Katarzyna Siemion

- Uniwersytet w Białymstoku
(University of Bialystok, Poland)
- e-mail: k.siemion@uwb.edu.pl
- ORCID: 0000-0003-4758-5512

DOI: 10.15290/mhi.2025.24.02.36

KSZTAŁTOWANIE SIĘ STATUSU PRAWNEGO INSPEKTORA OCHRONY DANYCH W POLSCE

Abstrakt

Status prawny inspektora ochrony danych ewoluował na przestrzeni poszczególnych lat obowiązywania przepisów o ochronie danych osobowych. Artykuł omawia, w jaki sposób się on kształtował i zmieniał od wprowadzenia funkcji administratora bezpieczeństwa informacji w przepisach prawa polskiego aż po wprowadzenie bezpośrednio obowiązujących na szczeblu unijnym przepisów RODO regulujących status prawny inspektora ochrony danych. Od 2018 roku kwestie dotyczące ochrony danych osobowych są bowiem głównie regulowane przez prawo unijne.

Artykuł omawia kwestie dotyczące powołania, zadań oraz innych wymogów mających na celu zapewnienie prawidłowego ich wykonywania przez osoby pełniące tę funkcję. Za hipotezę badawczą przyjęto założenie, że status prawny inspektora ochrony danych ewoluował w czasie, a jego status obecnie ma charakter mieszany (wewnętrzno-zewnętrzny). Artykuł przedstawia istotne wytyczne w zakresie wykładni przepisów prawa dotyczących ochrony danych osobowych w omawianym zakresie oraz dobre praktyki w zakresie stosowania przepisów prawa w praktyce.

W artykule wykorzystano metody dogmatycznoprawną i historycznoprawną oraz metodę analizy orzecznictwa, decyzji organu nadzorczego oraz wytycznych i opinii wydawanych przez organy zajmujące się ochroną danych osobowych w Polsce i w Unii Europejskiej, które miały na celu weryfikację hipotezy badawczej przedstawionej

w artykule. Artykuł ma istotne znaczenie dla prawidłowego określenia statusu prawnego inspektora ochrony danych, co wpływa na interesy osób wykonujących ten zawód, ale także ma wpływ na realizację obowiązków nałożonych na administratorów danych osobowych oraz podmioty przetwarzające, które zatrudniają takie osoby.

Słowa kluczowe: dane osobowe, inspektor ochrony danych osobowych, status prawny, ochrona danych osobowych

THE DEVELOPMENT OF THE LEGAL STATUS OF THE DATA PROTECTION OFFICER IN POLAND

Abstract

The legal status of the Data Protection Officer has evolved since the introduction of personal data protection regulations. This article discusses how this role has developed and changed since the introduction of the Information Security Administrator function in Polish law, up to the introduction of the directly applicable GDPR regulations governing the legal status of the Data Protection Officer. Since 2018, issues relating to personal data protection have been mainly regulated by EU law.

The article discusses issues related to the appointment, tasks and other requirements aimed at ensuring the proper performance of their tasks by persons holding this position. The research hypothesis assumes that the legal status of the Data Protection Officer has evolved over time and is currently of a mixed nature (internal-external). It presents important guidelines for interpreting legal provisions concerning the protection of personal data in the discussed area, as well as good practices for applying legal provisions in practice.

The article employs dogmatic-legal, historical-legal and case law analysis methods, as well as analysing decisions made by supervisory authorities, and guidelines and opinions issued by bodies responsible for personal data protection in Poland and the European Union. These methods were employed to verify the research hypothesis presented in the article. This article is of significant importance in determining the legal status of Data Protection Officers, affecting the interests of those in this profession and the fulfilment of obligations imposed on Personal Data Controllers and Processors who employ them.

Keywords: personal data, Data Protection Officer, legal status, personal data protection

1. Wprowadzenie

Artykuł ma na celu zaprezentowanie, jak kształtował się status prawny inspektora ochrony danych w Polsce. Jest to istotne z tego względu, że podlegał on zmianom na przestrzeni lat w kontekście regulacji prawnych o ochronie danych osobowych. Prawidłowe jego określenie ma znaczenie dla całej grupy zawodowej, która pełniła, pełni obecnie lub będzie w przyszłości pełnić taką funkcję w organizacji przetwarzającej dane osobowe, a także dla wszystkich administratorów danych osobowych i podmiotów przetwarzających zatrudniających takie osoby w swoich organizacjach.

W artykule postawiono tezę, że status prawny inspektora ochrony danych ewoluował w czasie, a obecnie ma charakter mieszany (wewnętrzno-zewnętrzny).

Poniżej zostaną poruszone kwestie dotyczące: 1) statusu prawnego administratora bezpieczeństwa informacji, 2) wprowadzenia przepisów dotyczących funkcji inspektora ochrony danych, 3) relacji pomiędzy funkcją administratora bezpieczeństwa informacji a inspektora ochrony danych oraz 4) statusu prawnego inspektora ochrony danych w aktualnie obowiązujących przepisach prawa.

W artykule wykorzystano metodę dogmatycznoprawną w celu analizy i przedstawienia przepisów prawa powszechnie obowiązującego dotyczących ochrony danych osobowych oraz regulujących status prawny administratora bezpieczeństwa informacji, a następnie inspektora ochrony danych. Ponadto zastosowano metodę historycznoprawną, która posłużyła do zaprezentowania, jak na przestrzeni poszczególnych lat i obowiązujących regulacji prawnych zmieniał się ich status prawny. Wykorzystano także metodę analizy orzecznictwa i decyzji organów nadzorczych, celem wskazania praktyki stosowania prawa w tym zakresie. Dodatkowo wykorzystano opinie i wytyczne wydawane przez organy nadzorcze, Grupę Roboczą Art. 29 (obecnie: Europejską Radę Ochrony Danych), które wyjaśniają szczegółowe problemy praktyczne w omawianym zakresie oraz opracowują dobre praktyki w zakresie określonych kwestii związanych z procesami przetwarzania danych osobowych.

2. Wprowadzenie do przepisów prawa funkcji administratora bezpieczeństwa informacji oraz jego status prawny

W Polsce pierwszym aktem prawnym regulującym kompleksowo kwestie dotyczące ochrony danych osobowych była ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[1]. Stanowiła ona implementację dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2]. Regulowała ona w szczególności podstawowe zasady przetwarzania danych osobowych, prawa podmiotów danych oraz obowiązki podmiotów przetwarzających dane osobowe, w szczególności administratora danych osobowych[3].

Jednak dopiero w 2014 roku wprowadzono do tej ustawy przepisy dotyczące administratora bezpieczeństwa informacji, które weszły w życie od 1 stycznia 2015 roku[4]. Ustawa określiła przede wszystkim zadania, jakie powinny być wykonywane przez administratora bezpieczeństwa informacji. Przede wszystkim miał on zapewnić przestrzeganie przepisów o ochronie danych osobowych w organizacji, w szczególności poprzez: 1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych osobowych, 2) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych oraz przestrzegania zasad w niej określonych, 3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Ponadto administrator bezpieczeństwa informacji miał obowiązek prowadzenia rejestru zbiorów danych przetwarzanych przez administratora danych osobowych. W takiej sytuacji administrator danych osobowych był zwolniony z obowiązku rejestracji zbiorów w organie nadzorczym (czyli u Generalnego Inspektora Ochrony Danych Osobowych).

1 Dz.U. 1997 nr 133, poz. 882 i 883, z późn. zm.
2 Dz.U. L 1995 nr 281, poz. 31.
3 M. Odlanicka-Poczobutt, A. Szyszka-Schuppik, *Bezpieczeństwo danych osobowych w świetle nowych przepisów (RODO) – przegląd historyczny,* „Zeszyty Naukowe Politechniki Śląskiej" 2018, z. 118, s. 421.
4 Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. 2014, poz. 1662).

Szczegółowe kwestie dotyczące trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji określało rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[5].

Ustanowienie tej funkcji w organizacji było fakultatywne dla administratorów danych osobowych. To znaczy, że mogli powołać w swojej organizacji osobę pełniącą taką funkcję, ale nie musieli tego robić. Co jednak istotne, w przypadku niepowołania administratora bezpieczeństwa informacji zadania określone powyżej, z wyłączeniem obowiązku sporządzania sprawozdania, miał wykonywać samodzielnie administrator danych osobowych[6]. Co za tym idzie, administrator bezpieczeństwa informacji był podmiotem, na który miał być przełożony ciężar wykonywania obowiązków ciążących na administratorze danych osobowych. Dlatego też postulowano, aby administratorzy danych osobowych, którzy nie posiadali odpowiedniej wiedzy i kompetencji w zakresie ochrony danych osobowych, powoływali lub zatrudniali osobę, która się tym odpowiednio zajmie, a więc administratora bezpieczeństwa informacji[7].

W przypadku powołania administratora bezpieczeństwa informacji konieczne było jego zgłoszenie do Generalnego Inspektora Ochrony Danych Osobowych[8]. Wzory zgłoszeń regulowały przepisy rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 roku w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[9].

5 Dz.U. 2015, poz. 745, z późn. zm.

6 P. Fajgielski, *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Monitor Prawniczy" 2015, dodatek do nr 6, s. 3. Zob. szerzej: M. Byczkowski, *Zapewnianie przestrzegania przepisów o ochronie danych osobowych w sferze wewnętrznej bez powołania administratora bezpieczeństwa informacji*, „Monitor Prawniczy" 2015, dodatek do nr 6, s. 8–12.

7 K. Wygoda, *Powoływanie Administratora Bezpieczeństwa Informacji jako zasada bezpiecznego przetwarzania danych na gruncie ustawy o ochronie danych osobowych*, „Przegląd Prawa i Administracji" 2015, nr 100, s. 338–339.

8 Zob. szerzej: G. Sibiga, *Rejestracja administratorów bezpieczeństwa informacji. Postępowanie rejestracyjne Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy" 2015, dodatek do nr 6, s. 13–19.

9 Dz.U. 2014, poz. 1934, z późn. zm.

Przepisy prawa określały również wymagane kwalifikacje osoby na tym stanowisku. Były to: 1) posiadanie pełnej zdolności do czynności prawnych oraz korzystanie z pełni praw publicznych, 2) posiadanie odpowiedniej wiedzy w zakresie ochrony danych osobowych oraz 3) niekaralność za umyślne przestępstwo (art. 36a ust. 4).

Administrator danych osobowych miał obowiązek zapewnić prawidłowe wykonywanie funkcji przez administratora bezpieczeństwa informacji. Przede wszystkim administrator bezpieczeństwa informacji powinien podlegać bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych osobowych, a także powinien mieć zapewnione środki i organizacyjną odrębność niezbędną do niezależnego wykonywania swoich zadań[10].

Wskazuje się, że administrator bezpieczeństwa informacji mógł być zatrudniony w organizacji na podstawie umowy o pracę, jak też stosunku służbowego administracyjnoprawnego[11]. Możliwe było powierzenie mu przez administratora danych osobowych wykonywania innych obowiązków, z zastrzeżeniem, że nie mogło to naruszać prawidłowego wykonywania zadań w ramach powierzonej funkcji, które miały niejako pierwszeństwo[12].

3. Wprowadzenie do przepisów prawa funkcji inspektora ochrony danych

Funkcja inspektora ochrony danych została wprowadzona przez przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[13]. Przepisy te rozpoczęły stosowanie od 25 maja 2018 roku.

10 R. Szałowski, *Administrator bezpieczeństwa informacji*, „Ius Novum" 2016, nr 4, s. 210.

11 Zob. szerzej: J. Borowicz, *Z problematyki zatrudnienia administratora bezpieczeństwa informacji*, „Praca i Zabezpieczenie społeczne" 2016, nr 12, s. 16–25.

12 K. Wygoda, *Administrator Bezpieczeństwa Informacji a Inspektor Ochrony Danych na tle regulacji krajowych i unijnych – wybrane zagadnienia*, „Przegląd Prawa i Administracji" 2016, nr 105, s. 223.

13 Dz.U. L 2016 nr 119, poz. 1, dalej jako: RODO.

RODO określiło jego status prawny, w tym obowiązek powołania w określonych sytuacjach osoby pełniącej taką funkcję w organizacji oraz jej zadania. Kwestie te regulują przepisy art. 37–39 RODO.

Z uwagi na to, że przepisy te – jako przepisy rozporządzenia unijnego – mają charakter bezpośrednio obowiązujący we wszystkich państwach członkowskich Unii Europejskiej, dotychczasowa ustawa o ochronie danych osobowych z 1997 roku została zastąpiona przez ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych[14]. Ustawa ta zmieniła niejako swoją funkcję, ponieważ obecnie ma charakter jedynie uzupełniający przepisy RODO. Określa kwestie, które ustawodawca unijny pozostawił do samodzielnego uregulowania przez ustawodawców poszczególnych państw członkowskich[15].

Jednocześnie w przepisach przejściowych i końcowych w/w ustawy uregulowano kwestie związane ze statusem prawnym inspektora ochrony danych. Zgodnie z treścią art. 158 ustawy osoby pełniące w dniu 24 maja 2018 roku (a więc w przeddzień rozpoczęcia stosowania przepisów RODO) funkcję administratora bezpieczeństwa informacji stały się inspektorem ochrony danych. Miały pełnić swoją funkcję do dnia 1 września 2018 roku, chyba że przed tym dniem administrator danych osobowych zawiadomił organ nadzorczy, tj. Prezesa Urzędu Ochrony Danych Osobowych, o wyznaczeniu innej osoby na to stanowisko. Co za tym idzie, doszło do automatycznego, wynikającego z przepisów prawa, przekształcenia funkcji administratora bezpieczeństwa informacji w funkcję inspektora ochrony danych[16].

---

14 T.j. Dz.U. 2019, poz. 1781.

15 P. Fajgielski, *Komentarz do art. 1*, [w:] *Komentarz do ustawy o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* wyd. II, Warszawa 2022, LEX, t. 3; D. Lubasz, U. Góral, *Komentarz do art. 1*, [w:] E. Bielak-Jomaa, I. Bogucka, W. Chomiczewski, P. Drobek, M. Gawroński, K. Kloc, J. Łuczak-Tarka, P. Punda, N. Zawadzka, M. Żmijewski, D. Lubasz, U. Góral, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, LEX, t. 1. Zob. szerzej: G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia*, [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, red. G. Sibiga, Warszawa 2016, s. 18 i n.; P. Kozik, *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 18–22.

16 R. Brodzik, *Komentarz do art. 158*, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018, LEX, t. 5.

Z załącznika dotyczącego oceny skutków regulacji do projektu ustawy o ochronie danych osobowych wynika, że w Polsce w 2018 roku było 25 357 osób pełniących funkcję administratora bezpieczeństwa informacji[17]. Wraz z wejściem w życie przepisów RODO liczba ta miała się zwiększyć z uwagi na wprowadzenie w określonych sytuacjach obowiązku powołania inspektora ochrony danych, o czym będzie szerzej w dalszej części artykułu[18].

Ponadto wskazano, że osoby, które stały się inspektorem ochrony danych na podstawie w/w regulacji, mogły pełnić swoją funkcję także po dniu 1 września 2018 roku, jeżeli do tego dnia administrator danych osobowych zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o ich wyznaczeniu w sposób określony w przepisach ustawy.

Jednocześnie wskazano, że osoba pełniąca funkcję administratora bezpieczeństwa informacji mogła zostać odwołana przez administratora danych osobowych bez zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu innej osoby na inspektora ochrony danych. Mogło to mieć miejsce w przypadku, gdy administrator danych osobowych nie był na podstawie przepisów prawa obowiązany do wyznaczenia inspektora ochrony danych. Natomiast podmioty przetwarzające oraz administratorzy danych osobowych, którzy nie mieli powołanego administratora bezpieczeństwa informacji przed rozpoczęciem stosowania przepisów RODO, a na ich podstawie mieli taki obowiązek, musieli to zrobić do dnia 31 lipca 2018 roku.

4. Powołanie inspektora ochrony danych osobowych

W treści art. 37 ust. 1 RODO przewidziano sytuacje, w których powołanie inspektora ochrony danych jest obowiązkowe. Dotyczy to następujących sytuacji: 1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości, 2) główna działalność administratora danych osobowych lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego

17 Ocena skutków regulacji do projektu ustawy o ochronie danych osobowych z dnia 27 marca 2018 r., druk 2410, s. 18, https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410 (dostęp: 15.06.2025).

18 Ibidem, s. 18–19.

i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub 3) główna działalność administratora danych osobowych lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

Przepisy ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych doprecyzowują, jakie organy lub podmioty publiczne są zobowiązane do powołania inspektora ochrony danych. Zgodnie z treścią art. 9 ustawy organami publicznymi zobowiązanymi do powołania inspektora ochrony danych są: 1) jednostki sektora finansów publicznych, 2) instytuty badawcze, 3) Narodowy Bank Polski. Należy zatem uznać, że polski ustawodawca nie wprowadził w tej ustawie definicji legalnej pojęć organów i podmiotów publicznych, lecz jedynie doprecyzował, jakie organy i podmioty publiczne zostały zobowiązane do powołania inspektora ochrony danych[19]. Należy uznać tak przyjęte rozwiązanie za prawidłowe, aby zapewnić, że podmioty te realizują obowiązki wynikające z przepisów o ochronie danych osobowych oraz prawidłowo chronią prawa i wolności obywateli. Jednak biorąc pod uwagę najczęściej ograniczone możliwości finansowe i dyscyplinę finansów publicznych, dużym wyzwaniem może być pozyskanie do sprawowania tej funkcji specjalistów z dziedziny ochrony danych osobowych.

Drugim przypadkiem, gdy powołanie inspektora ochrony danych jest obowiązkowe, jest sytuacja, gdy dochodzi do 1) regularnego i systematycznego monitorowania osób, których dane dotyczą, 2) na dużą skalę, 3) w ramach głównej działalności administratora danych osobowych lub podmiotu przetwarzającego. Są to sformułowania o charakterze niedookreślonym, co z jednej strony może powodować wątpliwości praktyczne w zakresie ich stosowania, jednak z drugiej strony pozwala na pewną elastyczność i odporność na zmieniające się warunki przetwarzania danych osobowych.

Wskazuje się, że regularne i systematyczne monitorowanie będzie miało miejsce w przypadku stałego lub czasowego, cyklicznego śledzenia lub monitorowania zachowania osób, które jest zorganizowane lub występuje zgodnie z określonym

[19] D. Kuźnicka-Błaszkowska, *Organy samorządu gminnego a organ publiczny i podmiot publiczny w RODO*, „Finanse Komunalne" 2024, nr 4, s. 13.

systemem[20]. Przy określaniu pojęcia dużej skali należy brać pod uwagę liczbę osób, których dane dotyczą, zakres przetwarzanych danych osobowych, okres, przez jaki dane mają być przechowywane, oraz zakres geograficzny przetwarzania danych osobowych[21]. Natomiast główna działalność administratora danych osobowych lub podmiotu przetwarzającego powinna być rozumiana jako działalność podstawowa, która głównie jest przez niego wykonywana. Może to dotyczyć np. monitoringu miejskiego lub aplikacji śledzących wykorzystywanych przez dużą grupę odbiorców.

Trzecim przypadkiem, gdy powołanie inspektora ochrony danych jest obowiązkowe, jest sytuacja, w której główna działalność administratora danych osobowych lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz danych genetycznych i biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby) lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych. Może to mieć zastosowanie np. do szpitali czy też ubezpieczycieli.

W innych sytuacjach niż wskazane powyżej powołanie inspektora ochrony danych jest fakultatywne. Oznacza to, że decyzja co do jego powołania pozostaje po stronie administratora danych osobowych lub podmiotu przetwarzającego. Zatrudnienie w organizacji osoby pełniącej taką funkcję należy uznać za dobrą praktykę i działanie niewątpliwie pożądane, ułatwiające spełnienie przez organizacje obowiązków wynikających z przepisów o ochronie danych osobowych.

Tak jak było w przypadku administratora bezpieczeństwa informacji, także w przypadku inspektora ochrony danych konieczne jest jego formalne powołanie[22]. Podmiot, który powołał osobę do pełnienia tej funkcji, ma obowiązek zawiadomienia o tym Prezesa Urzędu Ochrony Danych Osobowych. Powinno to nastąpić w terminie 14 dni

20 Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243), wersja po zmianach z dnia 5 kwietnia 2017 r., s. 9–10, https://ec.europa.eu/newsroom/article29/items/612048/en (dostęp: 15.06.2025).

21 Ibidem, s. 9–10.

22 Decyzja PUODO z dnia 18 października 2024 r., DKN.5131.7.2024, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).

od dnia jego wyznaczenia, np. powołania czy zawarcia umowy o pracę lub współpracy. Konieczne jest przy tym wskazanie imienia, nazwiska oraz adresu poczty elektronicznej lub numeru telefonu inspektora ochrony danych oraz danych administratora danych osobowych albo podmiotu przetwarzającego. Zawiadomienia wymaga także każda zmiana w/w danych oraz odwołanie danej osoby z tej funkcji. W takiej sytuacji powinno się to odbyć w terminie 14 dni od dnia zaistnienia zmiany. Sporządzenie zawiadomienia odbywa się w postaci elektronicznej. Opatruje się je kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Niezależnie od zawiadomienia organu nadzorczego podmiot, który wyznaczył inspektora ochrony danych, powinien udostępnić jego dane na swojej stronie internetowej lub – w przypadku jej braku – w sposób dostępny w miejscu prowadzenia działalności (np. na tablicy ogłoszeń)[23]. Dane inspektora ochrony danych powinny bowiem być łatwo dostępne dla osób, których dane są przetwarzane w ramach danej organizacji, aby mogły się one z nim bezpośrednio skontaktować[24].

5. Zadania inspektora ochrony danych

Przepisy RODO w art. 39 określają zadania inspektora ochrony danych. Są to: 1) informowanie administratora danych osobowych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach, 2) monitorowanie przestrzegania tych przepisów oraz polityk administratora danych osobowych lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych oraz powiązane z tym audyty, 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO, 4) współpraca z organem nadzorczym, 5) pełnienie funkcji punktu kontaktowego dla organu

[23] *Czy administrator musi podać imię i nazwisko IOD na stronie internetowej?*, https://uodo.gov.pl/pl/495/2345 (dostęp: 16.06.2025).

[24] *Czy dane kontaktowe IOD muszą być łatwo dostępne?*, https://uodo.gov.pl/pl/495/2342 (dostęp: 16.06.2025).

nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz, w stosownych przypadkach, prowadzenie konsultacji we wszelkich innych sprawach.

Administrator danych osobowych może powierzyć inspektorowi ochrony danych wykonywanie także innych zadań, jeżeli nie stoją one w sprzeczności z jego statusem prawnym. Dopuszcza się możliwość udziału inspektora ochrony danych przy przygotowaniu dokumentacji wewnętrznej dotyczącej ochrony danych osobowych w organizacji, takiej jak rejestry przetwarzania danych osobowych lub polityk ochrony danych. Jednak należy mieć na uwadze to, że wdrożenie odpowiedniej dokumentacji jest obowiązkiem administratora danych osobowych i to on powinien ponosić odpowiedzialność za jej treść. Nie jest możliwe, żeby to inspektor ochrony danych był w całości odpowiedzialny za jej opracowanie i wdrożenie, ponieważ może to powodować konflikt interesów, o którym będzie mowa poniżej[25].

Podobna rola inspektora ochrony danych widoczna jest w zakresie naruszeń bezpieczeństwa danych osobowych. Przyjmuje się, że powinien on monitorować proces obsługi naruszeń, udzielać wskazówek dotyczących prawidłowego reagowania na naruszenie, doradzać w zakresie przygotowania dokumentacji dotyczącej naruszenia oraz przekazywać dodatkowe informacje o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą. Nie jest to podmiot, który powinien zgłaszać naruszenie do organu nadzorczego, zawiadamiać osoby, których dane zostały naruszone, czy podejmować zobowiązania dotyczące bezpieczeństwa przetwarzania w imieniu administratora danych osobowych[26]. Są to obowiązki ciążące bezpośrednio na administratorze danych osobowych. W tym zakresie przejawia się również wewnętrzno-zewnętrzny charakter funkcji inspektora ochrony danych. Pełni on bowiem wewnętrznie jedynie funkcje doradcze wobec administratora danych osobowych. Zewnętrzny charakter jego funkcji przejawia się przede wszystkim w zadaniu bycia punktem kontaktowym dla organu nadzorczego weryfikującego dokonane zgłoszenie naruszenia oraz dla podmiotów danych, co ma zapewnić ochronę ich praw i wolności.

25 Zob. szerzej: *Vademecum Inspektora Ochrony Danych*, red. M. Kołodziej, Warszawa 2020, s. 16–18.

26 *Poradnik na gruncie RODO. Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, v. 2*, s. 40–41, https://uodo.gov.pl/pl/138/3561 (dostęp: 26.10.2025).

Co istotne, inspektor ochrony danych powinien wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. W praktyce oznacza to, że powinien ustalić priorytety w swojej pracy i określić środki i metody działania dostosowane do specyfiki konkretnego administratora, u którego pełni tę funkcję. Powinien najbardziej koncentrować się na aspektach o największym ryzyku w zakresie ochrony danych osobowych i w tym kontekście przede wszystkim doradzać administratorowi danych osobowych, jaką metodologię zastosować przy ocenie skutków dla ochrony danych osobowych, które obszary należy poddać audytowi wewnętrznemu lub zewnętrznemu, jakie szkolenia dla pracowników przeprowadzić i na które operacje przetwarzania przeznaczyć najwięcej czasu oraz zasobów[27].

Mając na uwadze wyżej wymienione zadania, należy wskazać, że różnią się one od zadań nałożonych na podstawie wcześniej obowiązujących przepisów na administratora bezpieczeństwa informacji. Inspektor ochrony danych pełni funkcję mieszaną, tj. z jednej strony informuje i doradza administratorowi danych osobowych lub podmiotowi przetwarzającemu oraz ich pracownikom, czyli prowadzi działania wewnętrzne na rzecz tych podmiotów. Jednak ma też obowiązek monitorować przestrzeganie przez te podmioty przepisów o ochronie danych osobowych oraz pełnić funkcję punktu kontaktowego dla podmiotów danych[28], a także współpracować z Prezesem Urzędu Ochrony Danych Osobowych. Pełni zatem w pewien sposób funkcje nadzorcze oraz zewnętrzne wobec organizacji[29].

Co za tym idzie, inspektor ochrony danych nie jest osobą powołaną do wykonywania w imieniu administratora danych osobowych lub podmiotu przetwarzającego ich obowiązków, ale podmiotem doradczym i monitorującym wewnętrznie spełnianie przez nich wymogów dotyczących ochrony danych osobowych. Jednoczesne wykonywanie w imieniu administratora danych osobowych lub podmiotu przetwarzającego nałożonych na nich obowiązków, jak również monitorowanie

27 Wyrok Naczelnego Sądu Administracyjnego z dnia 7 lutego 2025 r., III OSK 6801/21, LEX nr 3833096; Decyzja PUODO z dnia 21 sierpnia 2020 r., ZSOŚS.421.25.2019, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).

28 Zob. szerzej: M. Młotkiewicz, *IOD jako punkt kontaktowy*, „ABI EXPERT" 2018, nr 2, s. 20–21.

29 W. Kupny, *Rola inspektora ochrony danych w strukturze organizacji,* „Roczniki Administracji i Prawa" 2019, nr 19(1), s. 279.

prawidłowego ich wykonywania może stanowić konflikt interesów, bowiem w takiej sytuacji inspektor ochrony danych monitorowałby swoje własne działania[30].

W mojej ocenie jest to istotna zmiana w kontekście statusu prawnego inspektora ochrony danych w porównaniu do poprzednio obowiązujących przepisów i statusu prawnego administratora bezpieczeństwa informacji. Administrator bezpieczeństwa informacji pełnił głównie funkcje wewnętrzne, jako podmiot powołany do pomagania administratorowi danych osobowych w wypełnianiu nałożonych na niego obowiązków w zakresie ochrony danych osobowych[31]. Przepisy RODO nałożyły na inspektora ochrony danych również nowe obowiązki, wcześniej nieznane administratorowi bezpieczeństwa informacji. Dotyczy to w szczególności takich działań jak udzielanie zaleceń co do oceny skutków dla ochrony danych czy też pełnienie roli punktu kontaktowego dla organu nadzorczego oraz dla osób, których dane dotyczą[32].

Osoba pełniąca funkcję inspektora ochrony danych może być zatrudniona wewnątrz organizacji, jako jej pracownik, jak również może pełnić tę funkcję zewnętrznie. Co jednak istotne, należy wybrać taką formę współpracy, która będzie w największym stopniu pozwalać realizować prawidłowo powierzone mu zadania (art. 37 ust. 6 RODO). Inspektor ochrony danych może w organizacji wykonywać inne zadania niż te związane z ochroną danych osobowych, jednak zadania te i obowiązki nie mogą powodować konfliktu interesów[33]. Jak wskazał TSUE w wyroku z 9 lutego 2023 roku, konflikt interesów w rozumieniu tego przepisu może istnieć w sytuacji, gdy osoba będąca inspektorem ochrony danych otrzymuje inne zadania lub obowiązki, które prowadzą

30 Wyrok TSUE z dnia 9 lutego 2023 r., C-453/21 ws. X-FAB DRESDEN GMBH & CO. v. FC, LEX nr 3483231; Decyzja PUODO z dnia 22 września 2020 r., ZWAD.405.31.331.2019, https://orzeczenia.uodo.gov.pl (dostęp: 16.06.2025).

31 Zob. szerzej: M. Chodorowski, *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych) w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 141–158.

32 Czy inspektor ochrony danych powinien być wyznaczany na podstawie takich samych kwalifikacji jak było to w przypadku administratora bezpieczeństwa informacji?, https://uodo.gov.pl/pl/497/200 (dostęp: 16.06.2025).

33 Zob. szerzej: G. Sibiga, *Opinia prawna – Konflikt interesów w wykonywaniu funkcji inspektora ochrony danych i jego unikanie. Problemy zaistniałe w praktyce i sposoby ich rozwiązania*, Warszawa 2024, https://sabi.org.pl (dostęp: 26.10.2025).

do określania przez nią celów i sposobów przetwarzania danych osobowych u administratora lub jego podmiotu przetwarzającego. Jednocześnie istnienie konfliktu interesów należy ustalać odrębnie w każdym przypadku, z uwzględnieniem wszystkich okoliczności, w tym struktury organizacyjnej administratora danych osobowych oraz obowiązujących u niego regulacji wewnętrznych[34].

Prezes Urzędu Ochrony Danych Osobowych w niedawno wydanej decyzji słusznie uznał, że nie jest możliwe pełnienie tej funkcji przez prezesa zarządu spółki[35]. Wskazuje się w praktyce, że nie jest możliwe łączenie funkcji inspektora ochrony danych ze stanowiskami kierowniczymi w danej organizacji (np. dyrektora finansowego, dyrektora ds. operacyjnych, kierownika działu marketingu, kierownika działu IT, kierownika działu HR czy też radcy prawnego) lub innymi stanowiskami, jeżeli osoby te uczestniczą w określaniu sposobów i celów przetwarzania[36].

6. Zasady związane z prawidłowym wykonywaniem funkcji inspektora ochrony danych

Przepisy RODO wprowadzają określone wymogi związane z zapewnieniem przez administratorów danych osobowych lub podmioty przetwarzające prawidłowego wykonania funkcji przez inspektora ochrony danych.

Przede wszystkim inspektor ochrony danych powinien być wyznaczany na podstawie kwalifikacji zawodowych, w szczególności posiadanej wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności realizacji powierzonych mu zadań (art. 38 ust. 5 RODO). Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora danych osobowych lub podmiot przetwarzający (motyw 97 RODO). Co za tym idzie, osoba pełniąca tę funkcję powinna posiadać odpowiednie wykształcenie

[34] Wyrok TSUE z dnia 9 lutego 2023 r., C-453/21 ws. X-FAB DRESDEN GMBH & CO. v. FC, LEX nr 3483231.

[35] Decyzja PUODO z dnia 12 września 2025 r., DKN.5131.7.2025, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).

[36] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243), s. 17.

lub wiedzę z zakresu ochrony danych osobowych, w tym obowiązujących przepisów prawa. Zasadne jest także, aby taka osoba była obeznana ze specyfiką działalności administratora danych osobowych lub podmiotu przetwarzającego i obowiązujących w tym zakresie regulacji prawnych oraz procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych przez te podmioty. W przypadku podmiotów i organów publicznych inspektor ochrony danych powinien również wykazywać się znajomością procedur administracyjnych oraz zasad funkcjonowania danego podmiotu[37].

Dzięki prawidłowej realizacji tego obowiązku możliwe jest spełnienie przez organizacje obowiązków prawnych wynikających z przepisów o ochronie danych osobowych. W mojej ocenie jednak powołanie inspektora ochrony danych jest zasadne wtedy, kiedy faktycznie znajdzie się odpowiednią osobę do pełnienia takiej funkcji. Powoływanie osób nieposiadających wymaganych kompetencji czy też powoływanie jedynie formalnie danej osoby, bez faktycznego wykonywania przez nią zadań związanych z tą funkcją, jest działaniem nieprawidłowym.

Celem należytego wykonania zadań nałożonych na inspektora ochrony danych powinien on być włączany we wszystkie sprawy dotyczące ochrony danych osobowych w organizacji[38]. Przy czym przyjmuje się, że jest to obowiązek administratora danych osobowych[39]. Jedynie wtedy, gdy inspektor ochrony danych będzie miał odpowiednią wiedzę o występujących w organizacji procesach, będzie mógł świadczyć usługi doradcze oraz monitorujące wykonywanie obowiązków nałożonych na administratora danych osobowych lub podmiot przetwarzający[40].

Obowiązkiem administratora danych osobowych lub podmiotu przetwarzającego jest wspieranie inspektora ochrony danych w wypełnianiu przez niego zadań poprzez zapewnienie niezbędnych zasobów, w tym lokalowych, organizacyjnych, technicznych,

37 *Kto może, a kto musi wyznaczyć IOD?*, https://uodo.gov.pl/pl/495/2364 (dostęp: 16.06.2025).

38 Zob. szerzej: E. Bielak-Jomaa, *Komentarz do art. 38*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. D. Lubasz, Warszawa 2018, LEX, t. 2.

39 Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 kwietnia 2024 r., II SA/Wa 1342/23, LEX nr 3790155; Wyrok Wojewódzkiego Sądu Administracyjnego z dnia 4 kwietnia 2024 r., II SA/Wa 1805/23, LEX nr 3764924.

40 Wyrok Naczelnego Sądu Administracyjnego z dnia 7 lutego 2025 r., III OSK 6801/21, LEX nr 3833096.

a także pozwalających na utrzymanie jego fachowej wiedzy, na przykład poprzez umożliwienie udziału w szkoleniach z zakresu danych osobowych czy też innych form podnoszenia kwalifikacji zawodowych.

Jednym z najistotniejszych elementów wpływających na status prawny inspektora ochrony danych jest zapewnienie mu niezależności. Powinien on podlegać najwyższemu kierownictwu administratora danych osobowych lub podmiotu przetwarzającego i nie otrzymywać instrukcji dotyczących wykonywania powierzonych mu zadań (art. 38 ust. 3)[41]. Wskazuje się, że to jeden z najważniejszych elementów wpływających na prawidłową realizację zadań przez inspektora ochrony danych. Tylko wtedy, gdy będzie on miał niezależną, wysoką pozycję w organizacji, będzie mógł sprawnie wykonywać swoje obowiązki, w szczególności podejmować działania naprawcze w sytuacji naruszenia ochrony danych osobowych[42].

Opisana powyżej zasada jest przejawem mieszanego charakteru funkcji wykonywanej przez inspektora ochrony danych. Nie może on bowiem otrzymywać instrukcji dotyczących wykonywania swoich zadań, a co za tym idzie, nie jest jedynie wykonawcą poleceń kierowanych przez administratora danych osobowych, lecz niezależnym doradcą i podmiotem monitorującym prawidłowość przetwarzania danych osobowych w organizacji[43].

Niezależnie od tego powinien on jednak podlegać kontroli administratora danych osobowych w zakresie realizacji powierzonych mu zadań, w szczególności pod kątem częstotliwości ich wykonywania, obszarów, w których podejmowane się odpowiednie działania, i rezultatów tych działań[44]. Nie może być on jednak odwołany ani karany przez administratora danych osobowych lub podmiot przetwarzający za wypełnianie

41 Zob. szerzej: G. Sibiga, *O formalnej i faktycznej niezależności inspektora ochrony danych oraz jej gwarancjach. Wybrane zagadnienia* [w:] *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, red. P. Lisowski, R. Kusiak-Winter, Wrocław 2024, s. 707–716.

42 *Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?*, https://uodo.gov.pl/pl/495/2407 (dostęp: 26.10.2025).

43 Decyzja PUODO z dnia 18 grudnia 2024 r., DKN.5112.14.2022, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).

44 Decyzja PUODO z dnia 2 kwietnia 2025 r., DKN.5110.14.2022, https://orzeczenia.uodo.gov.pl (dostęp: 20.06.2025).

swoich zadań. Oczywiście nie prowadzi to do zakazu rozwiązania umowy z taką osobą, jednak przyczyną tego stanu rzeczy nie powinno być prawidłowe realizowanie zadań przez inspektora ochrony danych, nawet jeżeli nie jest to spójne z interesami administratora danych osobowych lub podmiotu przetwarzającego.

7. Podsumowanie

Status inspektora ochrony danych ewoluował w czasie. Od 2015 roku w polskich przepisach prawa obowiązywała funkcja administratora bezpieczeństwa informacji, uregulowana w ustawie o ochronie danych osobowych z 1997 roku, która następnie została zastąpiona na podstawie przepisów RODO od 2018 roku przez funkcję inspektora ochrony danych. Osoby pełniące funkcję administratora bezpieczeństwa informacji stały się automatycznie, na podstawie przepisów prawa, inspektorami ochrony danych w swoich organizacjach. Co istotne, powołanie administratora bezpieczeństwa informacji było dobrowolne, natomiast powołanie inspektora ochrony danych w pewnych sytuacjach jest obowiązkowe. W związku z tym administratorzy danych osobowych oraz podmioty przetwarzające w 2018 roku stanęli przed wyzwaniem znalezienia odpowiedniej osoby do pełnienia tej funkcji, jeżeli było to wymagane.

W przepisach RODO znacznie rozszerzono zadania inspektora ochrony danych. Transformacji uległ także jego status prawny pod kątem jego roli w organizacji. Podczas gdy administrator bezpieczeństwa informacji miał za zadanie głównie wykonywanie obowiązków w imieniu administratora danych osobowych, inspektor ochrony danych jedynie doradza i monitoruje przestrzeganie przepisów dotyczących ochrony danych osobowych w organizacji (rola wewnętrzna), a także stanowi punkt kontaktowy dla podmiotów danych oraz dla organu nadzorczego (rola zewnętrzna). W przepisach RODO uszczegółowiono kompetencje wymagane na tym stanowisku.

Co istotne, od początku istnienia tych funkcji podmioty te miały mieć zapewnioną niezależność w realizacji zadań, co obecnie zostało jeszcze szerzej wskazane w przepisach prawa. Zostało wprost uregulowane, że osoby te nie mogą podlegać wiążącym instrukcjom wydawanym przez administratora danych osobowych lub podmiot przetwarzający, nie mogą być karane za realizację swoich zadań, a także mają unikać konfliktu interesów. Niewątpliwie rola inspektora ochrony danych

ma istotne znaczenie dla prawidłowego wypełniania obowiązków wynikających z przepisów o ochronie danych osobowych w organizacji, ale także ochrony praw i wolności osób, których dane są przetwarzane. Może stanowić również o kulturze organizacji i jej społecznej odpowiedzialności w kontekście ochrony prywatności, a także zapewnienia bezpieczeństwa przetwarzania danych osobowych.

Bibliografia

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 2016 nr 119, poz. 1).

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 1995 nr 281, poz. 31).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133, poz. 882 i 883, z późn. zm.).

Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. 2014, poz. 1662).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz.U. 2019, poz. 1781).

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. 2014, poz. 1934, z późn. zm.).

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015, poz. 745, z późn. zm.).

Orzecznictwo i decyzje organów

Wyrok TSUE z dnia 9 lutego 2023 r., C-453/21 ws. X-FAB DRESDEN GMBH & CO. KG v. FC, LEX nr 3483231.

Wyrok Naczelnego Sądu Administracyjnego z dnia 7 lutego 2025 r., III OSK 6801/21, LEX nr 3833096.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 kwietnia 2024 r., II SA/Wa 1342/23, LEX nr 3790155.

Wyrok Wojewódzkiego Sądu Administracyjnego z dnia 4 kwietnia 2024 r., II SA/Wa 1805/23, LEX nr 3764924.
Decyzja PUODO z dnia 12 września 2025 r., DKN.5131.7.2025, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).
Decyzja PUODO z dnia 2 kwietnia 2025 r., DKN.5110.14.2022, https://orzeczenia.uodo.gov.pl (dostęp: 20.06.2025).
Decyzja PUODO z dnia 18 grudnia 2024 r., DKN.5112.14.2022, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).
Decyzja PUODO z dnia 18 października 2024 r., DKN.5131.7.2024, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).
Decyzja PUODO z dnia 22 września 2020 r., ZWAD.405.31.331.2019, https://orzeczenia.uodo.gov.pl (dostęp: 16.06.2025).
Decyzja PUODO z dnia 21 sierpnia 2020 r., ZSOŚS.421.25.2019, https://orzeczenia.uodo.gov.pl (dostęp: 26.10.2025).

Literatura

Bielak-Jomaa Edyta, *Komentarz do art. 38*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. Dominik Lubasz, Warszawa 2018, LEX.
Borowicz Jacek, *Z problematyki zatrudnienia administratora bezpieczeństwa informacji*, „Praca i Zabezpieczenie Społeczne" 2016, nr 12, 16–25.
Brodzik Robert, *Komentarz do art. 158*, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. Bartosz Marcinkowski, Warszawa 2018, LEX.
Byczkowski Maciej, *Zapewnianie przestrzegania przepisów o ochronie danych osobowych w sferze wewnętrznej bez powołania administratora bezpieczeństwa informacji*, „Monitor Prawniczy" 2015, dodatek do nr 6, s. 1008–1012.
Chodorowski Maciej, *Nowe prawa i obowiązki administratorów bezpieczeństwa informacji (inspektorów ochrony danych) w świetle najnowszych opinii wydanych przez Grupę Roboczą Art. 29*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. Maciej Kawecki, Tomasz Osiej, Warszawa 2017, s. 141–158.
Fajgielski Paweł, [w:] *Komentarz do ustawy o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* wyd. II, Warszawa 2022, LEX.
Fajgielski Paweł, *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Monitor Prawniczy" 2015, dodatek do nr 6, s. 1003–1007.
Kozik Patrycja, *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego*, „Europejski Przegląd Sądowy" 2017, nr 5, s. 18–22.

Kupny Weronika, *Rola inspektora ochrony danych w strukturze organizacji,* „Roczniki Administracji i Prawa" 2019, nr 19(1), s. 295–310.
Kuźnicka-Błaszkowska Dominika, *Organy samorządu gminnego a organ publiczny i podmiot publiczny w RODO*, „Finanse Komunalne" 2024, nr 4, s. 7–14.
Lubasz Dominik, Góral Urszula, *Komentarz do art. 1*, [w:] Edyta Bielak-Jomaa, Iwona Bogucka, Witold Chomiczewski, Piotr Drobek, Maciej Gawroński, Katarzyna Kloc, Joanna Łuczak-Tarka, Paweł Punda, Natalia Zawadzka, Michał Żmijewski, Dominik Lubasz, Urszula Góral, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, LEX.
Młotkiewicz Monika, *IOD jako punkt kontaktowy*, „ABI EXPERT" 2018, nr 2, s. 20–21.
Odlanicka-Poczobutt Monika, Szyszka-Schuppik Aleksandra, *Bezpieczeństwo danych osobowych w świetle nowych przepisów (RODO) – przegląd historyczny,* „Zeszyty Naukowe Politechniki Śląskiej" 2018, z. 118, s. 419–432.
Sibiga Grzegorz, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia*, [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, red. Grzegorz Sibiga, Warszawa 2016, s. 16–21.
Sibiga Grzegorz, *Rejestracja administratorów bezpieczeństwa informacji. Postępowanie rejestracyjne Generalnego Inspektora Ochrony Danych Osobowych*, „Monitor Prawniczy" 2015, dodatek do nr 6, s. 13–19.
Sibiga Grzegorz, *O formalnej i faktycznej niezależności inspektora ochrony danych oraz jej gwarancjach. Wybrane zagadnienia*, [w:] *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, red. Piotr Lisowski, Renata Kusiak-Winter, Wrocław 2024, s. 707–716.
Wygoda Krzysztof, *Administrator Bezpieczeństwa Informacji a Inspektor Ochrony Danych na tle regulacji krajowych i unijnych – wybrane zagadnienia*, „Przegląd Prawa i Administracji" 2016, nr 105, s. 219–236.
Wygoda Krzysztof, *Powoływanie Administratora Bezpieczeństwa Informacji jako zasada bezpiecznego przetwarzania danych na gruncie ustawy o ochronie danych osobowych*, „Przegląd Prawa i Administracji" 2015, nr 100, s. 337–352.
Vademecum Inspektora Ochrony Danych, red. Maciej Kołodziej, Warszawa 2020.
Szałowski Ryszard, *Administrator bezpieczeństwa informacji*, „Ius Novum" 2016, nr 4, s. 208–224.

Inne źródła

Czy administrator musi podać imię i nazwisko IOD na stronie internetowej?, https://uodo.gov.pl/pl/495/2345 (dostęp: 16.06.2025).
Czy dane kontaktowe IOD muszą być łatwo dostępne?, https://uodo.gov.pl/pl/495/2342 (dostęp: 16.06.2025).

Czy inspektor ochrony danych powinien być wyznaczany na podstawie takich samych kwalifikacji jak było to w przypadku administratora bezpieczeństwa informacji?, https://uodo.gov.pl/pl/497/200 (dostęp: 16.06.2025).
Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?, https://uodo.gov.pl/pl/495/2407 (dostęp: 26.10.2025).
Kto może, a kto musi wyznaczyć IOD?, https://uodo.gov.pl/pl/495/2364 (dostęp: 16.06.2025).
Poradnik na gruncie RODO. Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, v. 2, https://uodo.gov.pl/pl/138/3561 (dostęp: 26.10.2025).
Ocena skutków regulacji do projektu ustawy o ochronie danych osobowych z dnia 27 marca 2018 r., druk 2410, https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410 (dostęp: 15.06.2025).
Sibiga Grzegorz, *Opinia prawna – Konflikt interesów w wykonywaniu funkcji inspektora ochrony danych i jego unikanie. Problemy zaistniałe w praktyce i sposoby ich rozwiązania*, Warszawa 2024, https://sabi.org.pl (dostęp: 26.10.2025).
Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243), wersja po zmianach z dnia 5 kwietnia 2017 r., s. 9–10, https://ec.europa.eu/newsroom/article29/items/612048/en (dostęp: 16.06.2025).

STRESZCZENIE

Kształtowanie się statusu prawnego inspektora ochrony danych w Polsce

W Polsce od 2015 roku obowiązywała funkcja administratora bezpieczeństwa informacji. Osoba ją pełniąca miała określone przez przepisy zadania, które miały głównie charakter realizacji obowiązków prawnych w zakresie ochrony danych osobowych ciążących na administratorze danych osobowych. Powołanie takiej osoby było w każdej sytuacji fakultatywne, a w przypadku jej niepowołania w organizacji obowiązek realizacji obowiązków prawnych dotyczących przetwarzania danych osobowych ciążył bezpośrednio na administratorze danych osobowych.

Wraz z wejściem w życie i rozpoczęciem stosowania przepisów RODO w 2018 roku uregulowano status i zadania inspektora ochrony danych. Jednocześnie ustalono, że osoby pełniące dotychczas funkcję administratora bezpieczeństwa informacji staną się z mocy prawa inspektorami ochrony danych do określonego czasu. Jednocześnie pojawił się w określonych przypadkach obowiązek powołania inspektora ochrony danych w organizacji. Ewolucji i rozszerzeniu uległy również zadania inspektora ochrony danych, a także wynikający z tego jego status prawny, który ma obecnie charakter mieszany wewnętrzno-zewnętrzny. Rolą inspektora ochrony danych jest zarówno doradzanie w sprawach dotyczących procesów przetwarzania danych osobowych oraz monitorowanie

przestrzegania przepisów z tym związanych, jaki i pełnienie roli punktu kontaktowego dla podmiotów danych oraz organu nadzorczego. Powołanie kompetentnej osoby na tym stanowisku w organizacji odgrywa istotne znaczenie dla prawidłowego wypełniania obowiązków wynikających z przepisów prawa, ochrony praw i wolności osób, których dane dotyczą, oraz stanowi przejaw społecznej odpowiedzialności w zakresie ochrony prywatności i bezpieczeństwa przetwarzanych danych osobowych.

SUMMARY

The Development of the Legal Status of the Data Protection Officer in Poland

The position of Information Security Administrator has been in force in Poland since 2015. The role involves specific legal responsibilities, primarily fulfilling the Personal Data Controller's legal obligations in the area of personal data protection. Appointing someone to this role was optional, and if no one was appointed, the obligation to fulfil legal obligations relating to the processing of personal data rested directly with the Personal Data Controller.

Following the introduction of the GDPR in 2018, the role and responsibilities of the Data Protection Officer were formalised. It was also established that individuals who had previously held the position of Information Security Administrator would automatically become Data Protection Officers for a specified period. In certain cases, there was also an obligation to appoint a Data Protection Officer within the organisation. The role of the Data Protection Officer has evolved and expanded, as has their legal status, which is now both internal and external. The Data Protection Officer's role is to advise on matters relating to the processing of personal data, monitor compliance with relevant regulations and act as a point of contact for data subjects and the supervisory authority. Appointing a competent person to this position within an organisation is essential for properly fulfilling legal obligations and protecting the rights and freedoms of data subjects. It also demonstrates social responsibility with regard to privacy and the security of personal data processing.