadzór sprawuje KRS. Formalnie przepisy zachowują więc odrębność organu nadzorczego od administratora danych.

Ze względu na skomplikowany przedmiot zadań administratora danych, można jednak dostrzec niebezpieczeństwo, że w praktyce czynności w zakresie administrowania danymi będzie wykonywał inspektor ochrony danych osobowych na terenie sądu (który powinien być tylko organem pomocniczym), przyczyniając się jednocześnie do realizacji działań nadzorczych w imieniu prezesa sądu w stosunku do sądów niższych szczebli. W istocie może to wypaczać efektywność działań nadzorczych, zwłaszcza że organ nadzorczy jest równocześnie organem podmiotu pełniącego funkcję administratora danych osobowych.

W tym stanie rzeczy znajdują uzasadnienie podnoszone przez PUODO wątpliwości dotyczące realizacji celów Dyrektywy i skutecznej ochrony praw obywateli w zakresie prawidłowej identyfikacji obszarów zagrożeń i sprawowania realnego, a nie tylko formalnego nadzoru.

Zgodzić się także należy, że uprawnienia poszczególnych organów nadzoru (prezesów sądów) nie są tak spójne i szerokie jak PUODO w zakresie jego właściwości. Do uprawnień tych powinno należeć: upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk (art. 46 ust. 1 lit. b Dyrektywy), doradzanie, 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 danych osobowych (art. 46 ust. 1 lit. c Dyrektywy), udzielanie osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących jej na mocy dyrektywy, a w stosownym przypadku współpraca w tym celu z organami nadzorczymi innych państw członkowskich (art. 46 ust. 1 lit. e Dyrektywy), pełnienie funkcji konsultacyjnych, o których mowa w art. 28 Dyrektywy, co do operacji przetwarzania (art. 46 ust. 1 lit. k Dyrektywy) oraz branie udziału w pracach Europejskiej Rady Ochrony Danych (art. 46 ust. 1 lit. l Dyrektywy). Organy nadzorcze właściwe dla sądów nie posiadają uprawnień doradczych pozwalających przedstawić administratorowi zalecenia zgodnie z procedurą uprzednich konsultacji oraz nie mają prawa wydawania z własnej inicjatywy lub na wniosek opinii skierowanych 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 (jak wymaga tego art. 47 ust. 3 Dyrektywy). PUSP nie przewiduje również mechanizmu zgłaszania naruszeń ochrony danych (art. 48 Dyrektywy), ani obowiązku sporządzania rocznego sprawozdania ze swojej działalności (art. 49 Dyrektywy). Wynika to właśnie z „kaskadowego” modelu nadzoru i braku jednego centralnego organu właściwego w tej materii.

W związku z tym konkluzja PUODO zawarta w sformułowaniu, zgodnie z którym *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 RODO, ale również nie organom nadzorczym usytuowanym w systemie sądownictwa*, nie jest pozbawiona uzasadnionych podstaw.

Należy także zgodzić się ze stanowiskiem, że dla lepszego zagwarantowania wykonywania praw wynikających z Dyrektywy można rozważyć stworzenie osobnego niezależnego centralnego organu nadzorczego, który kontrolowałby sposób przetwarzania danych osobowych przez sądy, ale nie byłby organem wchodzącym w skład struktury tych sądów. Ustrojowo mógłby to być organ działający w ramach KRS, a funkcję w ramach tego organu powinien sprawować sędzia wyróżniający się wiedzą w zakresie ochrony danych osobowych. Sprawowałby on nadzór nad danymi osobowymi w zakresie wynikającym z przepisów, a niezastrzeżonym dla PUODO z określonymi precyzyjnie uprawnieniami analogicznymi do PUODO, uwzględniającymi specyfikę materii objętej nadzorem.

3. Organy nadzoru w prokuraturze

W art. 45 ust. 2 Dyrektywy przewidziano możliwość wyłączenia spod właściwości organu nadzorczego czynności nadzorowania operacji przetwarzania danych osobowych dokonywanych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie tego wymiaru³⁶. Z kolei w motywie 80 Dyrektywy, jako przykład innego niezależnego organu wymiaru sprawiedliwości, który może zostać objęty przez państwo członkowskie przedmiotowym wyłączeniem, wskazano wprost prokuraturę.

W wystąpieniu w zakresie negującym zasadność wyłączenia prokuratury, PUODO słusznie podnosi, że prokuratura nie jest organem wymiaru sprawiedliwości. Niemniej jednak analizując treść Dyrektywy, a przede wszystkim kierując się jej motywami, należy wskazać, że prawodawca unijny, odwołując się

³⁶ Art. 45 ust. 2 Dyrektywy stanowi, 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. 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.

do pojęcia „*judicial authorities*” nie posługiwał się nim w takim znaczeniu, w jakim w Polsce rozumiany jest ustrojowo i funkcjonalnie wymiar sprawiedliwości. Jest oczywiste, że w świetle unormowań konstytucyjnych wymiar sprawiedliwości sprawują sądy, nie oznacza to jednak, że określenie to zostało wykorzystane w akcie unijnym właśnie w takim znaczeniu. Przystępując bowiem do wykładni tego sformułowania, trzeba po pierwsze mieć na uwadze, że w prawie unijnym określenie „*judicial authorities*” najczęściej tłumaczone jest jako „organy sądowe” lub „organy wymiaru sprawiedliwości”. Pojęcie to ma zarazem autonomiczne znaczenie w prawie unijnym, w związku z czym nie zawsze jest identyczne z definicjami przyjętymi w prawie krajowym poszczególnych państw. Najczęściej odnosi się to pojęcie do organów, które uczestniczą w sprawowaniu wymiaru sprawiedliwości, działają niezależnie od władzy wykonawczej, podejmują decyzje podlegające gwarancjom sądowym i ochronie praw podstawowych. W takim ujęciu istnieją podstawy, by pojęciem „*judicial authorities*” obejmować także polską prokuraturę, której status ustrojowy nie został klarownie unormowany. W tym zakresie można zwrócić uwagę na wyrok TSUE z 9 października 2019 r., w sprawie C-489/19³⁷, dotyczący austriackiej prokuratury i wykonywania Europejskiego Nakazu Aresztowania, w którym Trybunał przyjął, że prokuratura należy do grupy organów określanych jako „*judicial authorities*”, o ile jej działania podlegają kontroli sądowej. Brak podobnego orzecznictwa dotyczącego bezpośrednio polskiej prokuratury, niemniej jednak w świetle funkcji ustrojowej i wykonywanych zadań może być uznawana za organ stanowiący „*judicial authority*” i to pomimo tego, że unia personalna Ministra Sprawiedliwości i Prokuratora Generalnego jest czynnikiem osłabiającym jej niezależność³⁸.

W motywie 80 Dyrektywy w zakresie wyłączenia organu nadzoru zwrócono uwagę, że jego właściwość nie może obejmować działań sądów w ramach wykonywania wymiaru sprawiedliwości, co ma na celu ochronę niezawisłości sędziów w wykonywaniu ich zadań sądowych. Możliwość podobnego potraktowania z tego względu prokuratury i wyłączenia jej spod nadzoru PUODO w zakresie przetwarzania danych osobowych wywołuje kontrowersje interpretacyjne podniesione w uzasadnieniu. Do chwili obecnej nie pojawiły się jednak w tej materii żadne zastrzeżenia ze strony Komisji Europejskiej, a w procesie ewaluacji nie sformułowano jednoznacznej krytyki rozwiązań obowiązujących w prawie polskim.

Można zatem przyjąć, że w odniesieniu do prokuratury ustawodawca krajowy był uprawniony zarówno do wyłączenia organu nadzorczego, jak i do stosowania przepisów UDODO wprowadzonych do polskiego porządku prawnego w związku z Dyrektywą. Ma ona bowiem na celu umożliwienie państwom członkowskim dostosowania przepisów odnoszących się do konieczności ochrony danych osobowych zawartych w RODO do ochrony danych przez właściwe organy w związku z realizacją celów odnoszących się do zapobiegania przestępczości,

³⁷ LEX nr 2724994.

³⁸ Zob. wyrok TSUE z dnia 27 maja 2019 r., C-508/18 i C-82/19, Dz.U.UE.C.2019/263/16, LEX nr 2671250; wyrok TSUE z dnia 27 maja 2019 r., C-509/18, Dz.U.UE.C.2019/263/22, LEX nr 2671254.

prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. W takim przypadku organ nadzoru, o którym mowa w RODO, może mieć powierzone kompetencje nadzorcze w zakresie określonym w art. 1 Dyrektywy, jednak nie jest to warunek konieczny. Państwa członkowskie mogą bowiem ustanowić organ odrębny, który będzie nadzorował przetwarzanie danych osobowych w celach określonych przez Dyrektywę i nie nadzorował operacji przetwarzania danych przez sądy w toku sprawowania przez nie wymiaru sprawiedliwości. W tym aspekcie istnieje zatem prawna możliwość wyłączenia PUODO od wykonywania czynności nadzorczych nie tylko w zakresie sprawowania przez sądy wymiaru sprawiedliwości, ale także w zakresie kształtowania sposobu ochrony danych osobowych w zakresie odnoszącym się do Dyrektywy.

Warto w tym miejscu zwrócić uwagę na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 października 2020 r.³⁹, w którym analizowane było zagadnienie przetwarzania danych osobowych znajdujących się w aktach prokuratorskich. W orzeczeniu tym wskazano, że:

- Prezes Urzędu Ochrony Danych Osobowych nie ma uprawnień do merytorycznej kontroli sposobu przetwarzania danych w ramach postępowań prowadzonych przez prokuraturę;
- dostęp do akt i ich weryfikacja podlegają rygorom procedury karnej (np. art. 156 k.p.k.), a nie ogólnym przepisom o ochronie danych (RODO), co wyklucza ingerencję organów administracyjnych (autonomia prawa procesowego);
- wszelkie decyzje o tym, kto i w jakim zakresie może zapoznać się z dokumentami znajdującymi się w aktach prokuratorskich, podejmuje wyłącznie właściwy prokurator lub sąd powszechny, nie zaś organ nadzorczy ds. ochrony danych osobowych.

Przywołane wyżej stanowisko nie jest nowe. Analogiczną linię orzecniczą, wskazującą na niedozwoloną ingerencję organu administracji publicznej w działania prokuratury, sądy administracyjne prezentowały także pod rządami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 poz. 1182)⁴⁰.

Należy podkreślić, iż art. 3 pkt 1 UODO wyłącza stosowanie tej ustawy do ochrony danych osobowych znajdujących się w aktach, to jednak zgodnie z art. 4 pkt 16 UODO ma ona zastosowanie do prokuratury. W tym aspekcie art. 191a UPOP w istocie wskazuje UODO jako wzorzec, w oparciu o który sprawowany jest

³⁹ II SA/Wa 2620/1, LEX nr 3077608.

⁴⁰ Por. np. wyrok NSA z dnia 2 marca 2001 r., II SA 401/00, w uzasadnieniu którego stwierdzono, że „Generalny Inspektor Ochrony Danych Osobowych nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji, czy w inny sposób określony odpowiednimi procedurami”; wyrok WSA w Warszawie z dnia 8 czerwca 2009 r., II Sa/Wa 275/09, w którym z kolei przyjęto, że „sposób działania prokuratury, w tym kwestia zawartości akt określonego postępowania podlega kontroli wyłącznie ze strony organu wyższej instancji - w trybie i na zasadach określonych przepisami ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2002 r. Nr 21, poz. 206 ze zm.) oraz Kodeksu postępowania karnego.”

nadzór nad przetwarzaniem przez prokuraturę danych osobowych. W tym przypadku ustawodawca wyznaczył organy właściwe w zakresie czynności nadzoru nad przetwarzaniem danych osobowych w ramach realizacji zadań określonych w art. 2 UPOP, których administratorami, zgodnie z art. 13 § 6 UPOP, są powszechne jednostki organizacyjne prokuratury. Nadzór ten wykonują w zakresie działalności prokuratury rejonowej - prokurator okręgowy, prokuratury okręgowej - prokurator regionalny, prokuratury regionalnej i Prokuratury Krajowej - Prokurator Krajowy. Rozwiązanie to w swym kształcie jest zbliżone do koncepcji organów nadzoru w sądownictwie.

Analogicznie jak w przypadku sądów powszechnych, można zgodzić się ze stanowiskiem, że takie ukształtowanie formuły nadzoru nad przetwarzaniem danych osobowych przez administratora, jak ma to miejsce w prokuraturze, nasuwa zastrzeżenia pod względem zgodności z Dyrektywą. Co prawda, przepis art. 45 ust. 2 Dyrektywy stanowi, 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, a także niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości, jednak nie oznacza to wyłączenia potrzeby nadzoru nad innymi czynnościami wykonywanymi przez te organy. Ich działalność nie sprowadza się bowiem jedynie do wykonywania funkcji polegającej na sprawowaniu wymiaru sprawiedliwości. Nie jest to jednak równoznaczne z wnioskiem, że przetwarzanie danych osobowych przez prokuraturę w zakresie, w którym realizuje czynności określone w art. 1 Dyrektywy, miałoby podlegać nadzorowi PUODO.

W związku z powyższym, podejmując ewentualne prace legislacyjne, należy dążyć do takiego ukształtowania przepisów, aby funkcje nadzorcze nad czynnościami prokuratury powierzyć organowi niezależnemu o porównywalnej pozycji, jak w przypadku ochrony danych osobowych przetwarzanych przez sądy. Umożliwi to właściwą implementację postanowień Dyrektywy, a także nie spowoduje zagrożeń w sferze skuteczności wykonywania ustawowych zadań przez prokuraturę oraz pozwoli zapewnić realną i skuteczną ochronę praw na poziomie zagwarantowanym przez prawo unijne.