RES HISTORICA 55, 2023

DOI:10.17951/rh.2023.55.693-715

Małgorzata Szabaciuk
(Maria Curie-Skłodowska University, Poland)
https://orcid.org/0000- 0002-2119-134X
e-mail: malgorzata.szabaciuk@mail.umcs.pl

Rola i zadania Inspektora Ochrony Danych w Archiwach Państwowych – próba oceny z perspektywy pięciu lat po wprowadzeniu unijnego ogólnego rozporządzenia o ochronie danych osobowych (RODO)

The Role and Responsibilities of the Data Protection Officer in the State Archives – an Attempt to Assess from the Perspective of Five Years after the Introduction of the EU General Data Protection Regulation (GDPR)

ABSTRACT

This article aims to assess the issue of data protection and the role and tasks of the Data Protection Officer in the National Archives. With the introduction of the EU Data Protection Regulation (GDPR), much has changed in the perception of those who deal

PUBLICATION INFO

e-ISSN: 2449-8467
ISSN: 2082-6060

THE AUTHOR'S ADDRESS: Małgorzata Szabaciuk, the Institute of History of the Maria Curie-Skłodowska University in Lublin, 4A Maria Curie-Skłodowska Square, Lublin 20-031, Poland

SOURCE OF FUNDING: Statutory Research of the Institute of History of the Maria Curie-Skłodowska University in Lublin

SUBMITTED:	ACCEPTED:	PUBLISHED ONLINE:
2022.12.31	2023.06.13	2023.07.20

WEBSITE OF THE JOURNAL: https://journals.umcs.pl/rh

EDITORIAL COMMITTEE E-mail: reshistorica@umcs.pl

with these issues. The Data Protection Officer's main concern is the proper handling of records that are produced in the process of any organizational unit's activities, including those of the State Archives. The role and responsibilities of the Data Protection Officer in the state archives are the same as in other organizations. Due to the nature of the activities of the state archive network and the specific nature of an institution such as the archives, the duties of the Data Protection Officer are extremely important. On the one hand, the state archives service holds records with permanent retention, i.e. category A, and on the other hand it operates like a normal office serving the public with its organizational structure. The management of information security in the age of the knowledge society is the key issue in any institution, for which the Data Protection Officer is responsible. The information security system itself must be well designed and thought out. The EU legislator intended the function of the Data Protection Officer to protect our privacy as well. The system of personal data protection has been in place in Poland for twenty-six years, and after the implementation of the GDPR (along with penalties for improper processing of personal data), we are increasingly considering it as our inalienable right to have our personal data well processed and not shared with unauthorized persons.

Key words: protection of personal data, information security management, the general data protection regulation (GDPR), National Archives, documentation, Data Protection Officer, Controller

STRESZCZENIE

Artykuł ma na celu ocenę kwestii ochrony danych osobowych i roli oraz zadań Inspektora Ochrony Danych w Archiwach Państwowych. Wraz z wprowadzeniem unijnego rozporządzenia o ochronie danych osobowych (RODO) zmieniło się wiele w postrzeganiu osób, które tymi zagadnieniami się zajmują. Inspektor Ochrony Danych koncentruje się przede wszystkim na należytym postępowaniu z dokumentacją, która jest wytwarzana w toku działalności każdej jednostki organizacyjnej, w tym również w Archiwach Państwowych. Rola i zadania Inspektora Ochrony Danych w Archiwach Państwowych są takie same, jak w innych organizacjach. Ze względu na istotę działalności państwowej sieci archiwalnej i specyfikę instytucji, jaką są archiwa, zadania Inspektora Ochrony Danych są niezwykle ważne. Z jednej strony państwowa służba archiwalna posiada dokumentację o wieczystym przechowywaniu, tzn. kategorię A, a z drugiej strony działa jak normalny urząd obsługujący petentów wraz ze swoją strukturą organizacyjną. Właśnie zarządzanie bezpieczeństwem informacji w dobie społeczeństwa opartego na wiedzy jest kluczowym problemem w każdej instytucji, za który odpowiada Inspektor Ochrony Danych. Sam system bezpieczeństwa informacji musi być dobrze zaprojektowany i przemyślany. Ustawodawca unijny w swoim zamyśle stworzył funkcję Inspektora Ochrony Danych, aby chronić także naszą prywatność. System ochrony danych osobowych działa w Polsce od dwudziestu sześciu lat, a po wdrożeniu RODO (wraz z karami za nienależyte przetwarzanie danych osobowych) coraz bardziej podchodzimy do tego jako naszego niezbywalnego prawa, aby nasze dane osobowe były dobrze przetwarzane i nieudostępniane osobom nieupoważnionym.

Słowa kluczowe: ochrona danych osobowych, zarządzanie bezpieczeństwem informacji, rozporządzenie o ochronie danych osobowych (RODO), Archiwa Państwowe, dokumentacja, Inspektor Ochrony Danych, Administrator

DOI:10.17951/rh.2023.55.693-715

WSTĘP

Problem ochrony danych osobowych jest zagadnieniem, z którym coraz częściej spotykamy się na co dzień. Rewolucja informatyczna i informacyjna, masowe przetwarzanie danych to wyzwania, z którymi próbujemy się zmierzyć wszyscy. Rewolucja cyfrowa stworzyła szereg rozwiązań i w wielu aspektach ułatwiła nam życie, dając dostęp do nieograniczonej ilości informacji, ale jednocześnie przyniosła dużo nowych zagrożeń, ingerując bardzo mocno w sferę prywatną obywateli. Nielegalne przetwarzanie danych osobowych, w tym danych wrażliwych, narusza podstawowe prawa człowieka, godząc w jego prawo do prywatności[1]. Ze względu na skalę zjawiska nie jest to jednak problem pojedynczych osób, lecz łączy się bezpośrednio z szeroko rozumianym bezpieczeństwem państwa oraz systemem zarządzania bezpieczeństwem informacji[2].

Problemem ochrony danych osobowych zaczęto zajmować się w drugiej połowie XX w. Związane było to z ideą prawa idącego w kierunku prywatności. Regulacje prawne dotyczące ochrony danych osobowych we wszelkiego rodzaju zbiorach oraz w systemach komputerowych pojawiły się na przełomie lat sześćdziesiątych i siedemdziesiątych ubiegłego stulecia. Już wtedy obawiano się dużej automatyzacji, powstania nowych technologii, które będą nie tylko gromadziły, ale przede wszystkim przetwarzały informacje, w tym dane osobowe obywateli[3].

W Polsce ochrona danych osobowych ma już dwudziestosześcioletnią historię. W naszym kraju ochronę danych osobowych gwarantuje Konstytucja z dnia 2 kwietnia 1997 r.[4], zwłaszcza jej dwa artykuły. Pierwszy z nich to art. 47, który brzmi: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym"[5]. Natomiast drugi to art. 51, który porusza szersze kwestie związane z ochroną danych osobowych i mówi o tym, że: „Nikt nie może obowiązany inaczej niż na podstawie ustawy do ujawnienia

---

[1] Prawo do prywatności to prawo jednostki do życia własnym życiem z ograniczeniem do minimum wszelakiej ingerencji zewnętrznej, A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilne" 1972, 20, s. 16.

[2] M. Szabaciuk, *Transformacja systemów zarządzania bezpieczeństwem informacji w Polsce po 1989 r.*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2019, 17, 1, s. 319–332.

[3] A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, cz. I, „Biuletyn Administratorów Bezpieczeństwa Informacji. Ochrona Danych Osobowych" 2000, 1, s. 9.

[4] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. Dziennik Ustaw Rzeczypospolitej Polskiej [dalej: Dz.U.] 1997, nr 78, poz. 483.

[5] *Ibidem*.

DOI:10.17951/rh.2023.55.693-715

informacji dotyczących jego osoby"[6]. W tym samym roku Polska zaimplementowała Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.[7] Ustawą o ochronie danych osobowych z 29 sierpnia 1997 r., która do momentu wejścia w życie RODO była wielokrotnie nowelizowana[8].

W Polsce na sieć archiwów państwowych składają się trzy archiwa o charakterze centralnym, czyli Narodowe Archiwum Cyfrowe[9], Archiwum Akt Nowych[10] i Archiwum Główne Akt Dawnych[11] oraz trzydzieści archiwów o specyfice regionalnej[12], a nadzór nad nimi sprawuje Naczelny Dyrektor Archiwów Państwowych[13]. Sieć Archiwów Państwowych wraz z Naczelną Dyrekcją Archiwów Państwowych musi stosować przepisy z zakresu ochrony danych osobowych, jak każda inna instytucja

---

[6] *Ibidem*.

[7] 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 (Dziennik Ustaw Unii Europejskiej [dalej: Dz.U. UE] L.1995.281.31).

[8] Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (tekst jednolity Dz.U. 2016, poz. 922).

[9] Więcej na stronie Narodowego Archiwum Cyfrowego, https://www.nac.gov.pl/ [dostęp: 25 I 2023].

[10] Więcej na stronie Archiwum Akt Nowych, https://www.aan.gov.pl/ [dostęp: 25 I 2023].

[11] Więcej na stronie Archiwum Główne Akt Dawnych, https://agad.gov.pl/ [dostęp: 25 I 2023].

[12] Są to: Archiwum Państwowe w Białymstoku, Archiwum Państwowe w Bydgoszczy, Archiwum Państwowe w Częstochowie, Archiwum Państwowe w Gdańsku, Archiwum Państwowe w Gorzowie Wielkopolskim, Archiwum Państwowe w Katowicach, Archiwum Państwowe w Kaliszu, Archiwum Narodowe w Krakowie, Archiwum Państwowe w Kielcach, Archiwum Państwowe w Koszalinie, Archiwum Państwowe w Lesznie, Archiwum Państwowe w Lublinie, Archiwum Państwowe w Łodzi, Archiwum Państwowe w Malborku, Archiwum Państwowe w Olsztynie, Archiwum Państwowe w Opolu, Archiwum Państwowe w Piotrkowie Trybunalskim, Archiwum Państwowe w Płocku, Archiwum Państwowe w Poznaniu, Archiwum Państwowe w Przemyślu, Archiwum Państwowe w Radomiu, Archiwum Państwowe w Rzeszowie, Archiwum Państwowe w Siedlcach, Archiwum Państwowe w Suwałkach, Archiwum Państwowe w Szczecinie, Archiwum Państwowe w Toruniu, Archiwum Państwowe w Warszawie, Archiwum Państwowe we Wrocławiu, Archiwum Państwowe w Zamościu, Archiwum Państwowe w Zielonej Górze. Informacje na temat mapy Archiwów Państwowych znajdują się na stronie prowadzonej przez Naczelną Dyrekcję Archiwów Państwowych, https://www.archiwa.gov.pl/o-nas/mapa-archiwow-panstwowych/ [dostęp: 25 II 2023].

[13] Więcej o nadzorze Naczelnego Dyrektora Archiwów Państwowych można odnaleźć na stronie, https://www.archiwa.gov.pl/o-nas/archiwa-panstwowe/ [dostęp: 25 II 2023].

DOI:10.17951/rh.2023.55.693-715

publiczna czy też spółka prawa handlowego. Są to normalne urzędy, które są zobligowane do należytego postępowania z danymi osobowymi. Wraz z wprowadzeniem RODO uległa zmianie sama definicja ochrony danych osobowych, pewne rzeczy zostały doprecyzowane, bo pierwsze dwie dekady XXI w. to wielkie zmiany w technologii przetwarzania informacji[14], a co za tym idzie także i dokumentacji. Artykuł czwarty RODO definiuje je jako:

> [...] informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[15].

Z definicji wynika, że już samo imię i nazwisko jest daną osobową, co na początku stosowania RODO było zaskoczeniem dla wielu.

25 maja 2023 r. mija pięć lat od wejścia w życie RODO, które zmieniło dużo w postrzeganiu należytej ochrony danych osobowych oraz osób, które w archiwach zostały powołane przez Administratora[16] (czyli właściwe Archiwum Państwowe) na Inspektorów Ochrony Danych (IOD).

---

[14] R. Seweryn, *Technologie informacyjne i komunikacyjne – wprowadzenie w problematykę*, w: *Technologie informacyjne i komunikacyjne na rynku turystycznym*, red. J. Berbeka, K. Borodako, Warszawa 2017, s. 14–15.

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. UE L nr 119, s. 1 ze zm.), art. 4 pkt 1.

[16] „Administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania", art. 4 pkt 7 RODO.

DOI:10.17951/rh.2023.55.693-715

STATUS ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI PRZED ZASTĄPIENIEM GO INSPEKTOREM OCHRONY DANYCH W KONTEKŚCIE ARCHIWÓW PAŃSTWOWYCH

Wraz z nowelizacjami ustawy o ochronie danych osobowych z 1997 r. w Polsce wprowadzono szereg aktów prawnych, które wskazywały, jak należy zabezpieczać informacje, w jaki sposób prowadzić dokumentację z zakresu ochrony danych osobowych. Właśnie oprócz ustawy o ochronie danych osobowych z roku 1997 Administratorzy danych osobowych, czyli w naszym rozumieniu Archiwa Państwowe, byli zobligowani do przestrzegania aktów wykonawczych do niej. To w nich opisane są szczegółowe informacje, m.in. jak należało prowadzić dokumentację związaną z danymi osobowymi[17].

Bardzo ważną rolę w systemie ochrony danych osobowych w każdej organizacji pełnił Administrator Bezpieczeństwa Informacji (dalej: ABI)[18]. Był on powoływany na mocy art. 36a ust. 1 ustawy o ochronie danych osobowych, według którego: „Administrator danych może powołać Administratora Bezpieczeństwa Informacji"[19]. Ważne jest to, że przed RODO Administratorzy mogli powoływać osobę, która zajmowała się w organizacji ochroną danych osobowych, nie było to jednak obligatoryjne. Jeśli Administrator sam chciał sprawować kontrolę nad ochroną danych osobowych, to mógł to robić, powołanie ABI było więc alternatywą. Archiwa Państwowe niejednokrotnie decydowały się na powołanie ABI, bo ułatwiało to pracę. Chociażby nie musiały zgłaszać do Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO)[20] rejestru

[17] Były to akty wykonawcze do ustawy: Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015, poz. 719); Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015, poz. 745; 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); Rozporządzenie MSWiA z dnia 11 grudnia 2008 roku w sprawie wzoru zgłoszenia zbioru do rejestracji GIODO (Dz.U. 2008, Nr 229, poz. 1536); Rozporządzenie MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004, Nr 100, poz. 1024).

[18] T. Cygan, *Podręcznik administratora bezpieczeństwa informacji*, Wrocław 2011.

[19] Ustawa o ochronie danych osobowych (DZ.U. 2016, poz. 922).

[20] Generalny Inspektor Ochrony Danych Osobowych był urzędem do spraw ochrony danych osobowych funkcjonującym w latach 1997–2018, który został zastąpiony 25 V

DOI:10.17951/rh.2023.55.693-715

zbiorów danych osobowych, tylko taki rejestr prowadził ABI. Z dniem 1 lipca 2015 r., na mocy przepisów Ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[21], zostało dokonanych wiele zmian przepisów o ochronie danych osobowych. Wtedy to zdecydowano się na powołanie jawnego, ogólnopolskiego rejestru ABI[22]. Z danych archiwalnych widać, że na powołanie ABI zdecydowało się m.in. Archiwum Państwowe w Koszalinie, którym zarządzała obecna dyrektor Katarzyna Królczyk[23].

Od 1 stycznia 2015 r. obowiązek monitorowania zgodności z przepisami o ochronie danych osobowych precyzyjnie określała ustawa: „obowiązek został przypisany ABI, a w przypadku, gdyby go nie powołano – jego zadania wykonywał Administrator" (art. 36b), czyli – upraszczając – np. Archiwum Państwowe w Piotrkowie Trybunalskim (w jego imieniu dyrektor). Przez nadzorowanie rozumiano zapewnienie przestrzegania przepisów o ochronie danych osobowych (art. 36 a ust. 2 pkt 1).

Warto pamiętać, że ustawę o ochronie danych osobowych z 1997 r. stosowano niejako uzupełniająco w stosunku do aktów prawnych branżowych. Innymi słowy, jeżeli inny akt prawny przewidywał np. większe wymogi co do zabezpieczenia, to właśnie one miały zastosowanie, a jeżeli mniejsze, to wtedy zastosowanie miała ustawa o ochronie danych osobowych. Również przed wejściem w życie RODO, jeśli Archiwum Państwowe wybrało model z ABI, to już wtedy powodowało to, że ABI musiał mieć samodzielność organizacyjną oraz wyodrębnić środki na zapewnienie ochrony danych osobowych. ABI mógł wykonywać inne czynności na rzecz Administratora, jednak nie mogły one kolidować z pełnieniem nadzoru nad ochroną danych osobowych.

Swoje pierwsze zadania ABI wykonywał celem zabezpieczenia danych osobowych w systemach informatycznych. Wraz z kolejnymi nowelizacjami ustawy o ochronie danych osobowych rola ABI rosła. Zgodnie z nowelizacją ustawy o ochronie danych osobowych, która weszła w życie 1 stycznia 2015 r., zmienił się status ABI. Był on powoływany na mocy

2018 r. Prezesem Urzędem Ochrony Danych Osobowych, Ustawa o ochronie danych osobowych (Dz.U. 2018, poz.100, art. 166).

[21] Ustawa o dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. 2014 poz. 1662).

[22] Ogólnopolski rejestr ABI był dostępny na stronie GIODO, https://egiodo.giodo.gov.pl/index.dhtml [dostęp: 8 IV 2018].

[23] Rejestr działa jak normalna wyszukiwarka. Po wpisaniu właściwego Archiwum Państwowego strona pokazywała, kto pełni funkcje ABI, https://egiodo.giodo.gov.pl/search_results_ado.dhtml [dostęp: 8 IV 2018].

DOI:10.17951/rh.2023.55.693-715

art. 36a ust. 1 ustawy o ochronie danych osobowych[24]. W świetle ustawy o ochronie danych osobowych z 1997 r. ABI musiał spełniać trzy warunki (miał zdolność do czynności prawnych oraz korzystał z pełni praw publicznych, posiadał odpowiednią wiedzę z zakresu ochrony danych osobowych oraz nie był karany za umyślne przestępstwo)[25], aby Administrator danych osobowych, w naszym przypadku tym Administratorem była np. Naczelna Dyrekcja Archiwów Państwowych lub poszczególne Archiwa Państwowe, mógł go powołać na to stanowisko[26]. Zgodnie z ustawą obowiązującą do 25 maja 2018 r. o ochronie danych osobowych powołanie ABI bez względu na sytuację było zawsze opcjonalne. Państwowa sieć archiwalna, tak jak inne organizacje, mogła, ale nie miała obowiązku powoływania ABI. Była to rola pomocnicza, ponieważ w przypadku niepowołania ABI, jego zadania pełnił sam Administrator danych osobowych, czyli poszczególne Archiwa Państwowe.

Przepisy o ochronie danych osobowych przed 2018 r. nie mówiły, jaka miałaby być podstawa powierzenia wybranej osobie funkcji ABI. Należało to rozumieć tak, że dopuszczalne jest zatrudnienie jej zarówno na podstawie stosunku pracy, jak i umowy cywilnoprawnej. W myśl art. 36a ust. 7 ustawy o ochronie danych osobowych Administrator Bezpieczeństwa Informacji musiał podlegać bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. W spółkach prawa handlowego administratorem danych jest spółka, a ABI w strukturze podlegał bezpośrednio zarządowi, a w Archiwach Państwowych powinien był podlegać dyrektorowi. Należy podkreślić, że Administrator zobowiązany był zapewnić środki i organizacyjną odrębność ABI[27]. Miało mu to zagwarantować możliwość niezależnego wykonywania przez niego obowiązków. Analizując to wszystko, można uznać, że stosunek pracy nie był najbardziej odpowiednią podstawą obsadzania stanowiska ABI czy po 2018 r. Inspektora Danych Osobowych (IOD), bowiem charakterystyczną cechą stosunku pracy jest pracownicze podporządkowanie[28]. Status ABI bądź IOD powinien się cechować niezależnością w realizacji zadań wynikających z przepisów o ochronie danych osobowych. Umowa zlecenie czy umowa o świadczenie usług wydają się być zdecydowanie lepszymi

---

[24] Ustawa o ochronie danych osobowych (DZ.U. 2016, poz. 922), art. 36 a ust. 1 wskazywał, że „Administrator danych może powołać Administratora Bezpieczeństwa Informacji".

[25] *Ibidem*, art. 36a, pkt. 5.

[26] W art. 36a ust. 5 ustawy o ochronie danych osobowych była mowa o wymaganiach co do Administratora Bezpieczeństwa Informacji, który powinien mieć pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych, posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych oraz nie być karanym za umyślne przestępstwo.

[27] Art. 36 a ustawy o ochronie danych osobowych.

[28] Art. 22 par. 1 Kodeksu Pracy.

DOI:10.17951/rh.2023.55.693-715

formami zatrudnienia niż klasyczna umowa o pracę w przypadku osób zajmujących się ochroną danych osobowych[29].

Administrator, który zdecydował się na powołanie ABI, musiał ten fakt zgłosić do GIODO w terminie 30 dni od dnia jego powołania[30]. Ważne było, żeby w treści zgłoszenia powołania ABI Administrator oświadczył, czy osoba powołana do pełnienia tej funkcji spełniała poszczególne wymogi kwalifikacyjne oraz czy podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej Administratorem. Jeśli chodzi zaś o odwołanie ABI, to powinno nastąpić w takim samym trybie w terminie 30 dni od dnia jego zwolnienia.

Do zadań ABI należało przede wszystkim zapewnienie przestrzegania przepisów o ochronie danych osobowych:

- sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych opracowanie w tym zakresie sprawozdania dla Administratora;
- nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych osobowych oraz przestrzegania zasad w niej określonych;
- zapewnienie o zapoznaniu osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych („szkolenie").

Ponadto ABI prowadził rejestr zbiorów danych przetwarzanych przez Administratora, z wyjątkiem zbiorów wskazanych w ustawie jako zwolnionych[31].

Na zadania ABI składały się także zadania związane ze sprawdzeniem i sprawozdaniem z tej czynności. Sprawdzenie mogło odbywać się planowo bądź doraźnie dla Administratora lub gdy GIODO zwrócił się do ABI (wpisanego do rejestru) o dokonanie sprawdzenia u Administratora, który go powołał, wskazując zakres i termin sprawdzenia. Celem takiego sprawdzenia było ustalenie i przede wszystkim udokumentowanie stanu faktycznego przestrzegania przepisów o ochronie danych osobowych. W sprawozdaniu ABI informował, czy naruszone zostały przepisy o ochronie danych osobowych, a jeżeli tak, to jakie są planowane lub podjęte działania przywracające stan zgodny z prawem. Następnym zadaniem, które ABI musiał wykonywać, był nadzór nad dokumentacją przetwarzania danych. Były to dwa dokumenty, które powinny być w każdej organizacji: polityka bezpieczeństwa przetwarzania danych oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Tak jest

[29] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, tj. Dz. U. 2014, poz. 121, z późn. zm.

[30] Art. 46 b ust. 1.

[31] Art. 36a ust. 2 Ustawy o ochronie danych osobowych.

DOI:10.17951/rh.2023.55.693-715

i teraz, te dwa normatywy powinny funkcjonować w każdej instytucji, która dba o bezpieczeństwo informacji. Celem polityki bezpieczeństwa było zapewnienie należytej ochrony danych osobowych będących w zasobach Administratora, w szczególności odpowiedniej do zagrożeń i kategorii danych osobowych objętych ochroną. Poprzez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych. Zakres stosowania polityki bezpieczeństwa obejmuje wszystkie zbiory danych osobowych, które są przetwarzane przez administratora danych, zarówno w formie elektronicznej, jak i papierowej, oraz dane osobowe przetwarzane poza zbiorami danych. Drugi z dokumentów, czyli instrukcja zarządzania system informatycznym wykorzystywanym do przetwarzania danych osobowych, określa sposób i cel zabezpieczania danych osobowych przed wszelakimi zagrożeniami, a zwłaszcza przed ich udostępnianiem osobom nieupoważnionym. Chroni to Administratora przed nieautoryzowanymi zmianami, utratą, uszkodzeniem lub zniszczeniem. Taka instrukcja opisuje sposób nadawania uprawnień poszczególnym użytkownikom, określa sposoby pracy w systemach informatycznych w danej organizacji[32].

Zgodnie z przepisami z 2018 r. w każdej instytucji, w której przetwarza się dane osobowe, należy nadzorować zgodność ich przetwarzania z przepisami o ochronie danych osobowych. Należy zauważyć, że przed zmianami ustawa z 1997 r. podkreślała mocniej konieczność ochrony (zabezpieczania) danych osobowych, pozostawiając zapewnienie zgodności z przepisami niejako w domyśle. Nadzór ten miał pełnić przedsiębiorca, w naszym przypadku konkretne Archiwa Państwowe (art. 36 b ustawy o ochronie danych osobowych), czyli Administrator, który mógł powołać ABI, który ten nadzór pełnił w jego imieniu.

Wcześniej obowiązek nadzorowania zgodności z przepisami ustawy był niejako w domyśle. Nie wspominano o tym w ustawie z 1997 r., wychodząc zapewne z założenia, że skoro należy stosować przepisy prawa, to oczywiste jest, że trzeba weryfikować, czy są stosowane. Obowiązuje przecież zasada *ignorantia iuries nocet* (nieznajomość prawa szkodzi), która oznacza, że niezależnie od tego, jak skomplikowane, nieczytelne i restrykcyjne byłoby prawo – i tak trzeba je znać i stosować, a jego nieznajomość nie zwalnia w żaden sposób z odpowiedzialności[33].

---

[32] K. Gałaj-Emiliańczyk, *Administrator Bezpieczeństwa Informacji i Inspektor Ochrony Danych*, Warszawa 2017.

[33] D. Czerniak, *Granice obowiązywania zasady ignorantia iuris nocet w polskim procesie karnym*, „Folia Iuridica Universitatis Wratislaviensis" 2015, 4 (1), s. 201–218; też vide: wyr. TK z 2.4.2007 r., SK 19/06, OTK-A 2007, nr 4, poz. 37.

DOI:10.17951/rh.2023.55.693-715

RODO I JEGO KONSEKWENCJE W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W ARCHIWACH PAŃSTWOWYCH

Przepisy ogólnego rozporządzenia o ochronie danych osobowych[34] zaczęły obowiązywać we wszystkich krajach członkowskich Unii Europejskiej od 25 maja 2018 r. Wraz z nimi zostały zmienione mechanizmy ochrony danych osobowych w krajach członkowskich, w tym także w Polsce. Najważniejszą zmianą, jaka nastąpiła, jeśli chodzi o ABI, to ewolucja jego zadań, jak i nowa nazwa funkcji. Administrator Bezpieczeństwa Informacji został zastąpiony przez Inspektora Danych Osobowych[35]. Co należy podkreślić, osoby, które były zgłoszone jako ABI, zaczęły automatycznie pełnić funkcję IOD od 1 września 2018 r. Była to data graniczna wynikająca z ustawy o ochronie danych osobowych z 10 maja 2018 r. Po 1 września 2018 r. Administrator musiał zgłosić Inspektora Ochrony Danych do Prezesa Ochrony Danych Osobowych. Natomiast Archiwa Państwowe, które nie miały powołanego Administratora Bezpieczeństwa Informacji, musiały to zrobić do 31 lipca 2018 r.[36]

Od wejścia w życie RODO rola IOD znacznie wzrosła w porównaniu z ABI, który funkcjonował w poprzednim porządku prawnym. Obecnie reprezentują oni Administratora, czyli Archiwum Państwowe, w kontaktach zewnętrznych, zaś do wejścia w życie RODO ABI zajmował się tylko ochroną danych osobowych wewnątrz organizacji. IOD podejmuje działania mające na celu realizację uprawnień danych podmiotów. Wyznaczenie IOD jest obowiązkowe we wskazanych przypadkach w RODO[37]. Dotyczy to całego sektora publicznego, a Archiwa Państwowe takimi podmiotami są. W artykule 39 RODO zostały określone zadania IOD. Możemy wyróżnić w nich przede wszystkim działania informacyjne, monitorowanie przestrzegania przepisów o ochronie danych oraz współpracę z organem nadzorczym, czyli Urzędem Ochrony Danych Osobowych[38]. Zmiany, które wynikają z wejścia w życie RODO, pociągnęły za sobą konieczność

---

[34] 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. UE L nr 119, s. 1 ze zm.).

[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. UE L nr 119, s. 1 ze zm.).

[36] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz. 1000).

[37] Art. 37 ust. 1 RODO.

[38] Strona Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl [dostęp: 23 IV 2023].

DOI:10.17951/rh.2023.55.693-715

uwzględnienia nowych rozwiązań w zakresie przetwarzania danych osobowych w państwowej sieci archiwalnej. Przede wszystkim należało ocenić zgodność dotychczasowych praktyk z wymogami wynikającymi z RODO. Odnosi się to m.in. do takich kwestii jak obowiązek uwzględnienia ochrony danych w fazie projektowania oraz zapewnienia ochrony danych w ustawieniach domyślnych. Nie mniej istotną jest kwestia przekazywania danych do państwa trzeciego[39]. Bardzo ważnym problemem jest udostępnianie materiałów archiwalnych, które są przechowywane w archiwach zgodnie z art. 16a ustawy o narodowym zasobie archiwalnym i archiwach, w którym mamy zagwarantowane, że „każdemu przysługuje prawo dostępu do materiałów archiwalnych"[40]. Klauzule informacyjne, które są umieszczone w Archiwach Państwowych, zawierają informacje określające, na jakiej podstawie prawnej będą przetwarzane dane osobowe m.in. osób korzystających z zasobu archiwalnego[41].

INSPEKTOR OCHRONY DANYCH W ARCHIWACH PAŃSTWOWYCH

Zgodnie z RODO Naczelna Dyrekcja Archiwów Państwowych, która jest organem zarządzającym Archiwami Państwowymi (trzy archiwa centralne oraz trzydzieści archiwów państwowych), musi mieć wyznaczonego Inspektora Ochrony Danych. Jego dane kontaktowe powinny być zamieszczone na stronie internetowej, wynika to bezpośrednio z przepisów prawa[42]. Wytyczne Grupy Roboczej art. 29 dotyczące Inspektorów Ochrony Danych mówią wprost, że poza adresem poczty elektronicznej lub numerem telefonu Administrator jest zobligowany do podania imienia i nazwiska Inspektora Ochrony Danych. Niestety nie wszystkie Archiwa Państwowe publikują takie informacje, zamieszczając tylko informacje o adresie e-mail, adresie i numerze telefonu stacjonarnego, bez podania imienia i nazwiska.

Warto w tym miejscu podkreślić, że informacje dotyczące IOD powinny być łatwo dostępne, niestety w wielu przypadkach tak nie jest.

---

[39] Za państwo trzecie uważa się niewchodzące w skład Europejskiego Obszaru Gospodarczego.

[40] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. 2020, poz. 164).

[41] Zob. m.in. klauzule informacyjne w Archiwum Państwowym w Koszalinie dostępne w zakładce „Ochrona danych osobowych", http://www.koszalin.ap.gov.pl/klauzule-informacyjne/ [dostęp: 23 I 2023].

[42] Wątpliwości w tej kwestii rozwiewa zarówno art. 29 Grupy Roboczej, jak i Urząd Ochrony Danych Osobowych na swojej stronie internetowe, *Czy dane kontaktowe IOD muszą być łatwo dostępne?*, https://uodo.gov.pl/pl/495/2342 [dostęp: 24 IV 2023].

DOI:10.17951/rh.2023.55.693-715

Oczywiście część Archiwów Państwowych ma zakładkę „ochrona danych osobowych" bądź „RODO" na stronie głównej, niestety duża część Archiwów Państwowych informacje na temat IOD publikuje w BIP, właśnie przy klauzulach informacyjnych bądź w osobnej zakładce „ochrona danych osobowych".

Poniżej została zaprezentowana tabela w ujęciu całościowym, jeśli chodzi o Naczelną Dyrekcję Archiwów Państwowych oraz Archiwa Państwowe, pokazująca, czy wyznaczono w nich Inspektorów Ochrony Danych. Podano również interpretację definicji Administratora. Niestety nie dla wszystkich jest jednoznaczne, że wg RODO Administratorem jest jednostka organizacyjna, czyli Archiwum Państwowe. Osiem Archiwów Państwowych definiuje, że Administratorem danych osobowych jest Dyrektor Archiwum Państwowego, co jest błędną interpretacją przepisów RODO. Ponadto ze swojego obowiązku w sprawie podania informacji, kto pełni funkcję IOD, nie wywiązało się piętnaście Archiwów Państwowych oraz Naczelna Dyrekcja Archiwów Państwowych.

Do kwestii ochrony danych osobowych w państwowej sieci archiwalnej powinno się podejść w oparciu o obowiązujące przepisy i systemowo. Skoro RODO pozwala sprawować funkcję IOD w kilku podmiotach, czy też można wyznaczyć jednego IOD dla korporacji, to dlaczego nie zastosować takiego rozwiązania w państwowej sieci archiwalnej? Zadania w każdym Archiwum Państwowym są takie same. Specyfika instytucji powoduje, że powinniśmy mieć ludzi wyspecjalizowanych w tej materii. RODO co prawda dopuszcza możliwość, aby IOD miał też inne obowiązki, ale tylko w przypadku niekolidowania z obowiązkami z zakresu ochrony danych osobowych. Nie powinno być tak, że Archiwa Państwowe wyznaczyły IOD, bo mają taki obowiązek ustawowy. Powinna to być osoba, która zna się na tematyce, a nie zajmuje się tym „z doskoku".

Zmiany, które weszły po 25 maja 2018 r., to przede wszystkim kary administracyjne, które są wysokie[43]. Wprowadzenie RODO spowodowało ujednolicenie zasad przetwarzania danych osobowych, również w Archiwach Państwowych.

Inspektor Ochrony Danych w Archiwach Państwowych odpowiedzialny jest za dokumentację ochrony danych. Prowadzi rejestr zbiorów ochrony danych oraz szkolenia z zakresu ochrony danych osobowych i bezpieczeństwa informacji. Prowadzi także rejestr upoważnień do przetwarzania ochrony danych osobowych. Z racji tego, że podlega bezpośredniemu najwyższemu kierownictwu i jest tylko przed nim odpowiedzialny,

[43] *Z życia dialogu: RODO – potrzebne choć niełatwe*, red. I. Zakrzewska, Warszawa 2021, s. 17–18.

DOI:10.17951/rh.2023.55.693-715

Tabela 1. Definicja Administratora i dane kontaktowe Inspektora Ochrony Danych

Lp.	Nazwa archiwum	Zdefiniowanie administratora	Nazwisko i imię IOD	Kontakt e-mail
1.	Naczelna Dyrekcja Archiwów Państwowych	Administratorem jest Naczelna Dyrekcja Archiwów Państwowych	nie jest podany	jest podany
2.	Narodowe Archiwum Cyfrowe	Administratorem jest Narodowe Archiwum Cyfrowe	nie jest podany	jest podany
3.	Archiwum Akt Nowych	Admiratorem jest Archiwum Akt Nowych	jest podany	jest podany
4.	Archiwum Główne Akt Dawnych	Administratorem Państwa danych jest Dyrektor AGAD	jest podany	jest podany
5.	Archiwum Państwowe w Białymstoku	Administratorem jest Archiwum Państwowe w Białymstoku	nie jest podany	jest podany
6.	Archiwum Państwowe w Bydgoszczy	Administratorem jest Archiwum Państwowe w Bydgoszczy	nie jest podany	jest podany
7.	Archiwum Państwowe w Częstochowie	Administratorem jest Dyrektor Archiwum Państwowego w Częstochowie	jest podany	jest podany
8.	Archiwum Państwowe w Gdańsku	Administratorem jest Archiwum Państwowe w Gdańsku	nie jest podany	jest podany
9.	Archiwum Państwowe w Gorzowie Wielkopolskim	Administratorem jest Archiwum Państwowe w Gorzowie Wielkopolskim	jest podany	jest podany
10.	Archiwum Państwowe w Katowicach	Administratorem Archiwum Państwowe w Katowicach	nie jest podany	jest podany
11.	Archiwum Państwowe w Kaliszu	Administratorem jest Archiwum Państwowe w Kaliszu	nie jest podany	podane dwa różne adresy
12.	Archiwum Narodowe w Krakowie	Admiratorem jest Archiwum Narodowe w Krakowie	jest podany	jest podany

DOI:10.17951/rh.2023.55.693-715

13.	Archiwum Państwowe w Kielcach	Administratorem jest Archiwum Państwowe w Kielcach	nie jest podany	jest podany
14.	Archiwum Państwowe w Koszalinie	Administratorem jest Archiwum Państwowe w Koszalinie	jest podany	jest podany
15.	Archiwum Państwowe w Lesznie	Administratorem jest Archiwum Państwowe w Lesznie	jest podany	jest podany
16.	Archiwum Państwowe w Lublinie	Administratorem jest Archiwum Państwowe w Lublinie	jest podany	jest podany
17.	Archiwum Państwowe w Łodzi	Administratorem jest Dyrektor Archiwum Państwowego w Łodzi	jest podany	jest podany
18.	Archiwum Państwowe w Malborku	Administratorem jest Dyrektor Archiwum Państwowego w Malborku	nie jest podany	jest podany
19.	Archiwum Państwowe w Olsztynie	Administratorem jest Archiwum Państwowe w Olsztynie	jest podany	jest podany
20.	Archiwum Państwowe w Opolu	Administratorem jest Archiwum Państwowe w Opolu	nie jest podany	jest podany
21.	Archiwum Państwowe w Piotrkowie Trybunalskim	Administratorem jest Dyrektor Archiwum Państwowego w Piotrkowie Trybunalskim	nie jest podany	jest podany
22.	Archiwum Państwowe w Płocku	Administratorem jest Archiwum Państwowe w Płocku	jest podany	jest podany
23.	Archiwum Państwowe w Poznaniu	Administratorem jest Archiwum Państwowe w Poznaniu	jest podany	jest podany
24.	Archiwum Państwowe w Przemyślu	Administratorem jest Archiwum Państwowe w Przemyślu	jest podany	jest podany
25.	Archiwum Państwowe w Radomiu	Administratorem jest Dyrektor Archiwum Państwowego w Przemyślu	nie jest podany	jest podany

DOI:10.17951/rh.2023.55.693-715

26.	Archiwum Państwowe w Rzeszowie	Administratorem jest Archiwum Państwowe w Rzeszowie	nie jest podany	jest podany
27.	Archiwum Państwowe w Siedlcach	Administratorem jest Archiwum Państwowe w Siedlcach	jest podany	jest podany
28.	Archiwum Państwowe w Suwałkach	Administratorem jest Archiwum Państwowe w Suwałkach	jest podany	jest podany
29.	Archiwum Państwowe w Szczecinie	Administratorem jest Archiwum Państwowe w Szczecinie	jest podany	jest podany
30.	Archiwum Państwowe w Toruniu	Administratorem jest Archiwum Państwowe w Toruniu	nie jest podany	jest podany
31.	Archiwum Państwowe w Warszawie	Administratorem jest Dyrektor Archiwum Państwowego w Warszawie	jest podany	jest podany
32.	Archiwum Państwowe we Wrocławiu	Administratorem jest Archiwum Państwowe we Wrocławiu	nie jest podany	jest podany
33.	Archiwum Państwowe w Zamościu	Administratorem jest Archiwum Państwowe w Zamościu	jest podany	jest podany
34.	Archiwum Państwowe w Zielonej Górze	Administratorem jest Dyrektor Archiwum Państwowego w Zielonej Górze	nie jest podany	jest podany

Źródło: opracowanie własne na podstawie stron internetowych NDAP oraz 33 Archiwów Państwowych*. Stan na dzień 30 IV 2023 r.

* Informacje pozyskane bezpośrednio ze stron internetowych: Naczelnej Dyrekcji Archiwów Państwowych, https://www.gov.pl/web/archiwa/ochrona-danych-osobowych; Narodowego Archiwum Cyfrowego, https://nac.ssdip.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Akt Nowych, https://aan.gov.pl/formularz-pracownia/rodo.php; Archiwum Głównego Akt Dawnych https://agad.bip.gov.pl/struktura-organizacyjna/struktura-organizacyjna-agad.html; Archiwum Państwowego w Białymstoku, https://www.bialystok.ap.gov.pl/p,93,polityka-prywatnosci; Archiwum Państwowego w Bydgoszczy, https://apbydgoszcz.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego w Częstochowie, https://czestochowa.ap.gov.pl/index.php/pl/ochrona-danych-osobowych; Archiwum Państwowego w Gdańsku, https://www.gdansk.ap.gov.pl/pl/top/rodo; Archiwum Państwowego w Gorzowie Wielkopolskim, https://gorzow.ap.gov.pl/p,83,polityka-rodo; Archiwum Państwowego w Katowicach, https://archiwumkatowice.bip.gov.pl/ochrona-danych-osobowych/inspektor-ochrony-danych-archiwum-panstwowego-w-katowicach.html; Archiwum Państwowego w Kaliszu, https://www.archiwum.kalisz.pl/polityka-ochrony-danych-osobowych; Archiwum Narodowego w Krakowie, https://

DOI:10.17951/rh.2023.55.693-715

ank.gov.pl/ochrona-danych-osobowych/; Archiwum Państwowego w Kielcach, https://www.kielce.ap.gov.pl/p,96,ochrona-danych-osobowych; Archiwum Państwowego w Koszalinie, https://apkoszalin.bip.gov.pl/ochrona-danych-osobowych/; Archiwum Państwowego w Lesznie, https://www.archiwum.leszno.pl/new/container/KLAUZULA-OGRANICZENIA.pdf; Archiwum Państwowego w Lublinie, https://lublinarchiwum.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego w Łodzi, https://aplodz.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego w Malborku, https://malbork.ap.gov.pl/p,126,rodo; Archiwum Państwowego w Olsztynie, https://apolsztyn.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego w Opolu, https://ap_opole.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego w Piotrkowie Trybunalskim, https://appiotrkow.bip.gov.pl/ochrona-danych-osobowych/klauzula-informacyjna-archiwum-panstwowego-w-piotrkowie-trybunalskim.html; Archiwum Państwowego w Płocku, https://plock.ap.gov.pl/index.php/ochrona-danych-osobowych/; Archiwum Państwowego w Poznaniu, https://poznan.ap.gov.pl/instytucja/podo/, https://appoznan.bip.gov.pl/ochrona-danych-osobowych/klauzula-informacyjna-polityki-ochrony-danych-osobowych.html; Archiwum Państwowego w Przemyślu, https://www.przemysl.ap.gov.pl/p,117,ochrona-danych-osobowych; Archiwum Państwowego w Radomiu, https://www.radom.ap.gov.pl/p,91,rodo; Archiwum Państwowego w Rzeszowie, https://aprzeszow.bip.gov.pl/rodo/klauzula-informacyjna-o-przetwarzaniu-danych-osobowych.html; Archiwum Państwowego w Szczecinie, https://www.szczecin.ap.gov.pl/pl/polityka-ochrony-danych-osobowych; Archiwum Państwowego w Toruniu, https://aptorun.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego w Warszawie, https://2564fftxyr.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego we Wrocławiu, https://apwroclaw.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html; Archiwum Państwowego we Zamościu, https://archiwumzamosc.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.htm; Archiwum Państwowego w Zielonej Górze, https://apzg.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html. [Dostęp do wszystkich stron: 30 IV 2023].

DOI:10.17951/rh.2023.55.693-715

powinien być niezależny[44]. Jak już wspomniałam, jego dane kontaktowe muszą być podane na stronie internetowej i musi on być wymieniony z imienia i nazwiska.

Każda instytucja, także Archiwa Państwowe, powinna mieć swoją politykę bezpieczeństwa informacji. Jak już podnoszono, właśnie IOD ma za zadanie czuwać nad jej poprawnością i należytym jej stosowaniem. Oprócz polityki bezpieczeństwa powinna być również opracowana instrukcja zarządzania systemami informatycznymi. RODO to przede wszystkim ujednolicenie zasad przetwarzania danych osobowych. Należy pamiętać, że chronimy nie tylko dane osobowe, ale samą dokumentację. Przecież trudno chronić dane osobowe bez dokumentacji. Praktycznie w każdej dokumentacji są dane osobowe.

Z punktu widzenia archiwisty i IOD należy także podkreślić znaczenie prawa do bycia zapomnianym[45], to jedno z rozwiązań, które w zamyśle ustawodawcy europejskiego dawało możliwości usunięcia danych konkretnej osoby z Internetu. Koncepcja ta ma pewne wady natury technicznej, gdyż nie daje się zrealizować w stu procentach. Znalezienie i usunięcie danych osobowych konkretnej osoby z wszelkich miejsc, które dostępne są w sieci publicznej, przypomina szukanie igły w stogu siana.

RODO A OKRESY PRZECHOWYWANIA DOKUMENTACJI

Wewnętrzne przepisy obowiązujące w Archiwach Państwowych oczywiście nie mogą być sprzeczne z obowiązującym powszechnie prawem. Archiwista powinien pogodzić normatywy kancelaryjno-archiwalne z kanonami ochrony danych osobowych. Wraz z zasadą minimalizacji liczby danych w zakresie przetwarzania danych musimy zmienić podejście do kwestii przechowywania dokumentacji. RODO wymusiło także zmianę w przepisach kancelaryjnych i archiwalnych, pojawiły się nowe klasy rzeczowe w jednolitych rzeczowych wykazach akt, takie jak np. zgłoszenie naruszeń ochrony danych osobowych[46], które powinno być

[44] *Poradnik dla początkującego inspektora ochrony danych. Jak należycie wykonywać swoje zadania? Jakie wymogi spełnić?*, red. M. Kowalski, Warszawa 2020, s. 67.

[45] Ciekawy przypadek o prawie do bycia zapomnianym został opisany w „Rzeczpospolitej" w artykule na temat archiwów prasowych, https://www.parp.gov.pl/component/content/article/82927:prawo-do-bycia-zapomnianym-czy-dane-osobowe-faktycznie-zawsze-mozna-usunac [dostęp: 27 II 2023].

[46] Administrator bez zbędnej zwłoki, nie później niż 72 godziny po stwierdzeniu naruszenia ochrony danych osobowych, powinien zgłosić Prezesowi Urzędu Ochrony Danych Osobowych, więcej o tym, w jaki sposób to zrobić, można dowiedzieć się na stronie Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/525 [dostęp: 24 II 2023].

DOI:10.17951/rh.2023.55.693-715

kategorią A, czy też dokumentowanie czynności związanych z przetwarzaniem danych osobowych.

Przepisy RODO dotyczą danych osobowych, a przepisy kancelaryjno-archiwalne dotyczą postępowania z dokumentacją[47]. W jednolitym rzeczowym wykazie akt określona jest kategoria archiwalna, a co za tym idzie informacja, ile powinna ona być przetwarzana w omawianym przez nas przypadku, tj. w Archiwach Państwowych. Należy podkreślić, że w przypadku kontroli Administrator będzie musiał wykazać odpowiednią podstawę prawną do dalszego przetwarzania danych osobowych w dokumentacji. Oczywiście art. 5 ust. 1 lit. b[48] i e[49] RODO daje możliwość dalszego przechowywania i przetwarzania danych osobowych do celów archiwalnych[50].

PODSUMOWANIE

Po pięciu latach od wejścia w życie RODO wiele się zmieniło. Coraz bardziej jesteśmy świadomi ochrony naszych danych osobowych. W Archiwach Państwowych IOD powinien pełnić istotną rolę i przede wszystkim być niezależnym od swojego kierownictwa. Zgodnie z zapisami RODO powinien on być usytuowany w strukturze organizacyjnej bezpośrednio pod dyrektorem archiwum. Niestety w żadnym Archiwum Państwowym IOD nie jest tak powołany. Nawet nowe zarządzenia Naczelnego Dyrektora Archiwów Państwowych w sprawie nadania

---

[47] M. Brzozowska-Pasieka, *RODO a okresy przechowywania dokumentacji firmowej*, „Dokumentacja ODO zgodna z RODO i najnowszymi przepisami" 2020, 45, s. 13–14.

[48] RODO art. 5 ust. 1 lit. b, tj. „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami («ograniczenie celu»)".

[49] RODO art. 5 ust. 1 lit. E, tj. „przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą («ograniczenie przechowywania»)".

[50] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. UE L nr 119, s. 1 ze zm.).

DOI:10.17951/rh.2023.55.693-715

statutu poszczególnym Archiwom Państwowym, które weszły w życie od 1 stycznia 2023 r., nie wspominają o IOD[51].

Rola i zadania IOD są bardzo duże i powinny być coraz większe. Przede wszystkim musi on nadzorować cały system zarządzania bezpieczeństwem informacji, szkolić się i być także odpowiedzialnym za szkolenie personelu zgodnie z art. 39 RODO. Oddziały kształtowania narodowego zasobu archiwalnego powinny udzielać wskazówek, jeśli chodzi o ochronę danych osobowych w archiwach zakładowych. Podczas kontroli powinno się instruować archiwistów zakładowych, w jaki sposób postępować z dokumentacją z danymi osobowymi.

Brakowanie jest dla jednostki organizacyjnej przywilejem, a nie obowiązkiem. Podejście do tego zagadnienia zmienia się. Czy jednostki organizacyjne nie narażą się na zarzut ze strony UODO, że przetrzymują dokumentację? RODO dopuszcza przetwarzanie danych osobowych dla celów archiwalnych, ale czy możemy zawsze się na nie powoływać. Jeśli mamy kategorię B5, to czy dozwolone jest jej niebrakowanie w nieskończoność? Wydaje się, że odpowiedź jest prosta, nie możemy przetrzymywać dokumentacji, jeśli jej okres przydatności już minął i według jednolitego rzeczowego wykazu akt, po zgodzie właściwego Dyrektora Archiwum Państwowego, należy ją zniszczyć.

Można pokusić się o stwierdzenie, że cała sieć Archiwów Państwowych nie dostała należytego wsparcia od NDAP. Wydaje się, że lepszym rozwiązaniem byłoby zatrudnienie jednego IOD dla wszystkich archiwów, jak to się robi w grupach kapitałowych. Przecież rola i zadania IOD w każdym archiwum są takie same. Możemy pokusić się o wniosek, że NDAP boi się kar finansowych, bo jeśli dostanie ją jeden Dyrektor Archiwum Państwowego, to nie będzie to cała sieć.

Poprzez kary finansowe UODO zyskało narzędzie do egzekwowania RODO. Można spodziewać się, że kontrole również dotrą do Archiwów Państwowych. W jaki sposób Archiwa Państwowe powinny się przygotowywać na kontrole? Kontrola w archiwach nie będzie się różniła od przeprowadzonych w innych instytucjach. Będzie sprawdzana dokumentacja związana z danymi osobowymi, m.in. upoważnienia do przetwarzania danych osobowych i ich rejestry. Czy sieć archiwalna jest przygotowana na takie kontrole i czy na pewno ochroną danych osobowych zajmują się osoby, które mają odpowiednią wiedzę i doświadczenie? Na te pytania nie ma jednoznacznej odpowiedzi. Warto podczas następnego Powszechnego Zjazdu Archiwistów Polskich zorganizować forum IOD,

[51] Nowe statuty poszczególnych Archiwów Państwowych dostępne są w Dzienniku Urzędowym Naczelnej Dyrekcji Archiwów Państwowych, https://www.gov.pl/web/archiwa/dziennik-urzedowy-rok-2022 [dostęp: 10 II 2023].

DOI:10.17951/rh.2023.55.693-715

którzy są powołani w Archiwach Państwowych. Mogliby się wymienić swoimi doświadczeniami i problemami, z którymi mierzą się w pracy.

REFERENCES (BIBLIOGRAFIA)

Printed sources (Źródła drukowane)

TK z 2.4.2007 r., SK 19/06, OTK-A 2007, Nr 4, poz. 37.

Dziennik Ustaw Rzeczypospolitej Polskiej: 1997, 2004, 2008, 2014–2016, 2018, 2020, 2023.

Dziennik Ustaw Unii Europejskiej: 1995, 2016.

Studies (Opracowania)

Brzozowska-Pasieka M., *RODO a okresy przechowywania dokumentacji firmowej*, „Dokumentacja ODO zgodna z RODO i najnowszymi przepisami" 2020, 45.

Cygan T., *Podręcznik administratora bezpieczeństwa informacji*, Wrocław 2011.

Czerniak D., *Granice obowiązywania zasady ignorantia iuris nocet w polskim procesie karnym*, „Folia Iuridica Universitatis Wratislaviensis" 2015, 4 (1).

Gałaj-Emiliańczyk K., *Administrator Bezpieczeństwa Informacji i Inspektor Ochrony Danych*, Warszawa 2017.

Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia Cywilne" 1972, 20.

Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, cz. I, „Biuletyn Administratorów Bezpieczeństwa Informacji. Ochrona Danych Osobowych" 2000, 1.

Poradnik dla początkującego inspektora ochrony danych. Jak należycie wykonywać swoje zadania? Jakie wymogi spełnić, red. M. Kowalski, Warszawa 2020.

Seweryn R., *Technologie informacyjne i komunikacyjne – wprowadzenie w problematykę, w: Technologie informacyjnej i komunikacyjne na rynku turystycznym*, red. J. Berbeka, K. Borodako, Warszawa 2017.

Szabaciuk M., *Transformacja systemów zarządzania bezpieczeństwem informacji w Polsce po 1989 r.*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2019, 17, 1.

Z życia dialogu: RODO – potrzebne choć niełatwe, red. I. Zakrzewska, Warszawa 2021.

Internet sources (Źródła internetowe)

Archiwalna strona GIODO, https://egiodo.giodo.gov.pl/index.dhtml [dostęp: 8 IV 2018].

Archiwalna strona GIODO, https://egiodo.giodo.gov.pl/search_results_ado.dhtml [dostęp: 8 IV 2018].

Archiwum „Rzeczpospolitej" https://www.parp.gov.pl/component/content/article/829-27:prawo-do-bycia-zapomnianym-czy-dane-osobowe-faktycznie-zawsze-mozna-usunac [dostęp: 27 II 2023].

Archiwum Akt Nowych, https://aan.gov.pl/formularz-pracownia/rodo.php [dostęp: 30 IV 2023].

Archiwum Akt Nowych, https://www.aan.gov.pl/ [dostęp: 25 I 2023].

Archiwum Główne Akt Dawnych, https://agad.bip.gov.pl/struktura-organizacyjna/struktura-organizacyjna-agad.html [dostęp: 30 IV 2023].

Archiwum Główne Akt Dawnych, https://agad.gov.pl/ [dostęp: 25 I 2023].

Archiwum Narodowe w Krakowie, https://ank.gov.pl/ochrona-danych-osobowych/ [dostęp: 30 IV 2023].

DOI:10.17951/rh.2023.55.693-715

Archiwum Państwowe w Białymstoku, https://www.bialystok.ap.gov.pl/p,93,polityka-prywatnosci [dostęp: 30 IV 2023].

Archiwum Państwowe w Bydgoszczy, https://apbydgoszcz.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Częstochowie, https://czestochowa.ap.gov.pl/index.php/pl/ochrona-danych-osobowych [dostęp: 30 IV 2023].

Archiwum Państwowe w Gdańsku, https://www.gdansk.ap.gov.pl/pl/top/rodo [dostęp: 30 IV 2023].

Archiwum Państwowe w Gorzowie Wielkopolskim, https://gorzow.ap.gov.pl/p,83,polityka-rodo [dostęp: 30 IV 2023].

Archiwum Państwowe w Kaliszu, https://www.archiwum.kalisz.pl/polityka-ochrony-danych-osobowych [dostęp: 30 IV 2023].

Archiwum Państwowe w Katowicach, https://archiwumkatowice.bip.gov.pl/ochrona-danych-osobowych/inspektor-ochrony-danych-archiwum-panstwowego-w-katowicach.html. [dostęp: 30 IV 2023].

Archiwum Państwowe w Kielcach, https://www.kielce.ap.gov.pl/p,96,ochrona-danych-osobowych [dostęp: 30 IV 2023].

Archiwum Państwowe w Koszalinie, https://apkoszalin.bip.gov.pl/ochrona-danych-osobowych/ [dostęp: 30 IV 2023].

Archiwum Państwowe w Koszalinie, zakładka „Ochrona danych osobowych, http://www.koszalin.ap.gov.pl/klauzule-informacyjne/ [dostęp: 23 I 2023].

Archiwum Państwowe w Lesznie, https://www.archiwum.leszno.pl/new/container/KLAUZULA-OGRANICZENIA.pdf [dostęp: 30 IV 2023].

Archiwum Państwowe w Lublinie, https://lublinarchiwum.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Łodzi, https://aplodz.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Malborku, https://malbork.ap.gov.pl/p,126,rodo [dostęp: 30 IV 2023].

Archiwum Państwowe w Olsztynie, https://apolsztyn.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Opolu, https://ap_opole.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Piotrkowie Trybunalskim, https://appiotrkow.bip.gov.pl/ochrona-danych-osobowych/klauzula-informacyjna-archiwum-panstwowego-w-piotrkowie-trybunalskim.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Płocku, https://plock.ap.gov.pl/index.php/ochrona-danych-osobowych/ [dostęp: 30 IV 2023].

Archiwum Państwowe w Poznaniu, https://poznan.ap.gov.pl/instytucja/podo/, https://appoznan.bip.gov.pl/ochrona-danych-osobowych/klauzula-informacyjna-polityki-ochrony-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Przemyślu, https://www.przemysl.ap.gov.pl/p,117,ochrona-danych-osobowych [dostęp: 30 IV 2023].

Archiwum Państwowe w Radomiu, https://www.radom.ap.gov.pl/p,91,rodo [dostęp: 30 IV 2023].

Archiwum Państwowe w Rzeszowie, https://aprzeszow.bip.gov.pl/rodo/klauzula-informacyjna-o-przetwarzaniu-danych-osobowych.html [dostęp: 30 IV 2023].

Archiwum Państwowe w Szczecinie, https://www.szczecin.ap.gov.pl/pl/polityka-ochrony-danych-osobowych [dostęp: 30 IV 2023].

DOI:10.17951/rh.2023.55.693-715

Archiwum Państwowe w Toruniu, https://aptorun.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].
Archiwum Państwowe w Warszawie, https://2564fftxyr.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].
Archiwum Państwowe w Zielonej Górze, https://apzg.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].
Archiwum Państwowe we Wrocławiu, https://apwroclaw.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].
Archiwum Państwowe w Zamościu, https://archiwumzamosc.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.htm [dostęp: 30 IV 2023].
Dziennik Urzędowy Naczelnej Dyrekcji Archiwów Państwowych, https://www.gov.pl/web/archiwa/dziennik-urzedowy-rok-2022 [dostęp: 10 II 2023].
Naczelna Dyrekcja Archiwów Państwowych, https://www.archiwa.gov.pl/o-nas/mapa-archiwow-panstwowych/ [dostęp: 25 II 2023].
Naczelna Dyrekcja Archiwów Państwowych, https://www.archiwa.gov.pl/o-nas/archiwa-panstwowe/ [dostęp: 25 II 2023].
Naczelna Dyrekcja Archiwów Państwowych, https://www.gov.pl/web/archiwa/ochrona-danych-osobowych [dostęp: 30 IV 2023].
Narodowe Archiwum Cyfrowe, https://nac.ssdip.bip.gov.pl/ochrona-danych-osobowych/ochrona-danych-osobowych.html [dostęp: 30 IV 2023].
Narodowe Archiwum Cyfrowe, https://www.nac.gov.pl/ [dostęp: 25 I 2023].
Urząd Ochrony Danych Osobowych *Czy dane kontaktowe IOD muszą być łatwo dostępne?* https://uodo.gov.pl/pl/495/2342 [dostęp: 24 IV 2023].
Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl [dostęp: 23 IV 2023].

NOTA O AUTORZE

Małgorzata Szabaciuk – doktor nauk humanistycznych, od 2011 r. adiunkt w Katedrze Archiwistyki i Nauk Pomocniczych Historii Uniwersytetu Marii Curie-Skłodowskiej w Lublinie. Absolwentka studiów podyplomowych w zakresie Zarządzania Bezpieczeństwem Informacji Szkoły Głównej Handlowej. Specjalistka w dziedzinie zarządzania dokumentacją i bezpieczeństwem informacji. Wieloletni praktyk z zakresu archiwistyki i ochrony danych osobowych. Członek zarządu Sekcji Edukacji Archiwalnej Stowarzyszenia Archiwistów Polskich oraz członek Stowarzyszenia SABI – Inspektorów Ochrony Danych.

ABOUT THE AUTHOR

Małgorzata Szabaciuk – PhD in the humanities, since 2011 assistant professor in the Department of Archival Studies and Auxiliary Sciences of History at Maria Curie-Skłodowska University in Lublin. Graduate of postgraduate studies in Information Security Management at the Warsaw School of Economics. Specialist in records management and information security. Long-term practitioner in the field of archival science and personal data protection. Member of the Board of the Archival Education Section of the Association of Polish Archivists and member of the Association of Data Protection Inspectors – SABI.

DOI:10.17951/rh.2023.55.693-715