



dr Olgierd Jakubowski

Kryminolog; główny specjalista w Departamencie Prawa i Nowych Technologii UODO
(ORCID: <https://orcid.org/0000-0002-5530-1025>).

Ryzyka związane z przetwarzaniem danych osobowych w aktach postępowań prowadzonych w sądach w świetle przepisów prawa Unii Europejskiej

Słowa kluczowe: dane osobowe, sprawowanie wymiaru sprawiedliwości, systemy teleinformatyczne, nowe technologie, informatyzacja

Artykuł dotyczy problematyki przetwarzania danych osobowych w aktach postępowań prowadzonych przez sądy w kontekście prawa Unii Europejskiej oraz krajowych regulacji ustrojowych. Analizie poddano obowiązujące w Polsce rozwiązania prawne, ze szczególnym uwzględnieniem problemów wynikających z nieprawidłowej implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającej decyzję ramową Rady 2008/977/WSiSW¹ oraz niejednoznacznej interpretacji pojęcia sprawowania wymiaru sprawiedliwości. W opracowaniu omówiono także ryzyka związane z przetwarzaniem danych osobowych w aktach postępowań sądowych, w tym zagrożenia wynikające z postępującej informatyzacji wymiaru sprawiedliwości, wykorzystania systemów teleinformatycznych oraz nowych technologii. Wskazano również, że obecny model ochrony danych osobowych w działalności sądów jest niespójny i wymaga doprecyzowania granic wyłączenia nadzoru Prezesa Urzędu Ochrony Danych Osobowych (UODO).

1. Wprowadzenie

Sprawowanie wymiaru sprawiedliwości jest jednym z kluczowych zadań państwa. Zgodnie z art. 175 ust. 1 Konstytucji Rzeczypospolitej Polskiej z 2.04.1997 r.² wymiar sprawiedliwości w Rzeczypospolitej Polskiej sprawują Sąd Najwyższy, sądy powszechne, sądy administracyjne oraz sądy wojskowe. W literaturze³ podkreśla się, że zarówno w doktrynie, jak i orzecznictwie sądowym i trybunalskim formułowanych jest wiele definicji wymiaru sprawiedliwości. W ujęciu przedmiotowym za wymierzanie sprawiedliwości należy uznać: „działalność państwa polegającą na wiążącym rozstrzyganiu sporów o prawo, w których przynajmniej jedną ze stron jest jednostka lub inny podmiot podobny”⁴.

W ramach wykonywania tych zadań w sądach dochodzi do przetwarzania znacznej liczby danych osobowych, podlegających ochronie zarówno na podstawie Konstytucji RP (art. 51), jak i prawa Unii Europejskiej. Jak podkreśla Monika Florczak-Wątor, art. 51 Konstytucji RP statuuje autonomię informacyjną jednostki oraz określa podstawowe gwarancje związane z ochroną informacji dotyczących osoby fizycznej⁵, natomiast art. 47 Konstytucji RP chroni prawo do prywatności. Ochrona danych osobowych wynika również z art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej⁶ oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej⁷.

Na tle tych standardów konstytucyjnych i unijnych powstaje pytanie o ich praktyczną realizację w działalności sądów, w szczególności odnośnie do ochrony danych osobowych

1 Dz.Urz. UE L 119, s. 89, ze zm. – dalej dyrektywa 2016/680.

2 Dz.U. Nr 78, poz. 483 ze zm. – dalej Konstytucja RP.

3 B. Naleziński [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2023, art. 175.

4 B. Naleziński [w:] *Konstytucja...*, art. 175.

5 M. Florczak-Wątor [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2023, art. 51.

6 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389.

7 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47.

znajdujących się w aktach postępowań sądowych. Celem artykułu jest analiza ryzyk związanych z takim przetwarzaniem, wynikających zarówno z przyjętych rozwiązań prawnych, jak i z praktycznych problemów funkcjonowania sądów oraz nowych wyzwań związanych z informatyzacją wymiaru sprawiedliwości.

2. Podstawy prawne przetwarzania danych osobowych w sądach

Zmiany prawa Unii Europejskiej dotyczące ochrony danych osobowych miały kluczowe znaczenie dla polskiego systemu prawnego w tym obszarze. Wejście w życie przepisów Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)⁸, uchwalenie przepisów ustawy z 10.05.2018 r. o ochronie danych osobowych⁹, a także implementacja dyrektywy 2016/680, a co za tym idzie – uchwalenie przepisów ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości¹⁰ doprowadziło do istotnej przebudowy krajowego systemu ochrony danych osobowych.

RODO w motywie 20 wskazuje, że ma ono zastosowanie do działań sądów i innych organów wymiaru sprawiedliwości, przy czym prawo Unii Europejskiej lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez te podmioty. Jednocześnie w motywie tym podkreślono konieczność ochrony niezawisłości sądów poprzez wyłączenie właściwości organów nadzorczych wobec przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości¹¹. Rozwiązanie to znalazło normatywne odzwierciedlenie w art. 55 ust. 3 RODO.

Jak podkreśla Paweł Fajgielski, wyłączenie kompetencji organu nadzorczego nie ma jednak charakteru całkowitego, ponieważ poza działalnością orzeczniczą sądy przetwarzają dane osobowe również w innych obszarach w innych obszarach, w szczególności administracyjnych, które nadal podlegają nadzorowi organu ochrony danych osobowych¹². W literaturze podkreśla się jednocześnie, że ograniczenie kompetencji Prezesa UODO w zakresie sprawowania wymiaru sprawiedliwości ma służyć ochronie niezawisłości sądów¹³.

Podobne rozwiązania dotyczące sądów i innych niezależnych organów wymiaru sprawiedliwości zostały przyjęte w art. 45 ust. 2 dyrektywy 2016/680, a także w jej motywie 80.

W prawie krajowym szczególne rozwiązania dotyczące nadzoru nad przetwarzaniem danych osobowych przez sądy wprowadzono m.in. w ustawie z 12.05.2011 r. o Krajowej Radzie Sądownictwa¹⁴ oraz ustawie z 27.07.2001 r. – Prawo o ustroju sądów powszechnych¹⁵. Na podstawie art. 3 ust. 2 pkt 10 ustawy o KRS organ ten sprawuje nadzór nad przetwarzaniem danych osobowych przez Trybunał Konstytucyjny, Trybunał Stanu, Sąd Najwyższy, Naczelny Sąd Administracyjny oraz sądy apelacyjne, w ramach prowadzonych przez nie postępowań¹⁶.

Szczegółowe rozwiązania dotyczące przetwarzania danych osobowych oraz nadzoru nad tym przetwarzaniem zawarto w dziale IVA p.u.s.p. (zob. art. 175db i art. 175dd). Przepisy te wskazują, że administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są sądy, a kompetencje nadzorcze w tym zakresie powierzono prezesom sądów oraz Krajowej Radzie Sądownictwa. Organy te uprawnione są m.in. do rozpatrywania skarg osób, których dane dotyczą, podejmowania działań edukacyjnych oraz współpracy z innymi organami nadzorczymi.

Odrębne rozwiązania przyjęto w odniesieniu do sądownictwa administracyjnego. Przepisy ustawy z 25.07.2002 r. – Prawo o ustroju sądów administracyjnych¹⁷ przewidują, że administratorami danych osobowych przetwarzanych w postępowaniach sądowych są sądy administracyjne, natomiast nadzór nad tym przetwarzaniem sprawuje Prezes Naczelnego Sądu Administracyjnego. Jednocześnie regulacje te odsyłają częściowo do rozwiązań przyjętych w ustawie – Prawo o ustroju sądów powszechnych.

3. Problem niewłaściwej implementacji dyrektywy 2016/680 i jego wpływ na przetwarzanie danych osobowych w aktach postępowań

W doktrynie od lat wskazuje się, że obowiązujące przepisy dotyczące przetwarzania danych osobowych w kontekście nadzoru nad sądami i prokuraturą budzą istotne wątpliwości systemowe. Dotyczą one przede wszystkim wyłączenia prokuratury spod nadzoru Prezesa UODO oraz powierzenia kompetencji nadzorczych Krajowej Radzie Sądownictwa i prezesom sądów, którzy mają sprawować niezależny nadzór w tym zakresie¹⁸.

Podkreśla się również, że w sytuacji gdy sądy i prokuratura przetwarzają dane osobowe do celów wynikających z ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, ale poza

8 Dz.Urz. UE L 119, s. 1, ze zm. – dalej RODO.

9 Dz.U. z 2019 r. poz. 1781 ze zm.

10 Dz.U. z 2023 r. poz. 1206 – dalej u.o.d.o.z.p.

11 W motywie tym podkreślono jednak, że: „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 niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takimi operacjami przetwarzania danych”.

12 P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025, art. 55 ogólnego rozporządzenia o ochronie danych.

13 P. Korzeniowski, P. Szustakiewicz, *Model prawny sprawowania przez sądy administracyjne wymiaru sprawiedliwości w rozumieniu przepisów rozporządzenia RODO*, „Zeszyty Naukowe Sądownictwa Administracyjnego” 2024/4, s. 79.

14 Dz.U. z 2024 r. poz. 1186 – dalej ustawa o KRS.

15 Dz.U. z 2024 r. poz. 334 ze zm. – dalej p.u.s.p.

16 W ramach sprawowania ww. nadzoru nad sądami w 2024 r. w KRS zarejestrowano 21 nowych pism oraz wystosowano dwa pisma do różnych organów. Zob. KRS, *Informacja o działalności Krajowej Rady Sądownictwa w 2024 roku*, s. 64, <https://krs.pl/pl/dzialalnosc/sprawozdania/2905-informacje-o-dzialalnosci-krs-w-2024.html> (dostęp: 5.03.2026 r.).

17 Dz.U. z 2024 r. poz. 1267.

18 Zob. A. Grzelak, *Cel i zakres podmiotowy dyrektywy 2016/680 wyzwań dla polskiego ustawodawcy*, „Monitor Prawniczy” 2024/11, dodatek, s. 47–55, a także A. Grzelak, *Prawo pośredniego dostępu do danych na tle art. 17 dyrektywy 2016/680 – gwarancja ochrony czy iluzoryczny mechanizm? Analiza istoty i problemów implementacyjnych*, „Państwo i Prawo” 2026/5, s. 53–71. Zob. również M. Wróblewski, A. Grzelak, *Podstawy prawne systemu ochrony danych osobowych* [w:] *Ochrona danych osobowych w sądach i prokuraturze*, red. A. Grzelak, Warszawa 2019, s. 110.

zakresem prowadzonych postępowań, przepisy nie przewidują spójnego modelu nadzoru¹⁹.

Prezes UODO od wielu lat konsekwentnie wskazuje na nieprawidłową implementację dyrektywy 2016/680 do polskiego porządku prawnego. Zastrzeżenia w tym zakresie były zgłaszane już na etapie opiniowania projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości²⁰. Poważne wątpliwości do projektu wskazywali również eksperci²¹. W kolejnych latach Prezes UODO wielokrotnie występował o podjęcie działań legislacyjnych mających zapewnić prawidłowe stosowanie dyrektywy 2016/680²² oraz usuwać istniejące luki w systemie ochrony danych osobowych²³.

Szczególne znaczenie dla przetwarzania danych osobowych w aktach postępowań ma art. 3 pkt 1 u.o.d.o.z.p. Przepis ten wyłącza stosowanie ustawy do danych osobowych znajdujących się m.in. w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie Kodeksu karnego wykonawczego²⁴, Kodeksu postępowania karnego²⁵, Kodeksu karnego skarbowego²⁶, Kodeksu postępowania w sprawach o wykroczenia²⁷, ustawy – Prawo o prokuraturze²⁸ oraz innych ustaw wyliczonych w tym przepisie.

W doktrynie wskazuje się, że przyjęte rozwiązanie powoduje istotne ograniczenie zakresu ochrony przewidzianej dyrektywą 2016/680²⁹, ponieważ część operacji przetwarzania danych osobowych realizowanych do celów rozpoznawania, wykrywania i ścigania czynów zabronionych pozostaje poza zakresem ustawowych gwarancji.

Przedstawiony problem jest jednym z wielu przykładów nieprawidłowej implementacji wskazanej dyrektywy, które mają destrukcyjny wpływ na model ochrony danych osobowych w Polsce. Z tego powodu niezwykle istotne jest skierowanie 16.03.2026 r. przez Prezesa UODO do Ministra

Spraw Wewnętrznych i Administracji oraz Ministra Sprawiedliwości kompleksowego wystąpienia o podjęcie pogłębionej analizy i prac legislacyjnych prowadzących do zmiany przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości³⁰, w którym podkreślono, że w chwili obecnej rozwiązania gwarancyjne dla podmiotów danych wynikające z tego aktu, które powinny być wprowadzone do polskiego porządku prawnego, nie funkcjonują w wielu obszarach. Dotyczy to także ochrony danych osobowych znajdujących się w aktach postępowań karnych i w sprawach o wykroczenia.

Prawidłowa implementacja dyrektywy wymagałaby nie tylko nowelizacji ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, lecz także wymusiłaby zmianę praktyki i procedur przetwarzania danych osobowych w aktach postępowań karnych. Prezes UODO, opiniując w 2024³¹ i 2025 r.³² nowelizacje przepisów Kodeksu postępowania karnego, wskazał, że obecnie przepisy tego Kodeksu nie zawierają w istocie żadnych rozwiązań regulujących ochronę danych oraz postulował rozszerzenie przepisów powołanej ustawy o rozwiązania, które pozwolą w sposób adekwatny do *ratio legis* regulacji realizować ochronę danych osobowych w toku postępowania karnego na podstawie przepisów dyrektywy 2016/680. Wskazał również, że normy Kodeksu postępowania karnego powinny zostać rozszerzone o przepisy uszczegóławiające procesy przetwarzania danych osobowych, zwłaszcza tych o charakterze sensytywnym, a także rozwiązania gwarantujące poufność i integralność tych danych. Decyzja Komisji Europejskiej o wszczęciu postępowania naruszeniowego przeciw Polsce (INFR(2026)2130) potwierdziła, że zastrzeżenia wielokrotnie zgłaszane przez Prezesa UODO, a także naukowców nie miały charakteru wyłącznie interpretacyjnego, lecz dotyczyły rzeczywistych niezgodności polskich przepisów z prawem Unii Europejskiej³³.

4. Wątpliwości odnośnie do modelu przetwarzania danych osobowych w ramach sprawowania wymiaru sprawiedliwości

W praktyce istotne wątpliwości budzi zakres pojęcia sprawowania wymiaru sprawiedliwości wynikający z RODO oraz dyrektywy 2016/680. Problem ten był przedmiotem analiz doktryny³⁴ oraz orzecznictwa Trybunału Sprawiedliwości. Szczególne znaczenie ma w tym zakresie wyrok TS z 24.03.2022 r., C-245/20, X i Z przeciwko Autoriteit Persoonsgegevens³⁵, dotyczący czasowego udostępnienia dziennikarzom pism procesowych z akt postępowania. Trybunał Sprawiedliwości uznał,

19 M. Wróblewski, A. Grzelak, *Podstawy prawne systemu...*, s. 111.

20 Opinia Prezesa Urzędu Ochrony Danych Osobowych z 18.06.2018 r. (ZWME.070.1.2018) skierowana do Pani Karoliny Ostrzyńskiej – ówczesnej Sekretarz Komitetu do Spraw Europejskich; opinia Prezesa Urzędu Ochrony Danych Osobowych z 14.08.2018 r. (ZSOŚS.11815.2018) skierowana do Pani Małgorzaty Hirszel – ówczesnej Sekretarz Stałego Komitetu Rady Ministrów.

21 Zob. G. Sibiga, *Opinia prawna dotycząca rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (druk sejmowy nr 2989), „Zeszyty Prawnicze BAS” 2018/4(60), s. 95–107.

22 Wystąpienie Prezesa Urzędu Ochrony Danych Osobowych z 7.02.2022 r., DOL.413.4.2022.WL.AG, skierowane do Ministra Spraw Wewnętrznych i Administracji.

23 Zob. Prezes UODO Mirosław Wróblewski zgłosił uwagi do projektu zmian w Kodeksie karnym i Kodeksie postępowania karnego, a także w innych ustawach związanych ze zwalczaniem przestępczości, 31.12.2024 r., <https://uodo.gov.pl/pl/138/3494> (dostęp: 5.03.2026 r.).

24 Ustawa z 6.06.1997 r. – Kodeks karny wykonawczy (Dz.U. z 2025 r. poz. 911 ze zm.).

25 Ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2026 r. poz. 490 ze zm.) – dalej k.p.k.

26 Ustawa z 10.09.1999 r. – Kodeks karny skarbowy (Dz.U. z 2025 r. poz. 633 ze zm.).

27 Ustawa z 24.08.2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. z 2025 r. poz. 860 ze zm.).

28 Ustawa z 28.01.2016 r. – Prawo o prokuraturze (Dz.U. z 2026 r. poz. 810 ze zm.).

29 A. Grzelak, M. Wróblewski [w:] *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, red. A. Grzelak, Warszawa 2019, art. 3, nb 5.

30 Wystąpienie Prezesa Urzędu Ochrony Danych Osobowych z 16.03.2026 r., DPNT.413.28.2025.

31 Opinia Prezesa Urzędu Ochrony Danych Osobowych z 5.12.2024 r. do projektu ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw, DOL.401.437.2024.OJ.

32 Opinia Prezesa Urzędu Ochrony Danych Osobowych z 23.01.2025 r. do projektu ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw, DPNT.401.2.2025.OJ, <https://legislacja.gov.pl/docs/2/12393100/13104014/13104017/dokument702620.pdf> (dostęp: 5.03.2026 r.).

33 Zob. Komisja Europejska wszczęła wobec Polski postępowanie naruszeniowe w związku z niewdrożeniem dyrektywy policyjnej, 8.07.2026 r., <https://uodo.gov.pl/pl/138/3494> (dostęp: 18.08.2026 r.).

34 P. Korzeniowski, P. Szustakiewicz, *Model prawny...*, s. 66–70.

35 EU:C:2022:216.

że takie działanie stanowi przetwarzanie danych osobowych przez sąd „w ramach sprawowania wymiaru sprawiedliwości”, a więc poza właściwością organu nadzorczego na podstawie art. 55 ust. 3 RODO. W uzasadnieniu podkreślono znaczenie motywu 20 RODO oraz potrzebę ochrony niezawisłości i niezależności sądów.

Problem ten ma wymiar nie tylko teoretyczny, lecz także praktyczny. W stanowisku z 12.10.2022 r., *Przetwarzanie danych osobowych przez sądy w kontekście zgłaszania naruszeń ochrony danych osobowych oraz kontroli w świetle regulacji unijnych i krajowych – problemy praktyczne*³⁶ Prezes UODO zwrócił uwagę, że RODO dopuszcza możliwość doprecyzowania przez prawo państwa członkowskiego operacji i procedur przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Jednocześnie przepisy ustawy – Prawo o ustroju sądów powszechnych nie wskazują wprost, że organy określone w ustawie są uprawnione do przyjmowania zgłoszeń naruszeń ochrony danych osobowych. Oznacza to, że sąd jako administrator powinien każdorazowo ocenić, czy dany incydent stanowi naruszenie ochrony danych osobowych oraz czy dotyczy przetwarzania danych w trakcie sprawowania wymiaru sprawiedliwości.

W istocie w ramach przetwarzania danych osobowych w sądach powstaje dualizm w zakresie oceny, które przypadki naruszenia danych osobowych podlegają kognicji Prezesa UODO jako niezwiązane ze sprawowaniem wymiaru sprawiedliwości, a co za tym idzie – powinny być zgłaszane do organu nadzorczego, a które wchodzą w zakres wyłącznej kontroli sądów.

Analiza prawomocnych decyzji Prezesa UODO³⁷ dotyczących przetwarzania danych osobowych w sądach pokazuje, że organ nadzorczy przyjmował brak swojej właściwości w sprawach ściśle związanych z tokiem postępowań sądowych. Dotyczyło to m.in. spraw obejmujących udostępnienie danych z akt postępowania osobie nieuprawnionej, przetwarzanie danych przez opiniodawczy zespół sądowych specjalistów czy doręczenie odpisu postanowienia osobie niebędącej stroną postępowania.

Stanowisko to znajdowało potwierdzenie w orzecznictwie sądów administracyjnych. Przykładowo w wyroku z 29.08.2019 r. Wojewódzki Sąd Administracyjny w Warszawie³⁸ oddalił skargę na decyzję Prezesa UODO umarzającą postępowanie dotyczące przetwarzania danych osobowych przez Prezesa Sądu Rejonowego, wskazując, że organ nadzorczy nie może podejmować czynności dotyczących postępowań prowadzonych przez sądy na podstawie właściwych przepisów prawa.

Jednocześnie Prezes UODO wydawał decyzje merytoryczne w sprawach, w których uznawał, że przetwarzanie danych przez sąd nie następowało w ramach sprawowania wymiaru sprawiedliwości. Dotyczyło to zwłaszcza naruszeń związanych z bezpieczeństwem przetwarzania, korzystaniem z prywatnych

lub niezabezpieczonych nośników danych oraz niewdrożeniem odpowiednich środków technicznych i organizacyjnych. W tego rodzaju sprawach organ nadzorczy stwierdzał naruszenia art. 24, art. 32 oraz art. 5 ust. 1 lit. f i art. 5 ust. 2 RODO, a w niektórych przypadkach nakładał administracyjne kary pieniężne³⁹.

Największe trudności powstają jednak w sprawach granicznych. Przykładem jest sprawa dotycząca kary pieniężnej nałożonej przez Prezesa UODO na sąd okręgowy⁴⁰ w związku z naruszeniem ochrony danych przy doręczaniu korespondencji sądowej. Kara ta została uchylona przez Wojewódzki Sąd Administracyjny w Warszawie⁴¹, a skarga kasacyjna organu nadzorczego – oddalona przez NSA⁴². Naczelny Sąd Administracyjny przyjął szerokie rozumienie działalności jurysdykcyjnej sądu, obejmujące nie tylko wydawanie orzeczeń, lecz także czynności związane z gromadzeniem materiału procesowego i zewnętrznym prowadzeniem procesu.

Tak szeroka interpretacja pojęcia sprawowania wymiaru sprawiedliwości wzmacnia ochronę niezależności sądów, ale jednocześnie nie może prowadzić do zawężenia zewnętrznego nadzoru nad przetwarzaniem danych osobowych. Ryzyko to nie ma wyłącznie krajowego charakteru. W dokumencie Europejskiej Rady Ochrony Danych (EROD) z 15.01.2026 r.⁴³, przygotowanym w ramach oceny stosowania dyrektywy 2016/680, osiem organów nadzorczych wskazało na problemy dotyczące interpretacji pojęcia „działania w ramach wymiaru sprawiedliwości” oraz wynikające z tego trudności kompetencyjne.

Z tego względu w przypadku każdego naruszenia ochrony danych osobowych, których administratorem jest sąd, konieczna jest indywidualna ocena, czy dana sytuacja wiązała się z przetwarzaniem pozostającym w funkcjonalnym związku ze sprawowaniem wymiaru sprawiedliwości. Kryterium oceny nie powinno mieć charakteru wyłącznie formalnego i nie może sprowadzać się do ustalenia, czy dane znajdują się w aktach sądowych. Decydujące znaczenie powinien mieć związek konkretnej operacji przetwarzania z niezależnym wykonywaniem zadań jurysdykcyjnych. Czynności czysto techniczne, organizacyjne, związane z bezpieczeństwem IT, zarządzaniem nośnikami danych czy zgłaszaniem naruszeń nie powinny automatycznie korzystać z wyłączenia przewidzianego w art. 55 ust. 3 RODO.

39 Zob. np. decyzja z 14.12.2025 r., DKN.5112.63.2024; decyzja z 19.01.2023 r., DKN.5131.12.2020; decyzja z 13.07.2021 r., DKN.5131.22.2021.

40 Sprawa wiązała się z dostarczeniem adresatowi przez operatora pocztowego uszkodzonej i niekompletnej korespondencji zawierającej dane osobowe, wysłanej przez Konsulat Generalny RP na wniosek Sądu Okręgowego. Więcej na temat tej sprawy zob. w tym numerze „Europejskiego Przeglądu Sądowego” O. Sętowska, *Zakres wyłączenia z art. 55 ust. 3 RODO w działalności polskich sądów. Glosa do wyroku Naczelnego Sądu Administracyjnego z 14.11.2025 r.*, III OSK 250/25.

41 Wyrok WSA w Warszawie z 13.11.2024 r., II SA/Wa 252/24, LEX nr 3829901

42 Wyrok NSA z 14.11.2025 r., III OSK 250/25, LEX nr 3964332.

43 Zob. Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive ("LED") under Article 62 LED, https://www.edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-european-commissions-evaluation-data-0_en (dostęp: 5.03.2026 r.). Treść pytania: „7.1 Have you faced any difficulties stemming from your national law or practical difficulties in supervising processing operations pursuant to Article 45 LED? Have you faced difficulties as regards the supervision of processing operations by courts when they do not act in their judicial capacity?”.

36 Publikacja *Przetwarzanie danych osobowych przez sądy w kontekście zgłaszania naruszeń ochrony danych osobowych oraz kontroli w świetle regulacji unijnych i krajowych – problemy praktyczne*, UODO, 12.10.2022 r., <https://uodo.gov.pl/pl/138/2486> (dostęp: 5.03.2026 r.).

37 Portal orzeczeń Urzędu Ochrony Danych Osobowych, <https://orzeczenia.uodo.gov.pl/search>. Zob. np. decyzja z 15.07.2019 r., ZSOŚS.440.2.2019; decyzja z 23.05.2019 r., ZSOŚS.440.50.2019; decyzja z 20.05.2019 r., ZSOŚS.440.153.2018; decyzja z 25.03.2019 r., ZSOŚS.440.3.2019.

38 Wyrok WSA w Warszawie z 29.08.2019 r., II SA/Wa 633/19, LEX nr 2778823.

5. Dane osobowe przetwarzane w aktach postępowań

Analizując problem przetwarzania danych osobowych w aktach postępowań, należy wziąć pod uwagę, że takie akta ze względu na swą specyfikę są szczególnym środowiskiem wysokiego ryzyka (*high-risk processing*) dla zawartych w nich danych.

Zgodnie z art. 53 § 1 p.u.s.p. dla każdej sprawy tworzy się akta, które mogą być prowadzone oraz przetwarzane również z wykorzystaniem technik informatycznych. Przepisy przewidują ponadto długookresowe przechowywanie akt zarówno w sądach, jak i w systemach teleinformatycznych obsługujących postępowania sądowe, a następnie przekazywanie do archiwów państwowych. Szczegółowe zasady przechowywania, archiwizacji i niszczenia akt określają przepisy wykonawcze⁴⁴. Odrębne rozwiązania funkcjonują również w sądownictwie administracyjnym⁴⁵.

W aktach postępowań znajdują się liczne informacje dotyczące osób fizycznych, których zakres wiąże się ze specyfiką danego postępowania, a także z konkretnymi czynnościami podjętymi w jego ramach. Dane osobowe zawarte są m.in. w pismach procesowych, dokumentach składanych przez strony, protokołach przesłuchań, opiniach biegłych czy materiałach przekazywanych przez organy ścigania. Niejednokrotnie informacje te pozwalają także na identyfikację osób, które formalnie nie biorą udziału w postępowaniu sądowym, ale ich dane będą występowały np. w dokumentach złożonych jako dowody w sprawie.

Szczególne ryzyka wiążą się z funkcjonowaniem e-protokołu, stanowiącego integralną część akt sprawy. Nagrania rozpraw zawierają nie tylko dane identyfikacyjne uczestników postępowania, lecz także ich wizerunek, głos oraz informacje dotyczące sytuacji osobistej, zdrowotnej lub majątkowej. Dane te są podatne na ryzyko naruszenia integralności i autentyczności, a niekiedy ich wtórnego wykorzystania w celach niezgodnych z prawem, co wpływa na ocenę adekwatności środków technicznych określonych w art. 32 RODO i konieczność uwzględnienia tych ryzyk przez administratora. Jednocześnie – ze względu na wskazane zagrożenia – rozwiązania wprowadzane i funkcjonujące w sądach związane z e-protokołem powinny być objęte oceną skutków dla ochrony danych (art. 35 RODO).

Znajdujące się w aktach informacje o osobach fizycznych będą obejmować nie tylko tzw. zwykłe dane osobowe, lecz także dane szczególnych kategorii określone w art. 9 ust. 1 RODO, których przetwarzanie bez spełnienia warunków określonych w ust. 2 tego przepisu jest zakazane. W aktach mogą być również przetwarzane informacje o osobach fizycznych dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, podlegające dodatkowej ochronie na podstawie art. 10 RODO. Jednocześnie w ramach akt postępowań sądy rutynowo operują identyfikatorami

krajowymi (w Polsce – numery PESEL) w szerokim zakresie, co rodzi pytanie o rzeczywisty poziom zabezpieczeń stosowanych wobec tych danych oraz praktyczną realizację standardu określonego w art. 87 RODO.

Akta postępowań są więc miejscem kumulacji danych osobowych o najwyższej wrażliwości, często w konfiguracjach, które w innych sektorach byłyby traktowane jako wysokiego ryzyka, wymagające szczególnych zabezpieczeń (art. 32 RODO), a mimo to reżim ich ochrony jest rozproszony i niespójny.

Jednocześnie w aktach postępowań dochodzi do nakładania się reżimów ochrony danych osobowych na podstawie RODO z danymi chronionymi na podstawie innych ustaw w ramach tajemnic prawnie chronionych, np. objętych tajemnicą lekarską czy skarbową. Jednocześnie brak jest jasnych reguł kolizyjnych w zakresie dostępu do akt.

W przypadku gdy w ramach postępowania sądowego będą miały zastosowanie przepisy ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, należy zwrócić szczególną uwagę na ochronę tzw. danych wrażliwych na podstawie art. 14 tej ustawy. Jak wskazuje Tomasz M. Miłkowski, służby od zawsze traktują takie informacje jako źródło wiedzy o powodach niektórych zachowań ludzkich lub podejmowanych decyzji, a także – jak sugeruje autor – niektóre z tych informacji mogą towarzyszyć procesom werbunkowym osobowych źródeł informacji⁴⁶. Stąd niezwykle istotne jest to, że zgodnie ze wskazanym przepisem niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej.

6. Dostęp do danych osobowych przetwarzanych w aktach postępowań i związane z nim ryzyka

Proces udostępniania danych znajdujących się w aktach sprawy w części opiera się na przepisach prawa regulujących dostęp do akt⁴⁷. Jednocześnie w sytuacjach, w których przepisy pozostawiają administratorom możliwość ograniczenia tego dostępu, konieczne jest wzięcie pod uwagę ryzyk związanych z ujawnieniem informacji znajdujących się w aktach, uwzględniając przepisy o ochronie danych osobowych. Przykładem mogą być regulacje Kodeksu postępowania cywilnego (art. 9) dotyczące praw stron i uczestników postępowania do przeglądania akt oraz uzyskiwania odpisów, kopii i wyciągów z akt sprawy. Przepisy te przewidują jednocześnie możliwość ograniczenia dostępu do zapisu obrazu i dźwięku, jeżeli przemawia za tym ważny interes publiczny lub prywatny, a w przypadku posiedzeń przy drzwiach zamkniętych – ograniczają możliwość uzyskania wyłącznie zapisu dźwięku. Również art. 525 k.p.c.

44 Rozporządzenie Ministra Sprawiedliwości z 5.03.2004 r. w sprawie przechowywania akt spraw sądowych oraz ich przekazywania do archiwów państwowych lub do zniszczenia (Dz.U. z 2022 r. poz. 1697).

45 Ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2026 r. poz. 143 ze zm.) – dalej p.p.s.a. Zob. również rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 27.05.2019 r. w sprawie sposobu postępowania z aktami spraw sądowoadministracyjnych w wojewódzkich sądach administracyjnych i Naczelnym Sądzie Administracyjnym (Dz.U. poz. 1004).

46 T.M. Miłkowski, *Czynności operacyjno-rozpoznawcze a prawa i wolności jednostki*, Warszawa 2020, rozdz. 1, pkt 6: *Ochrona danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości*, s. 100–101.

47 Przykładami mogą być: art. 9 ustawy z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2026 r. poz. 468 ze zm. – dalej k.p.c.); art. 12 p.p.s.a.; rozdział 17 k.p.k.

pozostawia przewodniczącemu możliwość oceny, czy osoba spoza postępowania dostatecznie usprawiedliwiła potrzebę dostępu do akt.

W postępowaniu karnym problem ochrony danych osobowych ma jeszcze bardziej pośredni charakter. Jak wskazuje się w doktrynie, przepisy karnoprocesowe co do zasady nie traktują ochrony danych osobowych jako samodzielnego celu regulacji procesowej, a zagadnienia te pojawiają się jedynie incydentalnie przy okazji określonych instytucji procesowych (np. art. 156a k.p.k.)⁴⁸. Samo przeglądanie akt spraw, czynienie odpisów i kserokopii zostało natomiast unormowane w art. 156 k.p.k.⁴⁹

Szczególne ryzyka pojawiają się w przypadku wniosku o udostępnienie dokumentów z akt do celów naukowych lub w ramach przepisów ustawy z 6.09.2001 r. o dostępie do informacji publicznej⁵⁰. W takich przypadkach administrator, przeprowadzając analizę danych osobowych zamieszczonych w dokumentach, które mają zostać udostępnione, powinien rozważyć dokonanie ich anonimizacji zgodnie z regułami przyjętymi w ramach danego sądu⁵¹ i przy uwzględnieniu zasady minimalizacji danych oraz zasady ograniczenia celu wynikających z art. 5 ust. 1 lit. b i c RODO. Jednocześnie anonimizacja w praktyce sądowej często ma charakter techniczny i nie zawsze eliminuje ryzyko reidentyfikacji, zwłaszcza w sprawach o wąskim kręgu uczestników postępowania sądowego.

Dostęp do akt oraz zawartych w nich danych osobowych powinien odbywać się również na podstawie odpowiednich procedur organizacyjnych opracowanych przez administratora. Procedury te powinny gwarantować prawidłowość, integralność i poufność przetwarzanych w aktach danych zgodnie z art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 24 oraz art. 32 RODO. Powinny one uwzględniać także specyfikę organizacyjną sądów, w tym brak jednolitych standardów organizacyjnych oraz rozproszenie odpowiedzialności między prezesem sądu, dyrektorem i jednostkami organizacyjnymi.

Jak podkreślają eksperci, administrator ma obowiązek ocenić „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia”, a następnie powinien wdrożyć „odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku”⁵². Ryzyka i wdrażane, aby im zapobiec, środki powinny uwzględnić realia i specyfikę sektora wymiaru sprawiedliwości, które wpływają także na zagrożenia dla danych osobowych. Analizując rejestr czynności przetwarzania danych osobowych (art. 30 RODO), w ramach którego powinny być uwzględnione czynności na danych osobowych zawartych w aktach postępowań, administrator może

zidentyfikować ryzyka dla tych danych i zastosować odpowiednie metody w celu zapobiegnięcia im.

Dużym problemem związanym z dostępem do danych znajdujących się w aktach postępowań może być nieprawidłowa anonimizacja publikowanych wyroków. Jak wynika z raportu Naczelnego Sądu Administracyjnego za 2024 r.⁵³, skargi dotyczące funkcjonowania sądów administracyjnych, które – po przeprowadzeniu postępowania wyjaśniającego przez Naczelnego Sąd Administracyjny – zostały uznane za zasadne, odnosiły się w większości do uchybień w zakresie anonimizacji orzeczeń publikowanych w CBOŚA⁵⁴ oraz problemów z dostępem do tej bazy. W raporcie podkreślono, że w sprawach zgłoszeń dotyczących nieprawidłowej anonimizacji orzeczeń publikowanych właściwy wydział Naczelnego Sądu Administracyjnego podejmował niezwłoczne działania polegające na usunięciu z bazy danych osobowych stron postępowania, zaś Inspektor Ochrony Danych NSA dokonywał dalszych czynności wynikających z przepisów o ochronie danych osobowych, w szczególności z RODO⁵⁵. Pokazuje to, że nawet częściowo zautomatyzowane procesy anonimizacji nie eliminują ryzyka ujawnienia danych osobowych i wymagają stałego nadzoru organizacyjnego oraz technicznego.

7. Ochrona danych osobowych przetwarzanych w aktach postępowań po przekazaniu do archiwów

Po przekazaniu akt postępowań sądowych do archiwów państwowych będą one podlegały ochronie na podstawie przepisów ustawy z 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach⁵⁶ jako część narodowego zasobu archiwalnego. Ustawa ta przewiduje szczególne ograniczenia dostępu do materiałów archiwalnych ze względu na ochronę dóbr osobistych oraz danych osobowych. Jednocześnie przepisy dopuszczają możliwość uchylecia tych ograniczeń w sytuacji, gdy osoba zainteresowana ma szczególne uprawnienia albo realizuje cele korzystające ze szczególnej ochrony prawnej, nadrzędne wobec ograniczeń związanych z ochroną danych osobowych lub dóbr osobistych. W doktrynie podkreśla się przy tym, że udostępnianie materiałów archiwalnych zawierających dane osobowe stanowi formę przetwarzania danych osobowych i powinno się odbywać na zasadach określonych przepisami ustawy o ochronie danych osobowych⁵⁷.

Szczególne znaczenie ma art. 22c ust. 1 u.n.z.a., który nakłada na archiwa obowiązek wdrażania zabezpieczeń służących ochronie praw i wolności osób, których dane znajdują się w materiałach archiwalnych. Ustawa przewiduje w tym zakresie m.in. anonimizację danych osobowych, pseudonimizację danych w systemach teleinformatycznych oraz zawieranie z użytkownikami zasobu archiwalnego umów wyłączających dalsze przetwarzanie danych osobowych.

Istotnym mechanizmem ochronnym jest również ograniczenie czasowe dostępu do materiałów archiwalnych obejmujących dokumentację spraw sądowych i postępowań dochodzeniowych.

48 M. Wróblewski, A. Grzelak, *Podstawy prawne...*, s. 122.

49 Artykuł 156 k.p.k. na mocy art. 38 § 1 ustawy z 24.08.2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz.U. z 2025 r. poz. 860 ze zm.) stosuje się do postępowań w sprawach o wykroczenia, a na podstawie art. 113 § 1 ustawy z 10.09.1999 r. – Kodeks karny skarbowy (Dz.U. z 2025 r. poz. 633 ze zm.) – do postępowań w sprawach o przestępstwa skarbowe i wykroczenia skarbowe.

50 Dz.U. z 2022 r. poz. 902 ze zm. – dalej u.d.i.p.

51 Przy opracowaniu rozwiązań w dotyczących anonimizacji pomocna może być w pewnym zakresie opinia Grupy Roboczej Art. 29 w sprawie technik anonimizacji z 10.04.2014 r. (Opinia 05/2014). Należy jednak uwzględnić upływ czasu, który minął od powstania tego dokumentu, a co za tym idzie – nowe technologie wykorzystywane w tej dziedzinie.

52 J. Rzymowski, *Poziomy ryzyko na gruncie RODO*, „Przegląd Prawa Publicznego” 2024/5, s. 44.

53 NSA, *Informacja o działalności sądów administracyjnych w 2024 r.*, Warszawa 2025, s. 166, <https://www.nsa.gov.pl/dokumenty/sprawozdania-roczne/> (dostęp: 5.03.2026 r.).

54 Centralna Baza Orzeczeń Sądów Administracyjnych, <http://orzeczenia.nsa.gov.pl>.

55 NSA, *Informacja...*, s. 166.

56 Dz.U. z 2020 r. poz. 164 z ze zm. – dalej u.n.z.a. lub prawo archiwalne.

57 M. Konstankiewicz [w:] M. Konstankiewicz, A. Niewęglowski, *Narodowy zasób archiwalny i archiwa. Komentarz*, Warszawa 2016, art. 16b.

Co do zasady – dokumentacja taka może być udostępniana nie wcześniej niż po 70 latach od uprawomocnienia się orzeczenia lub zakończenia postępowania (art. 16b ust. 2 pkt 4 u.n.z.a.), chyba że dostęp uzyskują podmioty uprawnione na podstawie przepisów szczególnych.

Nie oznacza to jednak całkowitego wyłączenia dostępu do dokumentów zawierających dane osobowe przed upływem tego terminu. Problem ten był przedmiotem rozważań Naczelnego Sądu Administracyjnego w wyroku z 12.11.2024 r.⁵⁸, dotyczącym odmowy udostępnienia dziennikarzowi nagrania rozprawy rewizyjnej, znajdującego się w zasobie archiwalnym Sądu Najwyższego. Naczelny Sąd Administracyjny wskazał, że żądane materiały stanowią informację publiczną, jednak ich udostępnienie podlega szczególnym regulacjom ustawy o narodowym zasobie archiwalnym i archiwach.

Na tym tle widoczne są również problemy systemowe związane z relacją między prawem archiwalnym a ustawą o dostępie do informacji publicznej. Ustawa ta poza ograniczeniem prawa do informacji publicznej ze względu na prywatność osoby fizycznej⁵⁹ nie zawiera rozbudowanych mechanizmów ochrony danych osobowych i nie została kompleksowo dostosowana do RODO. Jak zwraca uwagę Łukasz Nosarzewski, konsekwencją zaniechań polskiego prawodawcy są trudności w pogodzeniu standardów ochrony danych osobowych wynikających z RODO z krajowymi regulacjami praw informacyjnych⁶⁰. Powoduje to swoisty paradoks systemowy. Przepisy prawa archiwalnego przewidują bowiem w praktyce rozbudowane mechanizmy ochrony danych osobowych zawartych w aktach postępowań, przekazanych do archiwów, niż rozwiązania funkcjonujące na gruncie ustawy o dostępie do informacji publicznej.

Z tego względu ocena ryzyk związanych z przetwarzaniem danych osobowych zawartych w aktach postępowań sądowych powinna obejmować również etap archiwizacji dokumentacji oraz zasady jej późniejszego udostępniania. Ochrona danych osobowych nie kończy się bowiem wraz z zakończeniem postępowania sądowego, lecz pozostaje aktualna na etapie funkcjonowania dokumentacji w narodowym zasobie archiwalnym.

8. Ryzyka dla danych osobowych przetwarzanych w aktach postępowań – analiza zagrożeń i wdrożenie rozwiązań w celu ochrony danych

W celu oceny ryzyk dla danych osobowych przetwarzanych w aktach postępowań należy wziąć pod uwagę nie tylko przepisy prawne regulujące działania sądów, lecz także praktykę ich funkcjonowania, na którą składa się wiele czynników, takich jak: braki kadrowe, problemy zarządcze, niewystarczające środki finansowe.

Niektóre rozwiązania, mające usprawnić pracę sądów, określone w Regulaminie urzędowania sądów powszechnych⁶¹, generują dodatkowe ryzyka w sferze ochrony danych osobowych.

Administrator musi je uwzględnić, wprowadzając odpowiednie polityki ochrony danych, o których mowa w art. 24 ust. 2 RODO. Przykładowo rozszerzenie możliwości wynoszenia akt postępowań w celu pracy w domu na asystentów sędziów, którego dokonano w 2025 r.⁶², wymaga wdrożenia wielu rozwiązań technologicznych (odpowiednio zabezpieczony komputer) i organizacyjnych (szkolenia i kontrole przestrzegania przepisów)⁶³. Ryzyko pracy z aktami poza budynkiem sądu dotyczy też sytuacji, gdy akta mają być udostępniane biegłym, którzy również powinni stosować określone przez administratora środki techniczne i organizacyjne, zapewniające stopień bezpieczeństwa odpowiadający ryzyku związanemu z korzystaniem z akt poza siedzibą sądu. Przy określaniu zarówno sposobów przetwarzania, jak i w czasie samego przetwarzania – wdrażając odpowiednie środki techniczne i organizacyjne – administratorzy w sądach powinni uwzględniać mechanizmy ochrony danych w fazie projektowania oraz domyślnej ochrony danych, wskazane w art. 25 RODO.

Należy pamiętać, że dane osobowe mogą być zawarte w projektach pism procesowych czy kopiach dokumentów z akt postępowania. Tego typu materiały powinny być więc przenoszone na zaszyfrowanym nośniku danych tak, aby w przypadku ich zagubienia nie doszło do naruszenia danych osobowych. Rozwiązania w tym zakresie powinny gwarantować bezpieczeństwo przetwarzania tych danych zgodnie z art. 32 RODO.

W świetle zasady rozliczalności określonej w art. 5 ust. 2 RODO administrator nie może ograniczać się wyłącznie do formalnego przyjęcia procedur bezpieczeństwa. **Konieczne jest rzeczywiste i ciągłe zarządzanie ryzykiem, obejmujące monitorowanie funkcjonowania przyjętych środków organizacyjnych i technicznych, ocenę ich skuteczności oraz reagowanie na pojawiające się zagrożenia. Samo ustanowienie procedur w aktach wewnętrznych – bez ich realnego egzekwowania i kontroli – nie zapewnią zgodności przetwarzania z wymaganiami RODO.**

9. Ryzyko wtórnego wykorzystania danych audiowizualnych

Analizując ryzyka dla danych osobowych przetwarzanych w aktach postępowań, należy zwrócić uwagę na rozwój technologii, który może mieć wpływ na nowe zagrożenia ingerujące m.in. w prywatność jednostki. Takie ryzyka wiążą się obecnie z będącymi częścią akt nagraniami obrazu i dźwięku rozpraw. Przy rozwoju AI, a także technologii deepfake dopuszczenie, by osoby fizyczne mogły pozyskiwać bez kontroli nagrania z rozpraw zawierające wizerunki i nagrana głosu oraz dalej je przetwarzać, w istocie prowadzi do tego, że administrator traci jakąkolwiek kontrolę nad tymi danymi. Przepisy w tym zakresie powinny zostać zmienione poprzez wprowadzenie dodatkowych warunków udostępniania takich materiałów, z uwzględnieniem ryzyk ich nieuprawnionego wykorzystania.

Zgłaszane są też poglądy optujące za poszerzeniem zakresu udostępnienia danych w postaci wizerunku i głosu uczestników rozpraw. Przykładowo Paweł Czarnecki postuluje wprowadzenie możliwości transmisji (streamingu) rozpraw sądowych w procesie karnym, mimo że dostrzega kolizję takiego rozwiązania z przepisami mającymi na celu ochronę danych

58 Wyrok NSA z 12.11.2024 r., III OSK 966/23, LEX nr 3844020.

59 Które to ograniczenie nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Zob. art. 5 ust. 2 u.d.i.p.

60 Ł. Nosarzewski, *Ochrona danych osobowych w informacji publicznej*, „Przegląd Prawa Publicznego” 2023/6, s. 39.

61 Rozporządzenie Ministra Sprawiedliwości z 18.06.2019 r. – Regulamin urzędowania sądów powszechnych (Dz.U. z 2024 r. poz. 867 ze zm.).

62 Zob. § 137 Regulaminu urzędowania sądów powszechnych.

63 Takie rozwiązania powinny oczywiście obejmować także sędziów w przypadku wynoszenia akt poza siedzibę sądu.

osobowych⁶⁴. Zagadnienie to zostało też dostrzeżone w praktyce – Marcin Szwed, współautor raportu przygotowanego m.in. przez Helsińską Fundację Praw Człowieka, wskazuje zagrożenia dla prywatności w ramach transmisji rozpraw w internecie. Jego zdaniem nie można wykluczyć, że fragmenty wideorozpraw (zawierające np. zeznania świadka) zostaną udostępnione w mediach społecznościowych czy serwisie YouTube⁶⁵. Należy się zgodzić, że takie udostępnione fragmenty wideorozpraw mogłyby zostać przy wykorzystaniu nowych technologii zmanipulowane lub wykorzystane do innych celów przez przestępców. Przy analizie ryzyka potencjalnego wykorzystywania upublicznionego nagrania wizerunku i głosu człowieka nie powinno się brać pod uwagę jedynie obecnych możliwości technologicznych, ale również ich rozwój i przyszły potencjał.

10. Ryzyka dla danych osobowych związane z cyfryzacją oraz wdrażaniem rozwiązań opartych na sztucznej inteligencji w wymiarze sprawiedliwości

Zagadnienie przetwarzania danych osobowych w aktach postępowań jest również ściśle związane z postępującą informatyzacją wymiaru sprawiedliwości. Cyfryzacja sądów ma służyć zwiększeniu sprawności postępowań, usprawnieniu pracy sędziów i pracowników sądów oraz ułatwieniu stronom i ich pełnomocnikom udziału w postępowaniu, a przez to ułatwieniu dostępu do wymiaru sprawiedliwości. Jednocześnie rozwój systemów teleinformatycznych wykorzystywanych przez sądy prowadzi do wzrostu skali i złożoności ryzyk związanych z ochroną danych osobowych⁶⁶.

W ostatnich latach w polskim sądownictwie wdrożono wiele rejestrów i systemów teleinformatycznych, w których są przetwarzane dane osobowe, w tym m.in. e-protokół⁶⁷, EPU (e-sąd)⁶⁸, SAWA⁶⁹, Sędzia 2⁷⁰, SLPS⁷¹, ROBUS⁷² czy PI – Portal

Informacyjny⁷³. Jednocześnie trwają prace nad projektem informatycznym Cyfrowy Sąd (CySad), z którym wiązać się będzie wiele zmian w już istniejących systemach⁷⁴. Należy założyć, że w ramach rozwoju technologii informatyzacja wymiaru sprawiedliwości będzie przyspieszać, że będą realizowane nowe projekty i modyfikowane już istniejące z wykorzystaniem nowoczesnej techniki, w tym systemów sztucznej inteligencji (AI). Wymaga to pogłębionej refleksji nad metodami zagwarantowania podmiotom danych ich praw do ochrony danych osobowych i prywatności.

W celu zapobiegania ryzykom dla danych osobowych przetwarzanych w aktach postępowań w sądach działania legislacyjne, jak również projektowanie rejestrów publicznych oraz systemów teleinformatycznych powinny być zgodne zarówno z przepisami dotyczącymi ochrony danych osobowych, w tym z RODO, jak i z innymi regulacjami mającymi zapewnić cyberbezpieczeństwo przechowywanym w nich danych⁷⁵. Samo tworzenie rejestrów publicznych, w których będą przetwarzane dane osobowe w ramach sprawowania wymiaru sprawiedliwości, powinno uwzględniać takie standardy jak „Dobre praktyki AIP tworzenia rejestrów publicznych” opracowane przez Ministerstwo Cyfryzacji⁷⁶. Na konieczność stanowienia odpowiednich rozwiązań mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w rejestrach publicznych zwracał także uwagę Prezes UODO w wystąpieniu z 29.10.2025 r. dotyczącym konieczności przeglądu przepisów prawa regulujących przetwarzanie danych osobowych w rejestrach publicznych, skierowanym do Ministra Cyfryzacji⁷⁷.

Przy nieodpowiednim zaprojektowaniu rozwiązań teleinformatycznych – które nie gwarantowałyby przetwarzania w danym systemie danych osobowych w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (wbrew zasadzie integralności i poufności określonej w art. 5 ust. 1 lit. f RODO) – ryzyko naruszeń, np. w związku z atakami hakerskimi, znacznie wzrasta.

Z tego powodu w trakcie wdrażania w ramach informatyzacji wymiaru sprawiedliwości nowych rozwiązań technologicznych, wiążących się z przetwarzaniem danych osobowych mogących powodować wysokie ryzyko⁷⁸ naruszenia praw lub wolności osób fizycznych, administratorzy powinni obligatoryjnie przeprowadzać

64 P. Czarnecki, *Rozprawa sądowa w Internecie. Postulat wprowadzenia możliwości transmisji (streamingu) rozpraw sądowych w rzetelnym procesie karnym*, „Prokuratura i Prawo” 2025/3.

65 M. Szwed, *Cyfryzacja sądownictwa a art. 6 Europejskiej Konwencji Praw Człowieka* [w:] *Nowe technologie. Nowa sprawiedliwość. Nowe pytania. Wdrażanie nowych technologii w wymiarze sprawiedliwości*, red. P. Kłodzki, K. Wiśniewska, Warszawa 2021, s. 48–49.

66 S. Kotecka-Kral, *Uwagi wstępne* [w:] *E-Sąd. E-doręczenia, rozprawy zdalne, systemy teleinformatyczne w sądownictwie. Komentarz praktyczny*, red. J. Gołaczyński, A. Zalesińska, Warszawa 2024.

67 System cyfrowej rejestracji rozpraw sądowych – system składający się z urządzeń technicznych oraz oprogramowania niezbędnego do realizacji procesu rejestracji rozpraw sądowych, zarządzania nagraniami, udostępniania i przechowywania nagrań. Podstawą funkcjonowania systemu są przepisy wprowadzone na mocy Kodeksu postępowania cywilnego oraz Kodeksu postępowania w sprawach o wykroczenia.

68 Elektroniczne Postępowanie Upominawcze – system teleinformatyczny obsługujący elektroniczne postępowanie upominawcze, które zostało wprowadzone ustawą z 9.01.2009 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. Nr 26, poz. 156 ze zm.).

69 System repertoryjno-biurowy wykorzystywany przez większość jednostek organizacyjnych sądownictwa w Polsce.

70 System repertoryjno-biurowy wykorzystywany przez niektóre jednostki organizacyjne sądownictwa w Polsce.

71 System Losowego Przydziału Spraw – centralne narzędzie informatyczne dokonujące losowego przydziału spraw (w wydziałach orzeczniczych sądów powszechnych) sędziom, asesorum sądowym, referendarzom sądowym i częściowo ławnikom. Podstawą funkcjonowania systemu są przepisy art. 47a p.u.s.p. wprowadzone ustawą z 12.07.2017 r. o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw (Dz.U. poz. 1452).

72 Rejestr Osób Biorących Udział w Postępowaniach Sądowych.

73 System zapewniający obywatelowi (stronie postępowania sądowego) wgląd do aktualnego stanu sprawy.

74 Zob. Program „Cyfrowy Sąd” *zmieni wymiar sprawiedliwości*, gov.pl, 19.03.2025 r., <https://www.gov.pl/web/sprawiedliwosc/program-cyfrowy-sad-zmieni-wymiar-sprawiedliwosci> (dostęp: 5.03.2026 r.).

75 Takim jak ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20) czy rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z 11.04.2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.Urz. UE L 2024/1183, ze zm.).

76 Dobre praktyki AIP tworzenia rejestrów publicznych, Rekomendacje Ministra Cyfryzacji, wersja 1.3, 18.01.2024 r., <https://www.gov.pl/web/ia/rejestry-publiczne-dobre-praktyki-architektoniczne-i-legislacyjne> (dostęp: 5.03.2026 r.).

77 Wystąpienie Prezesa Urzędu Ochrony Danych Osobowych z 29.10.2025 r., DOL.413.11.2024.WL.OJ; zob. <https://uodo.gov.pl/pl/138/3968> (dostęp: 5.03.2026 r.).

78 Przyjęte 4.04.2017 r., ale nadal aktualne Wytyczne Grupy Roboczej Art. 29 (poprzedniczką Europejskiej Rady Ochrony Danych – EROD), dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów RODO (WP248 rev.01), wskazując na konieczność wybierania metodyki dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 do wytycznych.

test prywatności wraz z oceną skutków dla ochrony danych (art. 25 i 35 ust. 1 RODO). Andrzej Krasuski podkreśla, że prawodawca unijny, wyróżniając w przepisach RODO dwa poziomy ryzyka naruszenia praw lub wolności osób fizycznych, tj. ryzyka zwykłego i ryzyka wysokiego, w art. 35 RODO wskazuje, kiedy ryzyko mogłoby mieć postać ryzyka wysokiego⁷⁹. Jednocześnie, w świetle zasady legalizmu wskazanej w art. 5 ust. 1 lit. a RODO, przetwarzanie danych osobowych w systemach teleinformatycznych i rejestrach wykorzystywanych w sądach może być prowadzone jedynie zgodnie z wyraźną podstawą prawną.

Obecnie jedna z najbardziej kluczowych dyskusji z punktu widzenia bezpieczeństwa danych osobowych przetwarzanych w ramach wymiaru sprawiedliwości wiąże się z zastosowaniem AI przez sądy. Jak słusznie wskazują naukowcy, rozwój i implementacja AI w wymiarze sprawiedliwości to nieunikniony proces, który niesie ze sobą zarówno ogromne szanse, jak i wyzwania. Z jednej strony AI może zrewolucjonizować sposób funkcjonowania wymiaru sprawiedliwości, zwiększając jego efektywność, dostępność i obiektywizm. Z drugiej strony pojawiają się pytania dotyczące etyki, odpowiedzialności, a nawet wpływu na podstawowe prawa człowieka⁸⁰. Należy się zgodzić z tym poglądem – przy wdrażaniu rozwiązań wykorzystujących systemy AI w sądach w sposób gwarantujący ochronę danych osobowych kluczowe będzie bowiem wprowadzenie i właściwe zastosowanie aktu w sprawie sztucznej inteligencji⁸¹. Nie można przy tym pominąć, że z art. 27 AIA wynika obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych. W załączniku III AIA, w którym wymieniono systemy AI wysokiego ryzyka, w pkt 8a wskazano: „systemy AI przeznaczone do wykorzystywania przez organ wymiaru sprawiedliwości lub w jego imieniu w celu wspomagania organu wymiaru sprawiedliwości w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego lub do wykorzystywania w podobny sposób w alternatywnych metodach rozwiązywania sporów”. Oznacza to, że wdrażanie rozwiązań zakładających wykorzystanie AI w sądach będzie wymagało spełnienia wynikających z AIA warunków dokonania wcześniejszej oceny tych systemów. Jednocześnie administratorzy danych osobowych w sądach – w ramach działań organizacyjnych – powinni uwzględnić szkolenia dla sędziów, asesorów i asystentów, wskazujące na ryzyka związane z korzystaniem w sposób nieautoryzowany z systemów AI przy wykorzystaniu danych osobowych z akt postępowań.

11. Zakończenie

Sprawowanie wymiaru sprawiedliwości nieodłącznie wiąże się z przetwarzaniem dużych ilości danych osobowych,

w tym danych dotyczących szczególnie wrażliwych aspektów życia prywatnego uczestników postępowań. Dane te są jednocześnie niezbędne dla prawidłowego wykonywania funkcji jurysdykcyjnych przez sądy, co powoduje konieczność poszukiwania równowagi między ochroną niezawisłości sądownictwa a zapewnieniem skutecznej ochrony danych osobowych.

Przeprowadzona analiza wskazuje jednak, że obecny model ochrony danych osobowych w działalności sądów pozostaje nieśpójny na poziomie zarówno regulacyjnym, jak i praktycznym. Wątpliwości budzi w szczególności zakres pojęcia „sprawowania wymiaru sprawiedliwości”, wpływający na granice właściwości organu nadzorczego, a także skutki nieprawidłowej implementacji dyrektywy 2016/680 do polskiego porządku prawnego. Problemy te prowadzą do powstawania luk w ochronie danych osobowych przetwarzanych w aktach postępowań.

Szczególne znaczenie mają również ryzyka związane z postępującą cyfryzacją wymiaru sprawiedliwości, funkcjonowaniem systemów teleinformatycznych, wykorzystywaniem danych audio-wizualnych oraz wdrażaniem rozwiązań opartych na AI. Rozwój technologiczny zwiększa efektywność funkcjonowania sądów, ale jednocześnie prowadzi do wzrostu skali i złożoności zagrożeń dla prywatności oraz bezpieczeństwa danych osobowych.

Z tego względu dalsza informatyzacja sądownictwa powinna się opierać na zasadach *privacy by design* i *privacy by default* oraz uwzględniać konieczność rzeczywistego zarządzania ryzykiem przetwarzania danych osobowych. Ochrona danych osobowych w działalności sądów nie może bowiem ograniczać się wyłącznie do formalnego istnienia procedur, lecz musi stanowić integralny element organizacji i funkcjonowania współczesnego wymiaru sprawiedliwości.

Abstract

dr Olgierd Jakubowski

Criminologist; chief specialist in the Law and New Technologies
Department, Personal Data Protection Office, Poland
(ORCID: <https://orcid.org/0000-0002-5530-1025>).

Risks Related to the Processing of Personal Data in Case Files in the light of the Provisions of EU Law

Keywords: *personal data, acting in judicial capacity, tele-information systems, new technologies, computerisation*

The article refers to the issues related to the processing of personal data in case files in the context of EU law and national systemic regulations. The legal solutions applied in Poland are analysed with a special focus on issues caused by incorrect implementation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, as well as the ambiguous interpretation of the notion of acting in judicial capacity. The article also discusses the risks associated with personal data processing in case files, including threats caused by the increasing computerisation of the justice system, use of tele-information systems and new technologies. The article also points out that the current model of personal data protection in the activities of the courts is vague and requires that the boundaries of exclusion of supervision by the President of the Personal Data Protection Office are specified.

79 A. Krasuski, *Ujęcie podmiotowe i przedmiotowe ryzyka naruszenia praw lub wolności osób fizycznych* [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022, s. 74.

80 P. Dolniak, T. Kuźma, A. Ludwiński, K. Wasik, *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*, Warszawa 2024, s. 335.

81 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), (Dz.Urz. UE L 2024/1689) – dalej AIA.

Bibliografia/References

Czarnecki P., *Rozprawa sądowa w Internecie. Postulat wprowadzenia możliwości transmisji (streamingu) rozpraw sądowych w rzetelnym procesie karnym*, „Prokuratura i Prawo” 2025/3.

Dolniak P., Kuźma T., Ludwiński A., Wasik K., *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*, Warszawa 2024.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025.

Florczak-Wątor M. [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2023.

Grzelak A., *Cel i zakres podmiotowy dyrektywy 2016/680 wyzwaniami dla polskiego ustawodawcy*, „Monitor Prawniczy” 2024/11, dodatek.

Grzelak A., *Prawo pośredniego dostępu do danych na tle art. 17 dyrektywy 2016/680 – gwarancja ochrony czy iluzoryczny mechanizm? Analiza istoty i problemów implementacyjnych*, „Państwo i Prawo” 2026/5.

Grzelak A., Wróblewski M. [w:] *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, red. A. Grzelak, Warszawa 2019.

Konstankiewicz M. [w:] M. Konstankiewicz, A. Niewęglowski, *Narodowy zasób archiwalny i archiwa. Komentarz*, Warszawa 2016.

Korzeniowski P., Szustakiewicz P., *Model prawny sprawowania przez sądy administracyjne wymiaru sprawiedliwości w rozumieniu przepisów rozporządzenia RODO*, „Zeszyty Naukowe Sądownictwa Administracyjnego” 2024/4.

Kotecka-Kral S., *Uwagi wstępne* [w:] *E-Sąd. E-doręczenia, rozprawy zdalne, systemy teleinformatyczne w sądownictwie*.

Komentarz praktyczny, red. J. Gołaczyński, A. Zalesińska, Warszawa 2024.

Krasuski A., *Ujęcie podmiotowe i przedmiotowe ryzyka naruszenia praw lub wolności osób fizycznych* [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022.

Miłkowski T.M., *Czynności operacyjno-rozpoznawcze a prawa i wolności jednostki*, Warszawa 2020.

Naleziński B. [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2023.

Nosarzewski Ł., *Ochrona danych osobowych w informacji publicznej*, „Przegląd Prawa Publicznego” 2023/6.

Rzymowski J., *Poziomy ryzyka na gruncie RODO*, „Przegląd Prawa Publicznego” 2024/5.

Sętowska O., *Zakres wyłączenia z art. 55 ust. 3 RODO w działalności polskich sądów. Glosa do wyroku Naczelnego Sądu Administracyjnego z 14.11.2025 r., III OSK 250/25*, „Europejski Przegląd Sądowy” 2026/8.

Sibiga G., *Opinia prawna dotycząca rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy nr 2989)*, „Zeszyty Prawnicze BAS” 2018/4(60).

Szwed M., *Cyfryzacja sądownictwa a art. 6 Europejskiej Konwencji Praw Człowieka* [w:] *Nowe technologie. Nowa sprawiedliwość. Nowe pytania. Wdrażanie nowych technologii w wymiarze sprawiedliwości*, red. P. Kładoczny, K. Wiśniewska, Warszawa 2021.

Wróblewski M., Grzelak A., *Podstawy prawne systemu ochrony danych osobowych* [w:] *Ochrona danych osobowych w sądach i prokuraturze*, red. A. Grzelak, Warszawa 2019.

REKLAMA



KONSTYTUCJA DLA INTERNETU OKIEM EKSPERTÓW

Książka omawia przepisy Aktu o usługach cyfrowych (DSA) od strony praktycznej – z uwzględnieniem aktualnego dorobku nauki polskiej i zagranicznej. Czytelnik znajdzie tu zmiany, jakie wprowadza DSA w stosunku do wcześniejszych regulacji. Unikalną wartością komentarza jest uwzględnienie polskiego projektu ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną.

Autorzy szczegółowo opisują nowe regulacje dotyczące m.in.:

- obowiązku moderowania nielegalnych treści w Internecie przez platformy typu Facebook czy Google,
- wprowadzania obowiązkowej oceny ryzyka i większej przejrzystości algorytmów, co pomoże w walce ze szkodliwymi treściami w sieci.

Książka przeznaczona jest przede wszystkim dla prawników praktyków, w tym sędziów, adwokatów, prokuratorów, radców prawnych, a także pracowników administracji oraz pracowników naukowych.

**ZAMÓW KSIĄŻKĘ Z RABATEM 20% W KSIĘGARNI PROFINFO.PL
W FORMULARZU ZAMÓWIENIA WPISZ KOD: WKCZA20**

AKT O USŁUGACH CYFROWYCH

Komentarz

redakcja naukowa Jacek Gołaczyński, Rafał Skibicki

Gabriela Bar, Kamila Brylak, Witold Chomiczewski, Wojciech Dubis
Maria Dymitruk, Krzysztof Garstka, Aleksandra Glanc-Gołaczyńska
Jacek Gołaczyński, Łukasz Goździaszek, Jarosław Greser, Bartosz Kolarz
Aleksandra Kuczerawy, Wojciech Lamik, Joanna Lentka-Wróbel
Martyna Mielniczuk-Skibicka, Magdalena Piech, Przemysław Polański
Patricia Sharp, Rafał Skibicki, Jędrzej Stępniewski, Agnieszka Sztoldman

KOMENTARZE PRAKTYCZNE

Wolters Kluwer