Obywatel w centrum działań e-administracji w Unii Europejskiej

Citizen-centric e-Government in the European Union

REDAKCJA / EDITED BY

Sławomir Dudzik · Inga Kawka · Renata Śliwa

Krakow Jean Monnet Research Papers

Obywatel w centrum działań e-administracji w Unii Europejskiej

Citizen-centric e-Government in the European Union

Krakow Jean Monnet Research Papers

2

Obywatel w centrum działań e-administracji w Unii Europejskiej

Citizen-centric e-Government in the European Union

REDAKCJA / EDITED BY

Sławomir Dudzik · Inga Kawka · Renata Śliwa

WYDAWNICTWO KSIĘGARNIA AKADEMICKA

Kraków 2023

Sławomir Dudzik
Uniwersytet Jagielloński, Kraków
s.dudzik@uj.edu.pl

Inga Kawka
Uniwersytet Jagielloński, Kraków
inga.kawka@uj.edu.pl

Renata Śliwa
Uniwersytet Pedagogiczny im. KEN, Kraków
renata.sliwa@up.krakow.pl

Recenzja: dr hab. Grzegorz Krawiec, prof. UP

Opracowanie redakcyjne: Joanna Cieślik, Anna Sekułowicz

Projekt okładki: Marta Jaszczuk

ISBN 978-83-8138-889-4
https://doi.org/10.127979788381388894

Publikacja dofinansowana przez Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego oraz Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie

With the support of Jean Monnet Activities within ERASMUS+ Programme of the European Union.

Projekt współfinansowany w ramach programu Unii Europejskiej Erasmus+

Wsparcie Komisji Europejskiej dla produkcji tej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie może zostać pociągnięta do odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl

Księgarnia internetowa: akademicka.pl

Spis treści | Table of contents

Obywatel w centrum działań e-administracji w Unii Europejskiej
Citizen-centric e-Government in the European Union | s. 141-156
https://doi.org/10.12797/9788381388894.08

Marcin Adamczyk[1]

Rola i zadania inspektora ochrony danych osobowych przy wdrażaniu e-administracji w jednostkach samorządu terytorialnego

Abstrakt: Administracji (jak i e-administracji) nie ma bez ludzi, bez petentów, stron i uczestników postępowania prowadzonego przed nią. Tym samym jednym z głównych działań administracji jest i będzie przetwarzanie danych osobowych. Przejście w coraz większym wymiarze na e-administrację rodzi pytanie o bezpieczeństwo danych użytkowników i osób korzystających z nowych usług. Tym bardziej, iż praktycznie każdy słyszał, jak i dotknął problemów związanych z bezpieczeństwem danych w sieci. Szczególnego znaczenia zatem nabiera rola inspektora ochrony danych osobowych (dalej: IODO) przy wdrożeniu procesów związanych z e-administracją. Każda z jednostek publicznych, w tym jednostki samorządu terytorialnego (dalej: jst) zobowiązane były do ustanowienia[2] IODO, i z tego obowiązku się wywiązała. Czy jednak administratorzy danych osobowych rozumieją zadania stawiane IODO, czy wykorzystują ich potencjał i możliwości? Niestety praktyka i kontrole, zwłaszcza Najwyższej Izby Kontroli (dalej: NIK), pokazują, iż rzeczywistość w wielu przypadkach jest daleka od ideału. Niniejszy artykuł jest próbą wskazania najczęstszych błędów jest przy współpracy z IODO oraz próbą odnalezienia przyczyn takiego stanu rzeczy.

[1] Dr Marcin Adamczyk, Uniwersytet Warmińsko-Mazurski w Olsztynie, Wydział Prawa i Administracji, Katedra Postępowania Administracyjnego i Sądownictwa Administracyjnego, https://orcid.org/0000-0002-0838-0488R.

[2] Art. 37 ust. 1 lit. a) *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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)*, Dz.Urz. UE 2016, L 119/1 (dalej: RODO).

Słowa kluczowe: inspektor ochrony danych osobowych, e-administracja, jednostki samorządu terytorialnego

The Role and Tasks of the Data Protection Officer in the Implementation of e-Government in Local Authorities

Abstract: There is no administration (and e-administration) without people, applicants, parties and participants in the proceedings conducted before it. Thus, one of the main activities of the administration is and will be the processing of personal data. Increasingly, the transition to e-government raises the question of the security of data of users and people using new services. The more so because practically everyone has heard and touched the problems related to data security in the network. Therefore, the role of the personal data protection officer (hereinafter referred to as DPO) is of particular importance when implementing processes related to e-administration. Each of the public units, including local government units (hereinafter referred to as local government units) were obliged to establish an DPO, and fulfilled this obligation. However, do the personal data administrators understand the tasks set for DPO or do they use their potential and capabilities? Unfortunately, practice and inspections, especially of the Supreme Audit Office (hereinafter referred to as NIK) show that the reality in many cases is far from ideal. This article is an attempt to identify the most common mistakes of local government units in cooperation with the IODO, and an attempt to find the reasons for this state of affairs.

Keywords: Data Protection Officer, e-administration, local government units

1. Wprowadzenie

E-administracja to z jednej strony nowe możliwości, z drugiej wiele wyzwań i zagrożeń. Możliwości, jakie daje obecna technologia, sugerują, iż przyszła e-administracja będzie miała zupełnie inny niż dotychczasowy wymiar. Procesy związane z automatyzacją, działania, których podstawą są algorytmy, nieuchronnie będą wkraczały do administracji i zmieniały jej oblicze. Do e-administracji przygotowujemy się i wdrażamy ją od lat, tyle że nie zawsze udolnie. W 2005 r. została uchwalona i weszła w życie (częściowo) *Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*[3], która m.in. określa zasady dostosowania rejestrów publicznych i wymiany informacji w formie elektronicznej z podmiotami publicznymi do minimalnych, gwarantujących otwartość standardów informatycznych, wymagań dla rejestrów publicznych i wymiany informacji z podmiotami publicznymi czy też wymiany infor-

[3] Pierwotny Dz.U. 2005, nr 64, poz. 565.

macji drogą elektroniczną, w tym dokumentów elektronicznych, pomiędzy podmiotami publicznymi a podmiotami niebędącymi podmiotami publicznymi. Nie powinno dziwić zatem nikogo w administracji, iż wymiana informacji drogą elektroniczną jest możliwa, i co więcej, będzie wypierała tradycyjną korespondencję papierową. Konsekwencją przyjętej ustawy były zmiany w *Kodeksie postępowania administracyjnego*[4], w wyniku których nowe brzmienie dostaje art. 63 § 1 k.p.a.[5] i pojawia się w tym przepisie § 3a. k.p.a.[6] Po nowelizacji podania (żądania, wyjaśnienia, odwołania, zażalenia) mogą być wnoszone pisemnie, telegraficznie lub za pomocą dalekopisu, telefaksu, poczty elektronicznej albo za pomocą formularza umieszczonego na stronie internetowej właściwego organu administracji publicznej, umożliwiającego wprowadzenie danych do systemu teleinformatycznego tego organu, a także ustnie do protokołu[7]. Podanie wniesione w formie dokumentu elektronicznego powinno, z ówcześnie obowiązującym nowym brzmieniem art. 63 § 3a, być opatrzone bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, przy zachowaniu zasad przewidzianych w przepisach o podpisie elektronicznym, oraz zawierać dane w ustalonym formacie, zawarte we wzorze podania określonym w odrębnych przepisach, jeżeli te przepisy nakazują wnoszenie podań według określonego wzoru[8]. Kolejna zmiana ustawy[9] o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw niesie niezwykle istotne z punktu analizowanego zagadnienia zmiany k.p.a., dotyczące m.in. komunikacji elektronicznej, a przede wszystkim określenia zasad tzw. domniemania zastępczego doręczenia korespondencji elektronicznej (art. 46 § 3[10] – przepis ten z czasem zostanie doprecyzowany i w art. 46 k.p.a. pojawią

---

4 *Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego*, Dz.U. 2021, poz. 735 (dalej: k.p.a.).

5 Art. 63 § 1 zmieniony przez art. 36 pkt 5 lit. a) *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. 2005, nr 64, poz. 565) z dniem 21 listopada 2005 r.

6 Art. 63 § 3a dodany przez art. 36 pkt 5 lit. b) *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. 2005, nr 64, poz. 565) z dniem 21 listopada 2005 r.

7 Art. 63 § 1 zmieniony przez art. 36 pkt 5 lit. a) *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. 2005, nr 64, poz. 565) z dniem 21 listopada 2005 r.

8 Art. 63 § 3a dodany przez art. 36 pkt 5 lit. b) *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. 2005, nr 64, poz. 565) z dniem 21 listopada 2005 r.

9 *Ustawa z dnia 10 stycznia 2014 r. o zmianie Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw*, Dz.U. 2014, poz. 183.

10 Art. 46 § 3 dodany przez art. 36 pkt 2 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. 2005, nr 64, poz. 565) z dniem 21 listopada 2005 r.

się art. § 4–6[11]). Wprowadzone zmiany są kolejnym realnym krokiem w stronę e-administracji, pojawia się bowiem m.in. możliwość wyrażenia zgody przez stronę lub innego uczestnika postępowania na komunikowanie się za pomocą środków komunikacji elektronicznej. Co ważne, to strona decyduje, jaką komunikację ma prowadzić z nią organ (papierową czy elektroniczną), następuje rozszerzenie dostępu strony do akt sprawy drogą elektroniczną, dopuszcza się formy elektroniczne dla czynności, dla których aktualnie zastrzeżona jest forma pisemna, np. wezwania na rozprawę, sporządzenia przez urzędnika adnotacji, ustanowienia pełnomocnictwa, składania zeznań i wyjaśnień, dopuszcza się stosowanie elektronicznych kopii dokumentów papierowych uwierzytelnionych przez wnoszącego pismo jako jego załączników. W uzasadnieniu ustawy wskazano, iż „sprawne państwo, aby mogło efektywnie spełniać swoje funkcje, powinno przede wszystkim zapewnić wysoką jakość usług administracji publicznej, która może być osiągnięta między innymi dzięki cyfryzacji". Od tego momentu nie powinno być wątpliwości i podania (pisma) składane do organu oficjalnie w trybie k.p.a. nie mogą być składane zwykłym mailem. W przypadku komunikacji elektronicznej zawsze chodziło i chodzi o identyfikację stron takiej korespondencji. Zasady tej identyfikacji zostały określone przez ustawodawcę. Spodziewając się problemów praktycznych z wdrożeniem nowych rozwiązań, ówczesny minister administracji i cyfryzacji wysłał do wszystkich jednostek samorządu terytorialnego pismo, w którym wyjaśnia i wskazuje, iż

> Droga elektroniczna nie oznacza jednak (w większości przypadków) komunikowania się mailem. Korespondencja do urzędu powinna być odpowiednio uwierzytelniona (tożsamość piszącego ma być potwierdzona – np. podpisem potwierdzonym profilem zaufanym albo bezpiecznym podpisem elektronicznym kwalifikowanym certyfikatem), a składający pismo musi otrzymać dowód, że dokument dotarł do urzędu. Dlatego ważne jest zwracanie obywatelom uwagi, że nowa ustawa ułatwia załatwianie spraw poprzez składanie pism w postaci elektronicznej za pośrednictwem ESP (a nie przez wysyłanie maila)[12].

Pismo to jednak nie wywołuje większych efektów i w praktyce wiele organów ma problemy ze stosowaniem nowych rozwiązań, po raz kolejny niestety najsłabszym

---

[11] Art. 46 § 4 – 6 dodany przez art. 2 pkt 3 *Ustawy z dnia 12 lutego 2010 r. o zmianie Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw* (Dz.U. 2014, poz. 230) z dniem 17 czerwca 2010 r.

[12] *Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej*, Dz.U. 2014, poz. 584, pkt 2, s. 1.

elementem okazują się ludzie i zarówno ich niechęć do nowych rozwiązań, jak i brak ich prawidłowego zrozumienia.

Administracji (jak i e-administracji) nie ma bez ludzi, bez petentów, stron i uczestników postępowania prowadzonego przed nią. Tym samym jednym z głównych działań administracji jest i będzie przetwarzanie danych osobowych. Przejście w coraz większym wymiarze na e-administrację rodzi pytanie o bezpieczeństwo danych użytkowników i osób korzystających z nowych usług. Tym bardziej, iż praktycznie każdy słyszał jak i dotknął problemów związanych z bezpieczeństwem danych w sieci. Szczególna uwaga powinna być zatem skierowana na zapewnienie zgodnych z prawem zasad ochrony danych osobowych. I tu powstaje pytanie, czy i jaką rolę powinni mieć inspektorzy ochrony danych osobowych przy wdrażaniu nowych rozwiązań w poszczególnych jednostkach administracji?

2. Obowiązek wyznaczenia inspektora ochrony danych osobowych w jednostkach samorządu terytorialnego

Administracja publiczna jest zobligowana do powołania IODO i mimo, iż faktycznie obowiązek ten zrealizowała, to w praktyce niestety nie zawsze zabieg ów dał jakościowy skok. Tezę tę potwierdzają zarówno raporty NIK[13] prezentujące wyniki kontroli w zakresie bezpieczeństwa informacji w jednostkach samorządu terytorialnego, jak i działania podejmowane w ostatnim czasie przez Prezesa Urzędu Ochrony Danych Osobowych (dalej: PUODO)[14], który rozpoczął akcję weryfikacji przestrzegania przepisów dotyczących IODO. Koncepcja inspektorów ochrony danych wyznaczanych przez administratora w sektorze publicznym i prywatnym pochodzi z niemieckiego prawa o ochronie danych[15]. Wejście w życie RODO wymusiło rozpoczęcie procesu przygotowania do ustanowienia IODO, mimo dwuletniego *vacatio legis* znaczna część włodarzy jst dopiero pod koniec tego okresu zaczęła podejmować działania bezpośrednio zmierzające do wyłonienia i ustanowenia IODO w swojej jednostce. Jeszcze

---

13 Najwyższa Izba Kontroli, *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, KAP.430.020.2018, nr ewid. 187/2018/P/18/006/KAP, https://www.nik.gov.pl/plik/id,20027,vp,22647.pdf (20.05.2022).

14 https://uodo.gov.pl/pl/138/2336 (16.08.2022).

15 Szerzej na temat europejskiej genezy IODO zob. D. Korff, M. Georges, *Podręcznik Inspektora Ochrony Danych. Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi-publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych*, (zatwierdzony przez Komisję Europejską w lipcu 2019 r.), s. 106 i wskazana tam literatura, https://www.ksoin.pl/wp-content/uploads/2020/01/podrecznik_inspektora_ochrony_danych.pdf (16.08.2022).

przed wejściem w życie RODO Grupa Robocza Artykułu 29 przedstawiła wytyczne dotyczące inspektorów ochrony danych w procesie przygotowania do rozpoczęcia stosowania RODO[16]. Europejska Rada Ochrony Danych, która przejęła zadania Grupy Roboczej Artykułu 29 po rozpoczęciu stosowania RODO, formalnie zatwierdziła te wytyczne (a także inne dokumenty w sprawach wynikających z RODO)[17]. Znane zatem były podstawowe zasady wyłaniania IODO nie tylko z suchych przepisów RODO, ale także z propozycji Grupy Roboczej Artykułu 29 – WP 243. IODO muszą wyznaczyć wszystkie organy lub organy publiczne przetwarzające dane osobowe, podlegające RODO, co wprost wynika z art. 37 ust. 1 lit. a RODO[18]. Ogólne rozporządzenie o ochronie danych osobowych nie definiuje „podmiotu lub organu publicznego". Zgodnie ze wskazaniami Grupy Roboczej Artykułu 29, termin ten należało ustalić w prawie krajowym[19]. Polski ustawodawca nie rozszerzył przedmiotowo ani podmiotowo katalogu podmiotów zobligowanych do wyznaczenia inspektora[20]. W nowej ustawie o ochronie danych osobowych[21] zagadnieniu temu poświęcił rozdział 2, gdzie doprecyzowano i wskazano w art. 8, iż administrator i podmiot przetwarzający są obowiązani do wyznaczenia IODO, w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679, regulującym zasady jego powoływania[22]. Zgodnie z tym przepisem administrator i podmiot przetwarzający wyznaczają IODO zawsze, gdy:

1. przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;

---

16 Grupa Robocza Art. 29 ds. Ochrony Danych, *Wytyczne dotyczące inspektorów ochrony danych ('DPO'). Przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.*, (WP243 rew.01), https://uodo.gov.pl/pl/10/7 (10.08.2022) (dalej: Wytyczne WP 243).

17 The European Data Protection Board, *Endorsement 1/2018*, zatwierdzenie m.in. Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (wymienione jako VII zaaprobowany dokument), 25.05.2018 r., https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf (9.04.2023).

18 Z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

19 Wytyczne WP243, s. 7.

20 Szerzej. zob. K. Kozieł, *Ustawa o ochronie danych osobowych. Przepisy wdrażające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Komentarz*, A. Grzelak et al. (red.), wyd. I, Warszawa 2018, s. 100.

21 *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*, Dz.U. 2019, poz. 1781 (dalej: uodo).

22 *RODO. Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2017, s. 765 i n., *Komentarze.*

3. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

Polski ustawodawca rozstrzygnął zakres podmiotowy pojęcia organów i podmiotów publicznych w art. 9 uodo, wskazując, iż przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się: 1) jednostki sektora finansów publicznych; 2) instytuty badawcze; 3) Narodowy Bank Polski. Sektor finansów publicznych tworzą m.in. jednostki samorządu terytorialnego oraz ich związki; samorządowe zakłady budżetowe[23]. Wszystkie zatem organy i podmioty publiczne, w tym jst (niezależnie od zakresu przetwarzanych danych), mają obowiązek wyznaczenia IODO. W literaturze przedmiotu podkreśla się, iż ustawodawca mimo wskazania w art. 9 nowej uodo podmiotów publicznych mających obowiązek powołać IODO, nie zakreślił zamkniętego katalogu jednostek organizacyjnych w sektorze publicznym, które mogą uzyskać status administratora danych lub podmiotu przetwarzającego[24], co przekładać się będzie na wspomniany obowiązek.

Instytucja IODO zastąpiła krajową instytucję administratora bezpieczeństwa informacji, której zasady powoływania, status i zadania wynikały z art. 36a ustawy z 29 sierpnia 1997 r. i poprzednio obowiązującej uodo[25]. Osoby, które w dniu wejścia w życie nowej uodo (24 maja 2018 r.) pełniły funkcję administratora bezpieczeństwa informacji, stały się inspektorami ochrony danych osobowych[26]. Administratorzy bezpieczeństwa informacji nie musieli być obligatoryjnie powoływani w jst. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone dla niego (z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a) wykonywali sami administratorzy danych[27]. W praktyce tylko nie-

---

[23] Pełen katalog podmiotów tworzących sektor finansów publicznych zawiera art. 9 *Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych*, Dz.U. 2022, poz. 1634; Zob. też *Ustawa o finansach publicznych. Komentarz dla jednostek samorządowych*, P. Walczak (red.), wyd. 2, Warszawa 2021, s. 62, *Ustawy w Praktyce*; na temat pojęcia „sektora finansów publicznych zob. *Ustawa o finansach publicznych. Komentarz prawno-finansowy*, H. Dzwonkowski, G. Gołębiowski (red.), Warszawa 2018, art. 9.

[24] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2018, s. 58 i n., *Prawo w Praktyce*.

[25] Dz.U. 2016, poz. 922.

[26] W art. 158 uodo z 2018 r. usytuowano przepisy przejściowe dotyczące osób pełniących funkcję administratora bezpieczeństwa informacji. Szerzej zob. D. Lubasz, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, s. 587-589, *Komentarze*.

[27] Tak stanowił art. 36 b. uodo z 29.08.1997 r., por. Dz.U. 2016, poz. 922.

wielki procent jst ustanowił administratora bezpieczeństwa informacji i konieczność powołania IODO wiązała się ze znalezieniem odpowiedniej osoby lub podmiotu, który będzie wykonywał obowiązki IODO. Zaczęły się wówczas poszukiwania kandydatów, które przypominały w wielu przypadkach swoistą „łapankę". Niestety spora część jst przy wyborze IODO kierowała się jedynie aspektami ekonomicznymi, wybierając najtańsze oferty na rynku (przy podmiotach zewnętrznych) lub powierzała pełnienie tej funkcji swoim pracownikom jako dodatkowe zadanie[28]. IODO powinien być wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia stawianych mu zadań (art. 37 ust. 5 RODO). IODO w jst powinien posiadać:

1. fachową wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych;
2. fachową wiedzę z zakresu praktyk w dziedzinie ochrony danych osobowych;
3. znajomość przepisów RODO;
4. wiedzę sektorową dotyczącą działalności administratora;
5. odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora;
6. wiedzę w zakresie procedur administracyjnych i funkcjonowania danej jednostki (z uwzględnieniem specyfiki administratora).

IODO powinien być swoistym ekspertem nadzorującym wypełnianie przepisów dotyczących ochrony danych w całej jednostce. To, czy dane kwalifikacje są wystarczające do pełnienia funkcji inspektora, podlega ocenie nie tylko kierownictwa danej organizacji (jst), ale także PUODO. Podmioty wyznaczające inspektora muszą być pewne, że konkretna osoba daje gwarancję prawidłowego i rzetelnego wywiązywania się ze swoich zadań. W przypadku kontroli ze strony PUODO, kierownik jednostki powinien umieć wykazać podstawy, jakimi się kierował przy ocenie kwalifikacji wyznaczonego inspektora. W praktyce bardzo często jedynym kryterium przy powoływaniu IODO była cena lub „potencjalne" oszczędności przy wyborze spośród swoich pracowników[29]. „Potencjalne", gdyż błędy IODO mogą narażać jst na spore kary finansowe, które będzie musiał ponosić administrator. Inspektor może być pracownikiem danej organizacji, może wykonywać zadania w ramach umowy zlecenia lub o dzieło, jak również może być osobą delegowaną w ramach outsourcingu (art. 37 ust. 6 RODO). Przepisy RODO wskazują, że inspektor może wykonywać inne zadania i obowiązki,

[28] Jedno z najczęściej zadawanych wówczas pytań to: czy informatyk, sekretarz gminy lub kadrowa może być IODO?

[29] Autor w trakcie swojej pracy i badań spotkał np. sekretarzy, bibliotekarkę czy też kierowcę wyznaczonych na inspektora w różnych jednostkach publicznych.

jednak nie powinny one powodować konfliktu interesów (art. 38 ust. 6 RODO). Mimo, jak się wydaje, jednoznacznych zapisów, kontrole prowadzone m.in. przez NIK pokazują, iż co prawda we wszystkich sprawdzanych urzędach na podstawie art. 37 ust. 1 RODO zostali powołani inspektorzy ochrony danych, jednak w 22% badanych jednostek stwierdzono, że inne zadania i obowiązki wykonywane przez osobę pełniącą funkcję IODO mogły powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO[30] (inspektorami byli m.in. informatycy zatrudnieni w danej jednostce).

Wzrastający udział technologii informatycznych w codziennych działaniach administracji, w tym jst, a także oczekiwania społeczne co do ułatwienia i przyspieszenia załatwiania spraw przy wykorzystaniu nowych technologii, wymuszają zmianę podejścia do klasycznej administracji. Oczekiwania społeczne dotyczą nie tylko usprawnień w zakresie funkcjonowania e-administracji, lecz także zapewnienia, że wszelkie dane posiadane przez administrację publiczną są właściwie zabezpieczone przed dostępem osób nieupoważnionych. Wzrastać będzie zainteresowanie obywateli cyfrową formą załatwiania spraw w urzędach, elektroniczną komunikacją z urzędem. Zatem zagwarantowanie bezpieczeństwa przetwarzania informacji, w tym ochrona danych, staje się jednym z najistotniejszych wyzwań stojących przed administracją publiczną. Punktem wyjścia do zapewnienia prawidłowego poziomu bezpieczeństwa jest przestrzeganie regulacji prawnych określających niezbędne wymagania i procedury. Niewłaściwe podejście do bezpieczeństwa danych może nie tylko doprowadzić do wycieku, utraty lub sfałszowania danych posiadanych przez urząd, ale możliwy jest także całkowity paraliż pracy urzędu. Jednym z filarów wzmacniających poziom bezpieczeństwa danych jest IODO. Inspektor dysponujący niezbędnymi kwalifikacjami, prawidłowo umiejscowiony w strukturze organizacyjnej, posiadający zarówno wiedzę fachową, jak i umiejętności pozwalające na jej wykorzystanie w praktyce. Taki pracownik jest niezbędny przy wdrażaniu e-administracji w jst. Jego rola i zadania zostały tak ukształtowane, by pomóc administratorowi danych prawidłowo wdrożyć nowe rozwiązania, dbając o właściwy poziom bezpieczeństwa.

3. Rola i zadania inspektora ochrony danych osobowych

Artykuł 39 RODO określa zakres obowiązków IODO, a także wskazuje ogólne sposoby ich realizacji. Naczelnym zadaniem inspektora jest kompleksowe wsparcie

[30] Najwyższa Izba Kontroli, *op. cit.*, s. 15-16.

administratora danych w wewnętrznym przestrzeganiu przepisów dotyczących ochrony danych osobowych. Obowiązki IODO można podzielić na kilka zasadniczych grup:

1. zadania informacyjne i doradcze;
2. zadania monitorujące i nadzorcze;
3. zadania w zakresie współpracy z organem nadzorczym;
4. inne zadania niewskazane w art. 39 RODO[31].

Odnosząc obowiązki IODO do wyzwania, jakie niesie wdrożenie i rozwój e-administracji, szczególną uwagę należy zwrócić na zadania informacyjne i doradcze. Zgodnie z art. 39 ust. 1 lit. a. RODO, inspektor musi informować administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisach Unii lub państw członkowskich o ochronie danych. IODO, mając odpowiednią wiedzę i doświadczenie nie tylko w zakresie prawa, ale i praktyki ochrony danych, powinien być merytorycznie najlepiej przygotowany do rozwiązywania problemów, jakie mogą wiązać się z przetwarzaniem danych[32], w tym zapewniania ich bezpieczeństwa. Inspektor ma informować i doradzać zarówno kadrze zarządzającej, jak i pracownikom w praktyce przetwarzającym dane osobowe o obowiązkach wynikających z przepisów dotyczących ochrony danych (w tym przepisów szczególnych), zwracać uwagę na potencjalne zagrożenia, których przyczyną mogą stać się ewentualne błędy w tym zakresie. Wszelkie kwestie wątpliwe powinny być poddane ocenie inspektora, a z jego stanowiskiem należy się liczyć przy ich rozwiązywaniu. Aby mógł nastąpić taki stan rzeczy (pożądany, ale w praktyce daleki od ideału), IODO (oraz jego zespół, o ile został powołany) musi być zaangażowany od najwcześniejszego etapu we wszystkie sprawy związane z ochroną danych osobowych. Przy ocenie skutków dla ochrony danych RODO wprost wskazuje na zaangażowanie IODO i stanowi, że administrator powinien konsultować się z nim przy okazji dokonywania takiej oceny[33]. Grupa Robocza Art. 29 zaleca konsultacje i informowanie inspektora w początkowych fazach, co wspomoże zapewnienie zgodności z RODO i uwzględnianie ochrony danych w fazie projektowania. W związku z tym angażowanie inspektora powinno być standardową procedurą w organizacji. Ponadto ważne jest, aby inspektor był postrzegany jako partner w dyskusji i włączany w prace grup roboczych poświęconych procesom związanym z przetwarzaniem danych osobowych w ramach organizacji[34].

---

31 P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 439, *Duże Komentarze*.

32 P. Fajgielski, *op. cit.*, s. 440.

33 Art. 35 ust. 2 RODO.

34 Wytyczne WP243 dotyczące IODO, s. 14, https://uodo.gov.pl/pl/10/7 (10.08.2022).

Mając powyższe na uwadze, przy wdrożeniu e-administracji jednostka samorządu terytorialnego, która będzie mierzyła się z takim zadaniem, powinna m.in.:

1. zapewnić udział IODO w spotkaniach kadry odpowiadającej za wdrożenie e-administracji (zasadne jest, aby inspektor był obowiązkowym członkiem grupy odpowiedzialnej za wdrożenie nowych rozwiązań);
2. zapewnić uczestnictwo IODO przy podejmowaniu wszelkich decyzji dotyczących przetwarzania danych osobowych (już na etapie projektowania nowych, poszczególnych e-usług w jst);
3. udostępnić IODO niezbędne informacje odpowiednio wcześniej, umożliwiając inspektorowi zajęcie stanowiska;
4. stanowisko inspektora powinno być zawsze brane pod uwagę (zalecane jest w ramach dobrych praktyk dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem IODO);
5. w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi niezwłocznie skonsultować się z IODO.

Należy także pamiętać, iż pożądane może stać się dodatkowe określenie przez administratora (lub podmiot przetwarzający) wytycznych określających przypadki wymagające konsultacji z IODO. Uzależnione może być to od struktury jst lub rodzaju wdrażanego projektu.

Przyjęcie poszczególnych rozwiązań w zakresie ochrony danych osobowych wymaga podejmowania ze strony IODO zadań monitorujących i nadzorczych. Zgodnie z art. 39 ust. 1 lit. b RODO, inspektor ma za zadanie monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Wydaje się, że właśnie wymienione w przepisie działania zwiększające świadomość oraz szkolenia personelu mogą być niezwykle istotnymi zadaniami decydującymi o skutecznym wdrożeniu e-administracji. Sami wdrażający nie mogą bać się przyjmowanych rozwiązań, muszą je nie tylko rozumieć od strony teoretyczno-prawnej, ale także znać potencjalne zagrożenia wynikające z błędów popełnianych przy wdrożeniu lub braku prawidłowego podejścia (np. związane z wyciekami lub utratą danych osobowych). Rola inspektora w tym zakresie jest bezcenna. To on w dużej mierze będzie odpowiadał nie tylko za poziom zrozumienia, ale i prawidłowego podejścia do problematyki ochrony danych osobowych przy wszelkich aspektach wdrażania e-administracji.

Samo wdrożenie IODO we wszystkie procesy związane z przetwarzaniem danych osobowych będzie niewystarczające do prawidłowego wykonywania wszystkich powierzonych mu zadań. Konieczne stanie się, na co zawraca uwagę art. 38 ust. 2 RODO, niezbędne wsparcie ze strony administratora poprzez zapewnienie mu niezbędnych zasobów do wykonywania obowiązków i utrzymania jego wiedzy fachowej. Administrator musi mieć świadomość dotyczącą realizacji zadań inspektora i zapewnić takie warunki jego funkcjonowania, żeby wszystkie obowiązki wynikające z rozporządzenia były w osobie tego IODO spełnione, a po drugie, aby mógł swoje zadania realizować w warunkach sprzyjających autonomii jego funkcjonowania i wyłącznej podległości administratorowi danych[35].

Te aspekty pracy inspektora w wielu wypadkach nie są jednak prawidłowo rozumiane i inspektorzy nie są traktowani jak partnerzy przy wdrażaniu nowych rozwiązań, nie wspominając już o zapewnieniu odpowiedniego wsparcia administratora. PUODO zwraca uwagę, iż od początku stosowania przepisów RODO Urząd Ochrony Danych Osobowych, zarówno w ramach prowadzonych postępowań, jak w reakcji na zgłaszane mu przypadki nieprzestrzegania przepisów dotyczących inspektorów ochrony danych reaguje na złe praktyki dotyczące IODO. Dotychczasowe doświadczenia organu nadzorczego w tym zakresie posłużyły do sformułowania listy zagadnień, do których – wraz z przedstawieniem odpowiednich dowodów – będą musieli się odnieść wezwani administratorzy i podmioty przetwarzające w ramach rozpoczętej przez Urząd akcji weryfikacji przestrzegania przepisów dotyczących IODO[36]. Akcję tę należy ocenić pozytywnie, gdyż pozwoli ona odpowiedzieć na pytania, czy administratorzy rozumieją zadania nałożone na nich w tym zakresie i jak podchodzą do współpracy z inspektorami ochrony danych osobowych. Warto zwrócić uwagę na kilka ciekawych kwestii, jakie są poruszane w ramach prowadzonej akcji, z pozoru niezwykle prostych, jednakże w praktyce bardzo często stwarzających duże problemy przy udzielaniu odpowiedzi. Urząd zadaje m.in. następujące pytania (ważne ze względu na analizowany problem): „Na podstawie jakich kwalifikacji administrator wyznaczył IODO (np. wykształcenie, doświadczenie, wiedza)? Jakie niezbędne zasoby, o których mowa w art. 38 ust. 2 rozporządzenia 2016/679, administrator zapewnia IODO? W jaki sposób administrator zapewnia, by IODO był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (np. czy zostały opracowane zasady dotyczące tego, jakie sprawy mają być konsultowane z IODO, kto i w jakich

[35] M. Krasińska, *Dyrektor Zespołu ds. Sektora Publicznego UODO*, [w:] *Podsumowanie pierwszego roku obowiązywania RODO w jednostkach samorządu terytorialnego*, S. Jakubczak (red.), Warszawa 2021, s. 27.

[36] https://uodo.gov.pl/pl/138/2336 (dostęp: 15.05.2022 r.).

sytuacjach powinien zgłaszać się w celu uzyskania konsultacji IODO, czy i na jakich zasadach IODO bierze udział w naradach kierownictwa)?"[37]. Wyniki tej akcji mogą przyczynić się do znaczącej zmiany podejścia do pracy, zadań i roli IODO, co z pewnością jest korzystne także w przypadku wdrażania e-administracji.

4. Podsumowanie

Nie czekając na wyniki działań podjętych przez PUODO, już dziś wskazać należy na konieczność zmiany w tym obszarze i będzie to zadanie niezwykle trudne z uwagi na czynnik osobowy, czyli samych pracowników. Transformacja administracji związana z przejściem na e-administrację zmusza do kompleksowego podejścia do kwestii bezpieczeństwa danych, w tym ochrony danych osobowych. Internet przesuwa tradycyjne granice prawa do prywatności, poszerza możliwości uzyskania informacji o danej osobie[38]. Upowszechnienie korzystania z sieci oraz dynamiczny rozwój technik przetwarzania informacji, w tym pojawienie się zupełnie nowych modeli przetwarzania, zwiększyło potrzebę wprowadzenia skutecznych mechanizmów ochrony praw w cyberprzestrzeni[39].

Wraz z „cyfrową transformacją" dane osobowe są coraz częściej przetwarzane w wysoce złożonych środowiskach i architekturze technicznej, w których różne podmioty współpracują ze sobą i posiadają wspólne lub powiązane zadania w odniesieniu do różnych czynności przetwarzania. Dzieje się tak także w sektorze publicznym, który w rzeczywistości ma swoje własne zawiłości pod względem zakresu autonomii, jaką różne organy mogą posiadać w szerszych ramach konstytucyjnych lub administracyjno-prawnych.

Brak kompleksowego podejścia do całego procesu zarządzania bezpieczeństwem, w tym ochrony danych osobowych przez osoby decyzyjne w administracji, może przełożyć się na znaczne wydłużenie procesu wdrożenia nowoczesnej e-administracji z jej pełnym zasobem możliwości. Aby administracja w wydaniu „e" osiągnęła sukces, musi być akceptowalna i zrozumiała zarówno dla wdrażających, jak i użytkowników. To, co zostanie wdrożone, musi być bezpieczne. Nowe technologie to nowe możliwości oraz nowe zagrożenia. Nie zawsze jest to droga łatwa, o czym mogą świadczyć negatywne doświadczenia administracji związane z funkcjonowaniem e-usług (np. problemy

---

37 *Ibidem.*

38 M. Brzozowska, *Ochrona danych osobowych w sieci*, Wrocław 2012, s. 19.

39 M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 20, *Monografie*.

z „GEOPORTAL2”[40]). Dobry, rozumiejący swoje zadania i potrafiący je realizować IODO jest niezbędnym elementem prawidłowego procesu wdrażania nowych rozwiązań w zakresie e-administracji. Należy dać mu (inspektorowi) szanse na wykazanie swej wartości poprzez prawidłowe stosowanie już istniejących przepisów regulujących jego pozycję, zadania oraz zakres obowiązków administratora, bez którego cały proces się nie uda. Administrator musi nie tylko rozumieć, ale i realizować nałożone na niego obowiązki, gdyż dopiero rzetelne podejście do nich i współpraca z IODO mogą przynieść pożądany efekt, jakim będzie bezpieczeństwo przetwarzanych w ramach wdrażanych e-usług danych osobowych.

Bibliografia

Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012.

Dudzik S., *Podstawy prawne przetwarzania danych osobowych przez administrację publiczną a ochrona danych osobowych*, [w:] *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej*, S. Dudzik, I. Kawka, R. Śliwa (red.), Kraków 2022, https://doi.org/10.12797/9788381386739.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, *Duże Komentarze*.

Gumularz M., *Ochrona danych osobowych w sektorze publicznym*, Warszawa 2018, *Prawo w Praktyce*.

Korff D., Georges M., *Podręcznik Inspektora Ochrony Danych. Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi-publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych*, Bruksela 2019, https://www.ksoin.pl/wp-content/uploads/2020/01/podrecznik_inspektora_ochrony_danych.pdf.

Lubasz D., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2019, *Komentarze*.

Podsumowanie pierwszego roku obowiązywania RODO w jednostkach samorządu terytorialnego, S. Jakubczyk (red.), Warszawa 2021.

RODO. Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2017, *Komentarze*.

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, *Monografie*.

Ustawa o finansach publicznych. Komentarz dla jednostek samorządowych, P. Walczak (red.), wyd. II, Warszawa 2021, *Ustawy w Praktyce*.

[40] Decyzja DKN.5112.12.2020: kara nałożona na Głównego Geodetę Kraju w związku z nieuprawnionym udostępnieniem danych na portalu „GEOPORTAL2” (geoportal.gov.pl), zob. S. Dudzik, *Podstawy prawne przetwarzania danych osobowych przez administrację publiczną a ochrona danych osobowych*, [w:] *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej*, S. Dudzik, I. Kawka, R. Śliwa (red.), Kraków 2022, s. 22 i n.

Ustawa o finansach publicznych. Komentarz prawno-finansowy, H. Dzwonkowski, G. Gołębiowski (red.), Warszawa 2018.

Ustawa o ochronie danych osobowych. Przepisy wdrażające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Komentarz, A. Grzelak et al. (red.), wyd. I, Warszawa 2018.

Monografia powstała jako druga w serii dotyczącej e-administracji – *Krakow Jean Monnet Research Papers* – w ramach realizowanego przez Katedrę Prawa Europejskiego Uniwersytetu Jagiellońskiego projektu Jean Monnet Module pt. „E-administracja – europejskie wyzwania dla administracji publicznej w państwach członkowskich UE i krajach partnerskich/eGovEU+".

Książka przedstawia analizę wdrożenia i funkcjonowania e-administracji w Polsce i w Europie ze szczególnym uwzględnieniem wpływu technologii informacyjno-komunikacyjnych na działalność administracji publicznej na rzecz obywateli. Monografia ukazuje również zagrożenia związane z transformacją cyfrową administracji oraz konieczność uwzględnienia centralnego miejsca człowieka w tym procesie.

Monografia adresowana jest do badaczy zajmujących się administracją, prawem administracyjnym i europejskim oraz do praktyków. Mamy nadzieję, że publikacja poszerzy wiedzę na temat cyfryzacji administracji oraz zachęci do dalszych studiów w tej dziedzinie.

The monograph was developed as the second in a series on e-government – *Krakow Jean Monnet Research Papers* – as part of the Jean Monnet Module project, implemented by the Chair of European Law of the Jagiellonian University entitled "E-government – European challenges for public administration in EU Member States and partner countries/eGovEU+."

The book presents an analysis of the implementation and functioning of e-government in Poland and Europe, with particular emphasis on the impact of information and communication technologies on the activities of public administration done for the benefit of citizens. The monograph also shows the threats related to the digital transformation of administration and the need to acknowledge the central place of a human in this process.

The monograph addresses researchers dealing with administration, administrative and European law, and practitioners. We hope the publication will broaden the knowledge about the digitization of administration and will encourage further studies in this field.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA

https://akademicka.pl

ISBN 978-83-8138-889-4