Wydział Prawa i Administracji
Uniwersytet Śląski

mgr Stanisław Hady - Głowiak

Tytuł pracy doktorskiej:

Status prawny Inspektora Ochrony Danych jako audytora w ujęciu administracyjno-prawnym

Promotor: prof. dr hab. Marcin Janik

Katowice 2021

Streszczenie

W dysertacji przedstawiony został kompleksowo model i istota funkcjonowania IOD w ujęciu systemowym. Pokreślony został problem dotyczący potrzeby ujednolicenia regulacji dotyczących usytuowania stanowiska IOD w przepisach krajowych, zasad i kryteriów jego wyznaczenia oraz nabywania przez niego uprawnień i ich weryfikacji. Biorąc pod uwagę wyżej wymienione elementy, należy stwierdzić, że w podejściu modelowym mocno podkreślona została rola IOD, jako audytora. Kolejnym elementem jest również wskazanie nieprawidłowości i wypracowanie najlepszych praktyk i jednolitego stanowiska w zakresie prawidłowego powoływania i pozycji prawnej IOD oraz wykonywania przez niego zadań. W pracy wskazano również na konieczność wykluczenia nieprawidłowości, jakie powstały w zakresie wyznaczania jednego IOD dla kilku podmiotów, nieuwzględnienia stanowiska IOD w przepisach szczegółowych oraz przypadków powstania konfliktu interesów w realizacji zadań. Ponadto praca stanowi odpowiedź na wymogi stawiane wobec IOD w zakresie prowadzenia audytów bezpieczeństwa informacji i ochrony danych osobowych, analizy ryzyka oraz czynności doradczych/naprawczych w sytuacji wystąpienia zagrożenia lub naruszenia przepisów o ochronie danych osobowych.

Summary

The dissertation presents a comprehensive model and the essence of Data Protection Officer functioning in a systemic perspective. There has been highlighted the need to unify the regulations concerning the DPO position in national regulations, the rules and criteria of appointing him as well as acquire rights by him and their verification. Taking into account the above-mentioned elements, it should be stated that in a model approach there has been strongly underlined DPO's role as an auditor. Another element is also the identification of irregularities and development of best practices and a uniform position regarding the correct appointment and legal position of the DPO as well as performing by him tasks correctly. The study also indicates the need to exclude irregularities which arose in the field of appointing one DPO for several entities, failure to take into account the position of DPO in specific provisions and cases of uprising the conflict of interest during the implementation of tasks. In addition, the paper is a response to the requirements for the DPO position in the scope of conducting security information and personal data protection audits, risk analysis and advisory / remedial activities in the event of a possible danger or violation of the provisions of personal data protection.

Wstęp

Podmioty zarówno w obszarze sektora publicznego, jak i prywatnego są zobowiązane do ochrony interesów osób fizycznych w związku z przetwarzaniem ich danych osobowych, jak również wszelkich zasobów, w tym informacji prawnie chronionych. Karta praw podstawowych Unii Europejskiej [1] oraz Traktat o funkcjonowaniu Unii Europejskiej [2] statuują ochronę danych osobowych jako jedno z praw podstawowych. Traktat o funkcjonowaniu Unii Europejskiej powierzył Parlamentowi Europejskiemu i Radzie określenie zasad ochrony danych osób fizycznych w zakresie przetwarzania danych osobowych oraz zasad swobodnego przepływu takich danych. Zasady i przepisy dotyczące ochrony danych osobowych obowiązujące w państwach członkowskich, nie mogą jednak naruszać podstawowych praw i wolności, szczególnie ograniczać prawa do ochrony danych, niezależnie od obywatelstwa czy miejsca zamieszkania osób fizycznych, których dane są przetwarzane. Nie jest to jednak prawo bezwzględne. Prawodawca nakazuje postrzegać je w kontekście funkcji społecznej i wyważać względem innych praw podstawowych, wolności i zasad [3]. W tym miejscu nie sposób wspomnieć o najważniejszym akcie obowiązującym w polskim porządku prawnym, Konstytucji Rzeczpospolitej Polskiej, gdzie zgodnie z treścią art. 51 ust. 1 „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby” [4]. Dążenie do harmonizacji prawa ochrony danych osobowych, w ramach Unii Europejskiej, skłoniło prawodawcę europejskiego do wdrożenia jednolitych zasad stosowania i wykładni tegoż prawa. Zasady te zostały nakreślone w 173 motywach, które umieszczono w Preambule Rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych, zwane dalej RODO) [5].

---

1 Karta praw podstawowych Unii Europejskiej z dnia 7.12.2000 r. Dz. Urz. UE C 326/391

2 Traktat o funkcjonowaniu Unii Europejskiej Dz. Urz. UE C 326

3 S. Hady – Głowiak, D. Kozłowski, *Dekalog ochrony danych osobowych- stosowanie zasad przestrzegania danych osobowych jako podstawa bezpieczeństwa przetwarzanych danych* [w:] red. J. Wołejszo, K. Rejman, M. Wilczyńska, *Bezpieczeństwo informacji w organizacjach*, Kalisz 2021, str. 15

4 Art. 51 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., nr 78, poz. 483)

5 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

Wobec powyższego RODO wskazało na potrzebę edukowania osób odpowiedzialnych za bezpieczeństwo informacji i ochronę danych osobowych przez Administratorów danych osobowych i podmioty przetwarzające. Kluczową rolę w tym zakresie w każdej instytucji powinien pełnić Inspektor Ochrony Danych (zwany dalej IOD), którego status prawny, jak również ogólne zasady powołania zostały określone w RODO. Ciągle zmieniająca się rzeczywistość i przepisy prawa oraz brak możliwości funkcjonowania na rynku pracy bez nowoczesnych technologii, za pomocą których przetwarzane są dane osobowe i informacje prawnie chronione wymaga zapewnienia efektywnego nadzoru nad bezpieczeństwem wykorzystywanych w jednostce systemów informacyjnych. Tym samym osoby wyznaczone do pełnienia funkcji IOD powinny posiadać z jednej strony wiedzę i umiejętności praktyczne w zakresie właściwej interpretacji przepisów prawa i stosowania praktyk w dziedzinie bezpieczeństwa informacji i ochrony danych osobowych, w tym umiejętności przeprowadzania skutecznego badania podatności systemów informatycznych na wszelkie zagrożenia. Z drugiej strony IOD jako niezależny audytor powinien dawać zapewnienie, że systemy informatyczne użytkowane przez instytucję wypełniają wymogi wynikające z obowiązujących przepisów i norm technicznych.

Główną tezą pracy jest wykazanie modelu funkcjonowania Inspektora Ochrony Danych (zwanego dalej IOD) jako audytora. Cel główny dysertacji doprowadził do konieczności zaprezentowania celów szczegółowych takich, jak konieczność kompleksowego uregulowania w przepisach prawa krajowego wymogów kwalifikacyjnych i kryteriów ich weryfikacji niezbędnych do wykonywania zadań na stanowisku IOD, mając na uwadze funkcjonowanie IOD zarówno w jednostkach sektora finansów publicznych, jak i w sektorze prywatnym. Należy również wskazać na konieczność ujednolicenia przepisów krajowych w zakresie usytuowania stanowiska IOD w przepisach krajowych. Kolejnym elementem jest również wskazanie nieprawidłowości i wypracowanie najlepszych praktyk i jednolitego stanowiska w zakresie prawidłowego powoływania i pozycji prawnej IOD oraz wykonywania przez niego zadań. Biorąc pod uwagę wyżej wymienione elementy, należy stwierdzić, że w podejściu modelowym mocno podkreślona została rola IOD, jako audytora, a wewnątrzorganizacyjne kompetencje, uprawnienia i sposób wykonywania zadań przez IOD odniesiono do uprawnień i zadań osób kierujących komórką audytu wewnętrznego. W pracy zostaną również wykazane nieprawidłowości oraz brak przygotowania u poprzedników IOD - Administratorów Bezpieczeństwa Informacji (zwanych dalej ABI) do wykonywania zadań inspektora ochrony

danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1)

danych. Powyższe zostanie wykazane w odniesieniu do zadań w zakresie analizy ryzyka, jak również prowadzenia audytu i działań doradczych. Ukazane zostanie również dotychczasowe podejście ADO i ustawodawcy do tego tematu. Wskazana analiza będzie punktem wyjścia dla wykazania konieczności ujednolicenia przepisów oraz wskazania nowych rozwiązań prawnych i dobrych praktyk w przedmiotowym zakresie. W dysertacji zwrócono również uwagę na istotę instytucji IOD, jako gwaranta przestrzegania i stosowania przepisów o ochronie danych osobowych oraz odpowiednika i reprezentanta stanowiska Urzędu Ochrony Danych Osobowych w instytucji, a także konsekwencje braku powołania takiej osoby i powołania osób niekompetentnych. Badania podjęte w pracy miały na celu ukazanie ważnej i kluczowej roli IOD, jako doradcy oraz podmiotu monitorującego przestrzeganie przepisów o ochronie danych osobowych i identyfikującego nieprawidłowości tym zakresie oraz podejmującego odpowiednie i adekwatne działania naprawcze/zaradcze dla ADO. W pracy wykorzystano metodę dogmatyczno-prawną polegającą na analizie tekstu normatywnego. Przedstawiono poglądy wyrażone w doktrynie, w orzecznictwie i piśmiennictwie administracyjnym w zakresie badanej problematyki. W pracy wykorzystano również pewne elementy analizy prawno-porównawczej przepisów, doktryny, literatury i publicystyki prawniczej, orzecznictwa, jak również dorobku acquis i stanowisko organów kontrolnych, a następnie ukazane zostało podeście praktyczne w oparciu o syntezę i analizę obejmującą badanie dokumentacji i obserwację uczestniczącą. W ramach wykonanej analizy prawno-porównawczej w zakresie wyznaczenia statusu, jak i zadań inspektora ochrony danych uwzględniono akty prawne i rozwiązania przyjęte w poszczególnych krajach członkowskich począwszy od Dyrektywy 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 [6], a skończywszy na przepisach RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych [7]. W pracy zwrócono również uwagę na pewne elementy statystyki pozyskane w drodze informacji publicznej z UODO i organów administracji publicznej oraz w oparciu o elementy praktyczne związane z realizacją audytów bezpieczeństwa informacji i ochrony danych osobowych w jednostkach administracji publicznej oraz podmiotach prywatnych. W ramach prezentowanych statystyk przedstawiono liczbę skarg kierowanych do

6 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.1995.281.31)

7 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych Dz. U. z 2019 r., poz. 1781, t. j.

Urzędu Ochrony Danych Osobowych i jego poprzednika GIODO, jak również zrealizowanych przez ten organ kontroli, a także kontroli przeprowadzonych przez inne organy państwowe, takie jak NIK.

Mając powyższe na uwadze należy stwierdzić brak jednoznacznych wytycznych i odpowiedniego przygotowania przepisów krajowych oraz ich ciągłe zmiany pomimo dwuletniego okresu na wdrożenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwane dalej RODO) [8]. Powyższe spowodowało częste ich nadinterpretacje oraz nieprawidłowości. Praca ma na celu wskazanie na konieczność ujednolicenia przepisów oraz wskazanie nowych rozwiązań prawnych w przedmiotowym zakresie. W pracy omówione zostaną zasady prawidłowego powoływania i usytuowania IOD zarówno w odniesieniu do podmiotów publicznych, jak i prywatnych ze szczególnym uwzględnieniem zarówno organów administracji publicznej (organów administracji rządowej i samorządowej), jak również państwowych jednostek organizacyjnych nieposiadających osobowości prawnej i innych jednostek, w stosunku do których brak jest odniesienia w tym zakresie w przepisach krajowych w ujęciu sektorowym. Przedstawione zostaną również nieprawidłowości, jakie powstały w zakresie wyznaczania jednego IOD dla kilku podmiotów, czy dotyczące nieuwzględnienia stanowiska IOD w przepisach szczegółowych. W oparciu o powyższe zostaną również omówione zagadnienia niezależności IOD w instytucji i rola ADO w tym zakresie oraz odpowiedzialności IOD, a także dobre praktyki zapewniające, by zadania i obowiązki wykonywane na innym stanowisku przez IOD nie powodowały konfliktu interesów. Z kolei obsługa klienta zewnętrznego i wewnętrznego przez IOD we wszystkich sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO zostanie oparta w szczególności na stanowisku doktryny i publicystyki. Celem wskazanej analizy jest wypracowanie najlepszych praktyk i jednolitego stanowiska w zakresie prawidłowego powoływania i usytuowania IOD oraz współpracy z klientem zewnętrznym i wewnętrznym we wszystkich sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

8 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 (Dz.U.UE.L.2016.119.1)

W dalszej części pracy omówione zostaną kwalifikacje i kompetencje wymagane na stanowisku IOD i zasady ich weryfikacji. Wskazana zostanie również potrzeba wprowadzenia stosownych zmian przepisów krajowych w tym zakresie mając na uwadze realizację zadań zapewniających i związanych z tym audytów w aspekcie teoretycznym oraz praktycznym. Nieodzownym elementem części praktycznej będzie ukazanie wymaganych kompetencji i realizowanych zadań IOD poprzez zobrazowanie realizacji zadania audytowego oceniającego aktualny stan bezpieczeństwa jednostki i ochrony danych osobowych w ujęciu sektorowym (sektor publiczny i prywatny). Omówiona zostanie istota, metodologia i zasady prowadzenia audytu w oparciu o obowiązujące przepisy (RODO, KRI) i normy (m.in. IOS/IEC 27001), rola, kompetencje i pozycja IOD jako audytora w tym zakresie, analogicznie jak ma to miejsce w przypadku audytora wewnętrznego. Przedstawione zostaną poszczególne etapy zadania audytowego i zastosowana metodologia oraz elementy dokumentacji wymaganej przeprowadzenia audytu, tj. ankieta/formularz zawierający pytania kontrolne niezbędne do przygotowania planu i programu zadania audytowego i jego zakresu, a także raport-sprawozdanie zawierające wnioski, zidentyfikowane ryzyka i rekomendacje po przeprowadzonym audycie. W pracy opisano narzędzia i techniki służące do przeprowadzenia zadania zapewniającego pomocne dla IOD oraz wskazano kryteria służące do oceny ustaleń stanu faktycznego. Wyżej wymienione elementy zostały uwzględnione w pracy w celu zrozumienia wymogu kompleksowego podejścia do przeprowadzenia zadania audytowego przez IOD, jako audytora wiodącego posiadającego niezbędną wiedzę i kompetencje w tym zakresie. Działania doradcze zostały ograniczone do obszarów związanych z ochroną danych osobowych w procesie zatrudnienia w zakresie pracy zdalnej i stosowania monitoringu wizyjnego oraz roli IOD w zakresie prawidłowego udostępniania i powierzania danych osobowych mając na uwadze zmieniające się obecnie przepisy w tym zakresie, ochronę prywatności jednostki i ukazanie specyfiki i istoty funkcjonowania IOD w ujęciu systemowym. Na koniec ukazano rolę IOD w przypadku wystąpienia incydentów i naruszeń w organizacji.

Praca została podzielona na 4 rozdziały zawierające zagadnienia teoretyczne oraz praktyczne, o których mowa powyżej.

Rozdział I Geneza instytucji IOD

W niniejszym rozdziale przedstawiono kształtowanie się instytucji Inspektora Ochrony Danych poczynając od roli urzędnika ds. ochrony danych osobowych zgodnie z Dyrektywą 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 (zwaną dalej dyrektywą 95/46/WE) [9]. Kolejnym etapem, jaki wyróżniono było dostosowywanie polskich przepisów i funkcji Administratora Bezpieczeństwa Informacji (zwanego dalej ABI) do RODO.

I.1. Instytucja Administratora Bezpieczeństwa Informacji jako urzędnika do spraw ochrony danych osobowych

Pozycja ABI wyznaczona została przepisami dyrektywy 95/46/WE. Podstawy jego funkcjonowania regulował art. 18 ww. dyrektywy [10]. Dyrektywa zaś była rezultatem funkcjonowania przez wiele lat konwencji nr 108 Rady Europy sporządzonej w Strasburgu 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych [11]. Część organizacji zdecydowała się mimo braku stosownych przepisów na wyznaczenie osób do nadzoru nad prawem do prywatności osób, których dane dotyczą. Początkowo osoby te wykonywały zadania najczęściej jako dodatkowe zajęcie w ramach realizacji szerszego zakresu obowiązków compliance. Jednak obowiązki związane z nadzorem nad tym obszarem zaczęły przeważać i ostatecznie pojawiła się na gruncie dyrektywy 95/46/WE funkcja inspektora ochrony danych [12]. W dyrektywie umożliwiono wprowadzenie w prawie krajowym przepisów przewidujących wyznaczenie przez administratorów urzędnika do spraw ochrony danych osobowych (zwanego dalej urzędnikiem ds. ODO). Urzędnik ds. ODO miał obowiązek zapewnić niskie prawdopodobieństwo wywierania przez czynności

9 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych Dz.U.UE.L.1995.281.31

10 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, Lex/el. 2018, dostęp z dnia 29.11.2019 r.

11 Konwencja nr 108 Rady Europy sporządzonej w Strasburgu 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz. U. z 2003 r., nr 3, poz. 25)

12 K.Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów,* ODDK Gdańsk 2018, str. 14-15

przetwarzania niekorzystnego wpływu na prawa i wolności osób, których dane dotyczą. Zgodnie z powyższym urzędnik do spraw ochrony danych osobowych odpowiedzialny był w świetle art. 18 ust. 2 dyrektywy w szczególności za zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy ww. dyrektywy oraz za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych, zapewniając przy tym, że nie zostaną naruszone prawa i wolności osób, których dane dotyczą [13]. Rejestr operacji przetwarzania danych wykonywanych przez administratora danych zawierał informacje identyfikujące administratora danych, określające cel przetwarzania danych, opis kategorii osób, których dane dotyczą oraz danych lub kategorii danych, które się do nich odnoszą, informacje dotyczące odbiorcy lub kategorii odbiorców, którym dane mogą być ujawnione oraz propozycje przekazania danych do państw trzecich. Dyrektywa 95/46/WE w art. 18 ust. 2 dopuściła jednak możliwość zwolnienia administratora danych z obowiązku zawiadamiania organu nadzorczego (według polskiej ustawy o ochronie danych osobowych – obowiązku zgłaszania zbiorów do zarejestrowania) wówczas, gdy administrator danych powołał „urzędnika" do spraw ochrony danych osobowych.

Z góry zatem założono, że inspektor ochrony danych (zwany dalej IOD), nazywany wówczas w literaturze polskiej ABI, miałby być organem kontroli wewnętrznej, gwarantującym prawidłowość przetwarzania danych osobowych przez administratora danych, będącym alternatywą dla obowiązku zgłaszania zbiorów danych do zarejestrowania [14].

W znacznej części ustawodawstw krajów UE wprowadzono nową nieformalną funkcję wewnętrznego urzędnika ds. ODO. Każdy kraj nieco inaczej określił warunki powołania takiej funkcji w organizacji oraz zakresy jej obowiązków. Przykładowo we Francji wyznaczenie tej funkcji – Correspondant Informatique et Libertes (CIL) – było całkowicie fakultatywne, a do zakresu jej obowiązków należało m.in. informowanie o prawach przysługujących osobom, których dane dotyczą [15]. Niemiecka ustawa o ochronie danych stanowi doskonały przykład wdrożenia w ustawodawstwie krajowym dyrektywy 95/46/WE. I tak zgodnie z § 4 f ust. 1 ustawy federalnej prywatne przedsiębiorstwa miały obowiązek wyznaczyć wewnętrznego urzędnika do spraw ochrony danych osobowych, jeżeli zatrudniają na stałe 10 lub więcej osób

13 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, Kontroler Info nr 5 z 2016r., str. 55

14 E. Kulesza, Problem niezależności inspektora ochrony danych [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019, str. 111

15 K.Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 15-16

zajmujących się zautomatyzowanym przetwarzaniem danych osobowych. Jak wyraźnie wskazano w dyrektywie, zdolność do osiągnięcia tego celu wymaga pewnej niezależności stanowiska urzędnika w ramach organizacji administratora [16].

W niemieckim porządku prawnym obowiązek zgłaszania zbiorów do zarejestrowania jako forma kontroli prawidłowości przetwarzania danych osobowych przez administratora danych krytykowany był od dawna. Uznawano bowiem, że jest to źródło zbędnej biurokracji i dodatkowych kosztów ponoszonych przez administratorów danych (zwanych dalej ADO). Jako alternatywę dla tak sformułowanych obowiązków przyjęto w niemieckich przepisach możliwość wyboru przez administratorów danych albo w ramach kontroli wstępnej zgłaszanie zbiorów do zarejestrowania do organu nadzorczego, albo powołanie zakładowego rzecznika ochrony danych jako podmiotu niezależnego od pracodawcy – ADO, który miał administratora danych wspomagać w ochronie danych, być swego rodzaju łącznikiem pomiędzy organem nadzorczym a administratorem, a jako siła fachowa zajmować się szkoleniami, prowadzeniem dokumentacji i podejmowaniem wszystkich innych działań w zakresie ochrony danych osobowych. Szczególna funkcja wykonywana przez „zakładowych" inspektorów polegała także na obowiązku wspierania i chronienia interesów osób, których dane były przetwarzane, co skutkowało nazywaniem inspektorów „zakładowych" w literaturze dotyczącej ochrony danych osobowych „adwokatami" podmiotów danych (osób, których dane były przetwarzane). Z tego też względu przepisy gwarantowały niezależność działania zakładowych inspektorów oraz zakaz ich karania, czy szykanowania za podejmowane działania. Wymaga podkreślenia, że owe działania zakładowych inspektorów skierowane były nie tylko na prawidłowe, zgodne z przepisami przetwarzanie danych osobowych przez administratora danych, ale także na realizowanie istoty i filozofii ochrony danych – zagwarantowanie prawa do prywatności i prawa do ochrony danych podmiotom danych. Stąd konieczność zawarcia w przepisach prawa gwarancji niezależności ich działania przez zakaz karania bądź szykanowania za podejmowane działania [17]. Należy jednoznacznie stwierdzić brak stosownych regulacji w polskim porządku prawnym dotyczących zakazu karania ABI, a następnie IOD za podejmowane działania, co istotnie podniosłoby rangę i niezależność tego stanowiska. Powyższe potwierdza obecny kształt ustawy federalnej Niemiec [18], gdzie w § 6 oprócz wymogów niezależności, wynikających

16 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, *op. cit.,* str. 55

17 E. Kulesza, Problem niezależności inspektora ochrony danych, op. cit., str. 111-112

18 Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44, ausgegeben zu Bonn am 5. Juli 2017, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf#__bgbl__

z RODO wskazano, iż rozwiązanie stosunku pracy z Inspektorem jest niedozwolone, chyba że istnieją fakty uzasadniające rozwiązanie przez organ publiczny z ważnej przyczyny bez zachowania okresu wypowiedzenia. Wskazano również, że po zakończeniu działalności IOD stosunek pracy nie może zostać rozwiązany w ciągu jednego roku, chyba że organ publiczny jest uprawniony do rozwiązania umowy z ważnego powodu bez zachowania okresu wypowiedzenia. Ponadto jeżeli IOD dowie się o danych w swojej działalności, w odniesieniu do których kierownictwo lub osoba zatrudniona przez organ publiczny ma prawo odmówić złożenia zeznań z przyczyn zawodowych, to ma to również zastosowanie do IOD oraz podległych mu pracowników. W zakresie, w jakim rozszerza się prawo inspektora ochrony danych do odmowy przedstawienia dowodów, jego akta i inne dokumenty podlegają zakazowi konfiskaty [19].

Na mocy noweli z dnia 22 stycznia 2004 r. do poprzednio obowiązującej wersji ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. [20] (zwanej dalej u.o.d.o.) w art. 36 ust. 3 ustawy została dodana regulacja stwarzająca możliwość wyznaczenia administratora bezpieczeństwa informacji (ABI), którego zadaniem było nadzorowanie przestrzegania zasad ochrony danych, chyba że administrator danych sam wykonywał czynności nadzorcze [21].

Ustawodawca polski wprowadzając do u.o.d.o. regulację dotyczącą ABI w dużej mierze wzorował się na rozwiązaniach przyjętych w niemieckim porządku prawnym, który stanowił i do dziś dnia jest doskonałym przykładem wdrażania rozwiązań niezbędnych do przyjęcia dzisiejszego kształtu funkcjonowania IOD, co zostanie szczegółowo omówione w kolejnych punktach niniejszego rozdziału. Należy podkreślić, że przyjęte rozwiązania polegały m.in. na zniesieniu obowiązku zgłaszania zbiorów do zarejestrowania, po przyjęcie roli inspektora jako fachowego łącznika pomiędzy organem nadzorczym a administratorem, zajmującego się szkoleniami, prowadzeniem dokumentacji i podejmowaniem wszystkich innych działań w zakresie ochrony danych osobowych gwarantujących poszanowanie prawa do prywatności i prawa do ochrony danych podmiotom danych, a kończąc na jego bezpośredniej podległości ADO, czy gwarancji niezależności działania inspektora. Jednakże w polskim porządku prawnym nie wprowadzono kluczowych z punktu funkcjonowania ABI, a następnie IOD gwarancji dotyczących zakazu jego karania, szykanowania za podejmowane działania do

%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1589796091814, dostęp z dnia 18.05.2020 r.

19 https://dsgvo-gesetz.de/bdsg/ , dostęp z dnia 18.05.2020 r.

20 Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Dz. U. z 2002 r., nr 101, poz. 926 z późn zm.

21 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, op. cit., str. 56

zakazu zwolnienia i odmowy składania zeznań włącznie. W polskim porządku prawnym przyjęto zasadę dobrowolności powołania ABI, co dopiero stało się obowiązkiem po wejściu w życie RODO, co w porównaniu do ustawodawstwa obowiązującego w Niemczech w perspektywie czasu nie okazało się właściwym rozwiązaniem.

I.2. Funkcjonowanie Administratora Bezpieczeństwa Informacji jako poprzednika Inspektora Ochrony Danych

W Polsce rozbudowane regulacje dotyczące zasad i warunków pełnienia funkcji ABI, wprowadzone nowelizacją u.o.d.o. z 2014 r., stworzyły zarówno osobom pełniącym tę funkcję, jak i administratorom danych, szansę na dobre przygotowanie się do stosowania przepisów RODO w tym zakresie. Podczas prac nad wspomnianą nowelizacją znany był już bowiem projekt tej nowej unijnej regulacji, dzięki czemu wiele aspektów w zakresie statusu ABI mogło zostać zbliżone do rozwiązań przyjętych w RODO [22].

Nie oznacza to jednak, że status i zadania IOD są zupełną nowością dla polskich administratorów i ABI. Możliwość swoistego przygotowania się do nowych regulacji przyniosła bowiem nowelizacja u.o.d.o. dokonana ustawą z dnia 7.11.2014 r. o ułatwieniu wykonywania działalności gospodarczej [23], która od 1.01.2015 r. istotnie zmieniła model funkcjonowania ABI. Nowe przepisy oprócz wprowadzenia dobrowolności powołania ABI przez administratora danych, wskazania wymogów wobec osób pełniących tę funkcję, czy określenia ich usytuowania w strukturze administratora danych, wyczerpująco zdefiniowały jego zadania, do których przede wszystkim należy zapewnienie przestrzegania przepisów o ochronie danych osobowych [24].

Powołanie ABI nie było obligatoryjne, a nawet jego powołanie nie ograniczało odpowiedzialności administratora za procesy dotyczące przetwarzania danych osobowych, zatem administratorzy często korzystali z możliwości niepowoływania go [25]. Powyższe rozwiązanie należy ocenić negatywnie, o czym wspomniano już wcześniej.

---

22 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, Informacja w Administracji Publicznej 2018 r., nr 1, str. 10, Legalis.pl, dostęp z dnia 28.05.2020 r.

23 Ustawa z dnia 7.11.2014 r. o ułatwieniu wykonywania działalności gospodarczej Dz. U. z 2014r., poz. 1662 z późn. zm.

24 E. Bielak-Jomaa, *Inspektor ochrony danych,* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, WKP, Warszawa 2018, str. 768

25 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

W związku z powyższym przed dniem wejścia w życie zmian wprowadzonych nowelizacją z dnia 7 listopada 2014 r., wyznaczenie ABI dotyczyło nie tylko administratorów, którzy przetwarzają dane w systemach informatycznych (jak było to pod rządami poprzedniego rozporządzenia), ale także administratorów przetwarzających dane w tradycyjnych zbiorach danych (ręcznie). Nieuchronnie pojawiła się dyskusja, czy każdy administrator danych musi wyznaczyć osobę do pełnienia funkcji ABI w swojej organizacji. W praktyce funkcja ta najczęściej pojawiała się w podmiotach sektora publicznego jako dodatkowe obowiązki przydzielane pracownikowi, który na co dzień zajmował się czymś zupełnie innym. Funkcję ABI obejmowały najczęściej osoby czuwające nad sprawami kadrowymi lub też informatycy nadzorujący systemy informatyczne. Przyjęte rozwiązanie i brak jednoznacznych ustawowych gwarancji niezależności i wykluczenia możliwości wystąpienia konfliktu interesów w sposób oczywisty prowadziło do sytuacji, w której osoba ta mogła sama siebie nadzorować. W tamtym czasie osoba pełniąca funkcję ABI zajmowała się realizacją wszystkich obowiązków, które należały do organizacji, a wynikały z ustawy o ochronie danych osobowych. Innymi słowy: kierownictwa podmiotów wyznaczały ABI po to, by nie zajmować się tym obszarem samodzielnie. Wskazane podejście stoi w sprzecznością z istotą tego, stanowiska, co może prowadzić do sytuacji, gdzie ABI będzie nadzorował własne działania. Dyskusja o konieczności wyznaczania ABI trwała dość długo, ze zmiennym skutkiem, gdyż dopiero na początku 2014 r. NSA rozwiał wszelkie wątpliwości w tej materii. Zgodnie z tezą wyroku NSA z dnia 21 lutego 2014 r. I OSK 2445/12 ostatecznie doprecyzowano, że osoby prawne muszą wyznaczyć ABI w organizacji, a podmiotami zwolnionymi z tego obowiązku są jednoosobowe działalności gospodarcze i spółki cywilne [26]. W praktyce funkcja ABI była często powierzana osobom mającym już inne obowiązki, co sprawiało, że efektywne wykonywanie tej funkcji mogło być trudne [27].W przepisach dotychczas obowiązującej ustawy nie określono jednak szczegółowo zakresu obowiązków ABI. Ustawodawca ograniczył się tylko do ogólnego stwierdzenia, że ABI ma nadzorować przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 u.o.d.o. Z tego sformułowania można było jedynie wyprowadzić wniosek, iż obowiązkiem ABI było nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. ABI powinien nadzorować przede wszystkim zabezpieczenie danych przed ich udostępnieniem osobom

26 K.Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.*, str. 16-17

27 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu,* Wolters Kluwer, Warszawa 2019, str. 149

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Mając powyższe na uwadze należy tutaj przytoczyć definicję nadzoru, który polega na kontroli połączonej z możliwością stosowania środków władczych, a więc wiążącego oddziaływania. Od czasów średniowiecza, nadzór stanowił formę sprawowania „pieczy" przez samodzielnego władcę nad podległą mu administracją państwa. Nadzór zawsze wykorzystywany był w celu wymuszenia przestrzegania prawa przez organy administracji. Wraz z rozwojem nowoczesnej administracji nadzór zachował swoje wcześniejsze znaczenie. Ponownie służyć miał kontrolowaniu należytego przestrzegania prawa przez organy administracji niższych szczebli. Z chwilą wykształcenia się w państwie struktur samorządu terytorialnego i przejęciem przez jego organy części zadań publicznych, nadzór zaczął być wykorzystywany jako środek do sprawdzania i kontrolowania wykonywania przez te organy zadań publicznych. Organy administracji centralnej uzyskały więc możliwość dopilnowania, czy organy samorządu terytorialnego wykonując zadania publiczne, czynią to w należyty sposób, czy uzyskały środki, dzięki którym mogły kontrolować przestrzeganie prawa. Obecnie istniejący nadzór nad samorządem terytorialnym bardzo mocno łączy się z kwestią niezależności i samodzielności w działaniu tego samorządu [28].

Według słownika języka polskiego pojęcie nadzór oznacza: „dozorowanie, strzeżenie, pilnowanie kogo lub czego, opieka, kontrola". Natomiast kontrola oznacza: „porównywanie stanu faktycznego ze stanem wymaganym, rozpatrywanie czego, wgląd w co, nadzór nad kim albo nad czym". Sens znaczeniowy nadzoru wiąże się zatem z dwoma płaszczyznami oddziaływania tj. ingerencją oraz opieką (pieczą) [29].

Mimo, że regulacje prawne wielokrotnie posługują się pojęciem nadzoru, to brak jest jego definicji normatywnej. Lukę tę stara się wypełnić doktryna, definiując nadzór jako uprawnienie organu nadrzędnego do wywierania wpływu na działalność organu podporządkowanego. Możliwość władczego ingerowania w działalność jednostki nadzorowanej wynika z regulacji prawnych oraz wzajemnych relacji pomiędzy nadzorującym i nadzorowanym. Szczególnym uprawnieniem władczym jest prawo kontrolowania i oceniania

28 Sikora Kamil, *Rola nadzoru w funkcjonowaniu administracji publicznej* [online]. Studia Iuridica Lublinensia, 2004, nr 3. str. 208, 2020-07-23 15:03 [dostęp: 2020-08-23 11:15]. Dostępny w Internecie: https://sip.lex.pl/#/publication/151054671

29 B. Pilc, *Rola administratora bezpieczeństwa informacji podczas inspekcji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych*, (dodatek MOP 7/2012) MOP 2012, Nr 7, str. 1038, Legalis.pl, dostęp z dnia 28.05.2020 r.

prawidłowości działań jednostek nadzorowanych pod względem zgodności z prawem i wyznaczonymi celami oraz wytycznymi sposobu ich realizacji [30].

W nauce prawa administracyjnego termin nadzór używany jest więc najczęściej do określenia sytuacji, w której organ nadzorujący jest wyposażony w środki oddziaływania na postępowanie organów czy też jednostek nadzorowanych. Oczywiście to władcze oddziaływanie odbywa się bez możliwości wykonywania za te organy obowiązków nałożonych na nie, czyli bez możliwości przejmowania ich kompetencji przez podmiot nadzorujący. Podmiot nadzorujący, na podstawie przyznanych mu w oparciu o powszechnie obowiązujące przepisy prawa, środków nadzoru (czyli uprawnień do władczego oddziaływania na organ lub jednostkę organizacyjną nadzorowaną) ma prawo do przeprowadzenia kontroli oraz w następstwie jej przeprowadzenia, wydania rozstrzygnięcia nadzorczego, które będzie wiążące dla podmiotu objętego nadzorem i będzie wpływało (modyfikująco) na sposób jego funkcjonowania. W skład uprawnień nadzorczych wchodzą więc środki nadzoru, które w nauce prawa administracyjnego dzielimy na środki oddziaływania merytorycznego oraz środki oddziaływania personalnego [31].

Celem nadzoru jest nie tylko zapewnienie przestrzegania prawa przez jednostki podległe lub nadzorowane, ale także zagwarantowanie realizacji ich celów i zadań. Negatywnie oceniane powinny być zarówno działania jednostek nadzorowanych, które są niezgodne z prawem, jak i te, które są nieskuteczne, mimo iż są legalne [32].

Nadzór nad prawem miejscowym samorządu terytorialnego (w zakresie wyłącznie ich zgodności z ustawami) realizują: Prezes Rady Ministrów, wojewodowie, a w zakresie spraw finansowych – również regionalne izby obrachunkowe. Natomiast nadzór nad prawem miejscowym terenowej administracji rządowej sprawują właściwi rzeczowo ministrowie [33].

Zatem ABI powinien więc mieć zapewnioną możliwość reagowania w sytuacjach zagrożenia, czy też naruszenia zasad ochrony danych osobowych. ABI mógł być pracownikiem administratora danych, ale mogła to być również osoba zatrudniona na podstawie umowy

30 *Analiza wybranych obszarów funkcjonowania nadzoru w administracji rządowej*, KPRM, Warszawa 2012, str. 4

31 A. Gołębiowska, A. Kociołek – Pęksa, *Kontrola i nadzór w prawie administracyjnym – wybrane zagadnienia teoretycznoprawne i dogmatycznoprawne,* Zeszyty Naukowe SGSP 2018, Nr 67/3/2018, str. 44 - 45

32 Analiza wybranych obszarów funkcjonowania nadzoru w administracji rządowej, KPRM, Warszawa 2012, str. 5

33 J.Zaleśny, *Prawo miejscowe* [w:] *Słownik pojęć w administracji publicznej,* red. I.Wieczorek, J.Szymanek, NIST, Łódź 2018, str. 171

cywilnoprawnej (np. zlecenia) - przepisy nie rozstrzygały tej kwestii. Niewątpliwie jednak bezpieczniejsze dla administratora było pierwsze ze wskazanych powyżej rozwiązań. W praktyce funkcja ABI jest i była niekiedy łączona ze sprawowaniem innych funkcji, np. pełnomocnika ds. ochrony informacji niejawnych. Choć formalnie nie ma przeszkód do przyjmowania takiego rozwiązania, jednak niekiedy mogło prowadzić to do sytuacji, w której ABI musiał nadzorować własne działania. Szczególnie wyraźnie widoczne było to w sytuacji, gdy ABI był Administrator Systemu Informatycznego (zwany dalej ASI). Z tego względu lepszym rozwiązaniem było wyznaczanie ABI spośród pracowników, którzy nie są zatrudnieni przy przetwarzaniu danych. W literaturze postulowało się, aby przyznać ABI pozycję niezależną od pionu służb informatycznych i podległość np. bezpośrednio dyrektorowi a nie kierownikowi działu informatyki. Są to niewątpliwie postulaty uzasadnione, lecz w praktyce niekiedy trudne do spełnienia, głównie ze względów finansowych [34]. Na początku niniejszego rozdziału wspomniano również o rozwiązaniu, gdzie zadania te wykonywały również osoby jako dodatkowe zajęcie w ramach realizacji szerszego zakresu obowiązków compliance, które mogą być zbieżne w zakresie zapewnienia zgodności działań struktury z przepisami o ochronie danych osobowych.

W hierarchii służbowej ABI podlegał bezpośrednio kierownikowi jednostki organizacyjnej (np. zarządowi) lub osobie fizycznej będącej administratorem danych [35]. Jednak należy tu zaznaczyć, że była to jedynie funkcja nie wyszczególniona w strukturze organizacyjnej podmiotu, co w rzeczywistości nie pozwalało ABI na podejmowanie realnych działań nadzorczych.

Artykuł 36 ust. 3 u.o.d.o.z 1997 r. nie zawierał także jakichkolwiek kompetencji gwarantujących ABI możliwość samodzielnego działania, w tym rzeczywistego nadzorowania przestrzegania zasad ochrony danych. Jak–zauważa E.Kulesza, powyższe było negatywnie komentowane w literaturze przedmiotu [36], co jednoznacznie potwierdza postawioną tezę.

Wątpliwości pojawiały się m.in., gdy chodziło o to, czy administrator danych mógł wyznaczyć więcej niż jednego ABI. P. Barta i P. Litwiński wskazali że wykładnia językowa jednoznacznie przemawia za wyznaczeniem jednego ABI, natomiast powołanie więcej niż jednego ABI nie jest dopuszczalne. Wskazani Autorzy opowiadali się natomiast za tworzeniem

34 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, op. cit., str. 57

35 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

36 E. Kulesza, *Problem niezależności inspektora ochrony danych, op. cit.,* str. 112

"wewnętrznej struktury podległej ABI'emu". Nie podzielam wskazanego wyżej poglądu, ponieważ sformułowanie zawarte w komentowanym przepisie nie wykluczało możliwości powoływania więcej niż jednego ABI, a w praktyce wyznaczenie kilku osób jako pełniących tę funkcję było rozwiązaniem zasadnym. Należy tu mieć na uwadze rozbudowaną strukturę organizacyjną administratora, gdzie procesy przetwarzania danych dokonywane są w miejscach znacznie od siebie oddalonych. Innym przykładem będzie sytuacja, gdzie jedna osoba miała nadzorować zabezpieczenia tradycyjnie przetwarzanych danych, a inna osoba sprawować nadzór nad przetwarzaniem danych w systemach informatycznych. Oczywiście komentowany przepis nie wykluczał również możliwości tworzenia wewnętrznej struktury organizacyjnej podległej ABI. Wyznaczenie ABI powinno mieć formę pisemną, choć brak regulacji prawnej w tym zakresie, warto było o to zadbać ze względów dowodowych. Wyznaczenie ABI powinno znaleźć także odzwierciedlenie w indywidualnym zakresie czynności, czy obowiązków - osoby wyznaczonej [37]. Wyodrębnienie ABI w strukturze organizacyjnej podmiotu oraz przygotowanie dla niego zakresu obowiązków przez Kierownika jednostki należy ocenić pozytywnie. Pozwalało to bowiem na zapewnienie ABI niezależności i realizację zadań nadzorczych ABI w zakresie przestrzegania przepisów w zakresie ochrony danych osobowych.

Pewne gwarancje niezależności działania ABI oraz dość szerokie kompetencje dała administratorowi bezpieczeństwa informacji nowelizacja ustawy o ochronie danych osobowych z dnia 7.11.2014 r [38]. Nowelą, o której mowa powyżej wprowadzono zmiany dotyczące m.in. pozycji prawnej administratora bezpieczeństwa informacji, zakresu wykonywanych przez niego zadań, jak również wymogów ustawowych niezbędnych do wykonywania zadań na tym stanowisku. Jeżeli chodzi o zakres wykonywanych zadań to zostały one w porównaniu do dotychczas obwiązującej regulacji szczegółowo określone w art. 36 a ust. 2 powołanej ustawy [39].

Zgodnie z art. 36a ust. 2 u.o.d.o. zadania ABI można było podzielić na dwie kategorie: zapewnianie przestrzegania przepisów o ochronie danych osobowych oraz prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych [40]. Rejestr, o którym

37 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, op. cit., str. 57

38 E. Kulesza, *Problem niezależności inspektora ochrony danych* , op. cit., str. 112-113

39 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, op. cit., str. 57

40 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań* (dodatek MOP 20/2016) MOP 2016, Nr 20, str. 80, Legalis.pl, dostęp z dnia 28.05.2020

mowa powyżej był jawny. Sam rejestr zawierał elementy wymagane przepisami uchylonej już Dyrektywy 95/46/WE, jak również wymaganego obecnie rejestru czynności przetwarzania. Zapewnianie przestrzegania przepisów o ochronie danych osobowych ABI realizował poprzez:
a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zadanie polegające na sprawdzaniu zgodności przetwarzania danych osobowych z prawem oraz opracowanie w tym zakresie sprawozdania dla administratora zostało szczegółowo opisane zarówno w przepisach u.o.d.o., jak i w przepisach wykonawczych. W art. 36 c u.o.d.o. wymienione były obligatoryjne elementy sprawozdania, które ABI przygotowywał po dokonaniu audytu prawidłowości przetwarzania danych. Natomiast sposób i tryb przeprowadzania sprawdzenia i przygotowywania sprawozdania zostały uregulowane w rozporządzeniu dotyczącym realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych. Jeżeli chodzi o zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych to nie doczekało się ono szczegółowej regulacji. Ogólne sformułowanie tego obowiązku powoduje, że może on być interpretowany w różny sposób: albo jako obowiązek zapewnienia, aby osoby upoważnione do przetwarzania danych same zapoznały się z przepisami o ochronie danych, albo jako obowiązek takich działań, aby to ABI zapoznawał osoby upoważnione do przetwarzania danych osobowych z przepisami o ochronie danych (np. poprzez przeprowadzanie szkoleń) [41].

Zdecydowanie bardziej precyzyjnie zadanie to zostało określone w RODO jako działania Inspektora ochrony danych zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Powyższe wskazuje nie tylko na zwiększenie świadomości personelu, ale na stałym monitorowaniu oraz minimalizacji ryzyka w tym zakresie poprzez zadania audytowe. Szczegółowo zagadnienia te zostaną omówione w trzecim rozdziale niniejszej pracy.

r.

41 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, op. cit.

Administrator danych mógł również powierzyć ABI dodatkowe zadania lub obowiązki, pod warunkiem, że będą wykonywane w sposób niekolidujący z zadaniami podstawowymi, wskazanymi w art. 36 a ust. 2 ustawy, które mają priorytet wykonania. Wśród zadań dodatkowych ABI można wskazać:

1) przygotowanie i aktualizację dokumentacji,
2) nadawanie upoważnień do przetwarzania danych osobowych,
3) prowadzenie ewidencji osób upoważnionych,
4) zgłoszenia zbiorów zawierających dane wrażliwe do rejestru GIODO,
5) przygotowanie i procesowanie wniosków o transfer danych do kraju trzeciego lub kompletowanie dokumentacji, na podstawie której transfer do krajów trzecich może odbywać się bez konieczności uzyskania zgody GIODO,
6) przygotowanie treści upoważnień, klauzul, umów, itp [42].

Podsumowując, ustawowe zadania ABI były uregulowane dosyć szczegółowo. Zadania te polegały przede wszystkim na działaniach wewnątrz organizacji, a charakter częściowo zewnętrzny ma jedynie przeprowadzenie sprawdzenia na wniosek GIODO i przygotowanie sprawozdania w tym zakresie. W polskich przepisach nie przewidziano takich zadań ABI, które wymagałyby kontaktu z osobami, których dane dotyczą [43].

Przyjęte w nowelizacji regulacje, zwłaszcza ustawowo określone zadania ABI, obowiązek zapewnienia środków i organizacyjnej odrębności, jak też podleganie bezpośrednio kierownikowi jednostki organizacyjnej bądź osobie będącej administratorem danych, zostały ocenione w literaturze jako wyraz niezależności działania i gwarancje prawidłowego wykonywania zadań przez administratora bezpieczeństwa informacji, co nie do końca odzwierciedlało rzeczywistość [44]. Negatywnie ocenić należy brak jednoznacznych rozwiązań ustawowych wykluczających możliwość wystąpienia konfliktu interesów, jak ma to miejsce w RODO w przypadku IOD.

Jeżeli chodzi zaś o uprawnienia ABI to zgodnie z przepisami posiadał prawo do:

1) przeprowadzania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych,
2) definiowania standardów,

42 M. Kołodziej, *Powołanie administratora bezpieczeństwa informacji* [w:] Maciej Kołodziej (red.), *Vademecum administratora bezpieczeństwa informacji*, C. H. Beck, Warszawa 2016, str. 33

43 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, op. cit.

44 E. Kulesza, *Problem niezależności inspektora ochrony danych*, op. cit., str. 113

3) stawiania wymagań,
4) nadzoru, czyli kontroli oraz wiążącego ingerowania w działalność administratora danych osobowych,
5) podejmowania decyzji o zmianie zasad lub doraźnym wstrzymaniu przetwarzania danych w przypadku stwierdzonego zagrożenia dla poufności, integralności lub naruszenia zasad ich przetwarzania [45].

Zmianie uległa również pozycja prawna ABI, który dotychczas był osobą wyznaczoną do pełnienia funkcji, a jego pozycja w strukturze organizacyjnej nie była prawnie uregulowana i pomimo powierzenia mu czynności nadzorczych w zakresie ochrony danych osobowych w praktyce spotykało się to z różnymi przeszkodami organizacyjno-prawnymi, wobec braku jednoznacznej pozycji prawnej ABI w strukturze organizacyjnej [46]. Zmianą, o której mowa powyżej na administratora nałożono obowiązek zapewnienia administratorowi bezpieczeństwa informacji środków i organizacyjnej odrębności, niezbędnych do niezależnego pełnienia tej funkcji (art. 36a ust. 8 u.o.d.o.). Mimo że sama idea zaproponowanych rozwiązań zasługiwała na aprobatę, to jednak za podstawową wadę tych regulacji należy uznać ich zasadniczo bez sankcyjny charakter [47]. Mając powyższe na uwadze, w niektórych organizacjach konieczne było wprowadzenie zmian organizacyjnych, czasami nawet zmiany statutu lub umowy spółki dla ustanowienia niezależności nowego stanowiska i możliwości bezpośredniego raportowania kierownictwu administratora danych osobowych [48]. RODO w tym zakresie idzie znacznie dalej wskazując na konieczność wspierania IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania. Dotychczas istniejące wątpliwości, co do możliwości powołania zastępców ABI zostały również uregulowane w ust. 6 ww. przepisu ustawy i w przedmiotowym zakresie w razie zaistnienia takiej potrzeby administrator danych mógł powołać zastępców ABI [49].

W świetle art. 36a ust. 5 u.o.d.o. funkcję ABI mogła wykonywać osoba, która:
„1) ma pełną zdolność do czynności prawnych [50] oraz korzysta z pełni praw publicznych,

45 M. Kołodziej, *Powołanie administratora bezpieczeństwa informacji, op. cit.*, str. 35

46 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, op. cit., str. 58

47 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, Lex/el. 2018, dostęp z dnia 5.03.2019 r.

48 M. Kołodziej, *Powołanie administratora bezpieczeństwa informacji, op. cit.*, str. 33

49 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*,op. cit., str. 58

50 Zgodnie z art. 11ustawy kodeks cywilny z dnia 23.04.1964 r. Dz. U. z 2019 r., poz. 1145 z późn.zm. pełną

2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
3) nie była karana za umyślne [51] przestępstwo."

Naczelny Sąd Administracyjny w orzeczeniu z dnia 19.04.2018 r., sygn. II FSK 1171/16 wskazał, że ocena, czy dana osoba ma zdolność do czynności procesowych odbywa się na gruncie przepisów Kodeksu cywilnego, który definiuje pojęcie zdolności procesowej w art. 11, art. 12 art. 13 i art. 15. Skoro zdolność procesowa osoby fizycznej jest pochodną jej statusu prawnego, to wyłącznie ten czynnik, a nie jej cechy psychofizyczne, decyduje o posiadaniu zdolności procesowej. Samo istnienie przesłanek ubezwłasnowolnienia nie wpływa na zdolność procesową osoby fizycznej, dopóki nie dojdzie do wydania postanowienia o ubezwłasnowolnieniu. Osoba chora psychicznie, ale nieubezwłasnowolniona, ma zdolność procesową. Zaburzenia psychiczne nie są warunkiem wystarczającym przyjęcia braku zdolności procesowej strony (uczestnika). Bez ubezwłasnowolnienia przez sąd powszechny skutek ten nie następuje.

Natomiast zgodnie z wyrokiem Sądu Najwyższego z dnia 21 sierpnia 2018 r., sygn. IV KK 365/17, przesłanka „niekaralności za przestępstwo umyślne" wymieniona w art. 66 § 1 KK, dotyczy prawomocnych skazań, które miały miejsce do dnia orzekania w przedmiocie warunkowego umorzenia postępowania.

Wymagania stawiane wobec ABI nie były przesadnie skomplikowane i rozbudowane. Oprócz zajmowania się ochroną danych osobowych ABI mógł wykonywać inne zadania związane z działalnością administratora, o ile nie kolidowało to z prawidłowym wykonywaniem zadań nałożonych na ABI przez przepisy prawa [52].

Wymóg ten zobowiązywał administratora w każdej konkretnej sytuacji do starannego przeanalizowania, czy jakiekolwiek inne zadania (lub funkcje), jakimi zamierzałby obarczyć ABI, nie utrudniłyby mu właściwego wykonywania jego ustawowych obowiązków. W tym zakresie brane musiały być pod uwagę rozmaite i liczne czynniki, np. ilość czasu potrzebnego na wykonywanie poszczególnych obowiązków, stopień skomplikowania i ważności zadań, rezerwa czasowa na nieplanowane zadania, ilość i rodzaj danych osobowych oraz procesów i systemów informatycznych służących do ich przetwarzania. Nie należy zgodzić się ze

zdolność do czynności prawnych nabywa się z chwilą uzyskania pełnoletności. Z kolei zgodnie z art. 8 § 1 ww. ustawy każdy człowiek od chwili urodzenia ma zdolność prawną.

51 Zgodnie z art. 9 §1 ustawy z dnia 6.06.1997 r., Dz. U. z 2019 r., poz. 1950 z późn. zm. czyn zabroniony popełniony jest umyślnie, jeżeli sprawca ma zamiar jego popełnienia, to jest chce go popełnić albo przewidując możliwość jego popełnienia, na to się godzi.

52 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

stanowiskiem, iż obowiązek przewidziany w tym przepisie u.o.d.o. można było traktować jako dobre przygotowanie do przestrzegania art. 38 ust. 6 RODO, bo konflikt interesów również wymaga starannego uwzględniania różnych czynników w konkretnym kontekście działalności danego podmiotu [53].

Wymagania określone na stanowisku ABI wymagały jednak doprecyzowania, bowiem wskazane kryteria nie miały żadnego przełożenia na charakterystykę wykonywanych zadań przez ABI, którym powinna być osoba legitymująca się specjalistyczną wiedzą w przedmiotowym zakresie i doświadczeniem zawodowym związanym z ochroną danych osobowych. Kryterium posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych nie ma bowiem żadnego przełożenia na wykonywane przez ABI czynności, bowiem każda osoba może legitymować się takim kryterium, chociażby poprzez ukończenie szkolenia z zakresu ochrony danych osobowych, które może świadczyć każdy podmiot zajmujący się zawodowo szkoleniami pracowników lub edukacją [54]. Na gruncie u.o.d.o. powołanie ABI w każdym przypadku było fakultatywne i żaden administrator danych nie miał obowiązku powołania ABI. Z kolei na gruncie RODO ta sytuacja uległa zmianie.

ABI mógł, ale nie musiał być powołany (a wówczas musiał być zgłoszony do rejestru prowadzonego przez Generalnego Inspektora Danych Osobowych). W przypadku nowego inspektora ochrony danych jego wyznaczenie jest obowiązkowe w zasadzie zawsze, gdy wskazuje na to kategoria przetwarzania danych, cel przetwarzania danych na dużą skalę albo gdy mowa jest o jednostce publicznej. Ponadto ABI prowadził rejestr zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, z obowiązku rejestracji których nie są zwolnieni administratorzy danych. Oczywiście w ramach tych obowiązków mieści się wiele bardziej szczegółowych czynności. Będzie to np. kontrola stanu wydanych upoważnień oraz ewidencji osób upoważnionych do przetwarzania danych osobowych zawartych w poszczególnych zbiorach, czy prowadzenie szkoleń z zakresu ochrony danych osobowych dla pracowników administratora danych. Pracodawca (administrator danych) mógł obciążyć administratora bezpieczeństwa informacji dodatkowymi obowiązkami (zarówno związanymi z ochroną danych osobowych, jak i takimi, które nie mają nic wspólnego z danymi

53 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych,* op. cit., str. 15

54 S. Hady-Głowiak, *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, op. cit., str. 58

osobowymi), ale tylko jeżeli nie naruszało to prawidłowego wykonywania podstawowych zadań ABI [55].

Fakultatywny charakter powołania ABI powodował, że tylko część ADO decydowała się na ten krok, reszta samodzielnie zapewniała przestrzeganie w swojej organizacji przepisów o ochronie danych osobowych, To znaczy, czy w danym przypadku powołanie ABI jest optymalne, zależało od wielu czynników, takich jak złożoność problematyki przetwarzania danych osobowych, ilość procesów z tym związanych, liczby posiadanych zbiorów, wielkość obszaru przetwarzania danych, itd. [56]

Korzyści płynące z ustanowienia ABI to wspomniane wcześniej zwolnienie z części obowiązków rejestracyjnych oraz oddanie nadzoru nad przetwarzaniem danych osobowych w organizacji profesjonaliście, który posiada odpowiednią wiedzę i zajmuje się tą problematyką w ramach swoich obowiązków. Powyższe pozwoliło na wzrost szansy na prawidłową realizację wymagań przepisów i zmniejszyło zagrożenie zarówno o charakterze wewnętrznym, jak i zewnętrznym. Uproszczona forma realizacji kontroli za pośrednictwem ABI jawiła się jako bardziej przyjazna. Dla części podmiotów przeszkodą w powołaniu ABI były warunki finansowe lub organizacyjne. Nie zmienia to faktu, że podmioty te musiały być przygotowane na to, że informacje będące przedmiotem zainteresowania organu kontrolnego i tak musiała zostać zebrana przez ADO bądź ustalone w toku ewentualnej kontroli inspektorów. Właśnie to spowodowało, że po wejściu w życie nowelizacji u.o.d.o. z 7.11.2014 r. podmioty publiczne – z powodu swoich rozmiarów i złożonego zakresu realizowanych zadań z udziałem różnorakich zbiorów danych osobowych - przez kilka miesięcy były najliczniejszą grupą podmiotów zgłaszających ABI do rejestracji. W późniejszym okresie ww. korzyści związane z powołaniem (i zgłoszeniem) ABI dostrzegły także podmioty prywatne [57].

Odpowiedzialność ABI wynikała z zaniechania nałożonych na niego obowiązków na podstawie obowiązującej w tamtym czasie ustawy, w tym za działania niezgodne z prawem lub nieprawidłową ochronę przez niego danych osobowych. ABI mógł ponieść odpowiedzialność cywilnoprawną (przed ADO) oraz w określonych przypadkach odpowiedzialność karną. Jeżeli działanie lub zaniechanie ABI spowodowało określone szkody, ADO mógł zażądać

55 M. Sarna, *Inspektor ochrony danych* [w:] pod red. W. Szczygielska, *RODO przewodnik po kluczowych zmianach*, WiP Warszawa 2008, str. 35

56 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Wrocław 2017, , str. 71

57 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 71

naprawienia jej maksymalnie do wysokości trzymiesięcznego wynagrodzenia, ale i również doprowadzić do rozwiązania stosunku pracy. Jeżeli ABI wykonywał swoje zadania bez umowy o pracę, ale na podstawie umowie cywilnoprawnej, ADO mógł dochodzić naprawienia szkody w pełnej wysokości [58].

ADO powinien był zatem przed nawiązaniem współpracy z ABI podobnie, jak ma to miejsce obecnie z IOD wymagać zabezpieczenia w postaci polisy OC.

Zgodnie z art. 38 ust. 3 RODO wskazuje, że „Inspektor nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań". Należy również podkreślić fakt, że w polskim porządku prawnym nie wprowadzono kluczowych z punktu funkcjonowania ABI, a następnie IOD gwarancji dotyczących zakazu jego karania, szykanowania za podejmowane działania do zakazu zwolnienia i odmowy składania zeznań włącznie. Takie rozwiązania przyjęto w Niemczech, o czym wspomniano w pkt. I.1. niniejszego rozdziału. Takie rozwiązania z pewnością podniosłyby rangę i niezależność tego stanowiska. Szczegółowe zasady odpowiedzialności IOD zostaną szczegółowo omówione w rozdziale drugim niniejszej pracy.

I.3. Inspektor Ochrony Danych jako następca ABI

Od 25 maja 2018 r. zmieniono nazwę powyższej instytucji. Od tej daty ABI stał się IOD, tj. inspektorem ochrony danych [59]. Zgodnie z okresem przejściowym wskazanym w art. 158 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych [60] pełnił on swoją funkcję do dnia 1 września 2018 r., chyba że przed tym dniem administrator zawiadomił Prezesa Urzędu o wyznaczeniu innej osoby na stanowisko IOD.

Inspektor ochrony danych osobowych jest odpowiednikiem administratora bezpieczeństwa informacji, który był przewidziany w ustawie o ochronie danych osobowych z 1997 r. Pełni on rolę osoby odpowiedzialnej za nadzór nad przestrzeganiem przepisów o ochronie danych osobowych u administratora lub podmiotu przetwarzającego [61].

58https://mcodszkodowania.pl/odpowiedzialnosc-abi-administratora-bezpieczenstwa-informacji-i-ado-administratora-danych-osobowych/ dostęp z dnia 29.11.2019 r.

59 K. Hamelusz, Zadania IOD względem ABI - analiza prawno-porównawcza, op. cit.

60 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych Dz. U. z 2019 r., poz. 1781, t.j. zwana dalej u.o.d.o.

61 D. Lubasz, W. Chomiczewski, C*ompliance w zakresie ochrony danych osobowych*, [w:] B. Jagura (red.), B. Makowicz (red.), *Systemy zarządzania zgodnością. Compliance w praktyce*, WKP 2020, dostęp z dnia 4.06.2021 r.

Przekształcenie administratorów bezpieczeństwa informacji w inspektorów ochrony danych nie może następować w sposób automatyczny. Wraz ze wzmocnieniem roli inspektorów RODO wprowadza bowiem wiele istotnych zmian w różnych obszarach. Wynikają one z tego, że inspektorzy mają być kluczowym elementem nowego zunifikowanego systemu ochrony danych osobowych i przyczyniać się do efektywnego wdrożenia i przestrzegania przepisów ogólnego rozporządzenia. Od 25.5.2018 r., wraz z rozpoczęciem stosowania RODO, we wszystkich państwach członkowskich Unii Europejskiej obowiązują: jednolita terminologia, zasady powołania i funkcjonowania inspektorów ochrony danych [62].

O roli inspektora ochrony danych (zwanego dalej IOD) jako podmiotu zapewniającego zgodność przetwarzania danych z przepisami o ochronie danych świadczy to, że na przestrzeni ostatnich kilkunastu lat coraz więcej państw członkowskich Unii Europejskiej oraz państw spoza niej w swoim ustawodawstwie przewidziało obowiązek lub możliwość powołania IOD. Na kluczową jego rolę w tym procesie również zwracała uwagę zarówno Komisja Europejska, jak i Grupa Robocza art. 29 (zwana dalej GR Art. 29) [63]. Koncepcja IOD nie jest niczym nowym. Choć dyrektywa 95/46/WE nie nakładała na żadnego administratora obowiązku powoływania IOD, to jednak na przestrzeni lat praktyka taka wykształciła się w szeregu państw członkowskich [64].

Jeszcze przed uchwaleniem i wejściem w życie RODO GR Art. 29 (obecnie Europejska Rada Ochrony Danych) podkreślała, że „wyznaczenie IDO może ułatwiać przestrzeganie przepisów z zakresu ochrony danych osobowych, umożliwiać budowanie przewagi konkurencyjnej na rynku oraz wdrożenie narzędzi rozliczalności (ocena skutków dla zakresie ochrony danych, przeprowadzanie lub ułatwianie audytów w zakresie bezpieczeństwa danych), a także zapewniać lepszą komunikację pomiędzy zainteresowanymi stronami (np. organami nadzoru, podmiotami danych i jednostkami biznesowymi w ramach organizacji)” [65].

Przed wejściem w życie RODO, jak potwierdziła między innymi przeprowadzona w latach 2009–2012 przez Confederation of National Data Protection Organisations (CEDPO) analiza stosownych przepisów państw członkowskich, w Unii Europejskiej nie istniało

62 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych,* op. cit., str. 10

63 E. Bielak-Jomaa, *Inspektor ochrony danych, op. cit.*, str. 766 - 767

64 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 5, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

65 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, PME 2018, Nr 4, C.H. Beck, str. 4, Legalis.pl, dostęp z dnia 28.05.2020 r.

jednolite podejście do uregulowania instytucji inspektora ochrony danych, co *notabene* widoczne było już na płaszczyźnie przyjętego nazewnictwa: niem. *Beauftragter für Datenschutz*, fr. *Correspondant Informatique et libertés*, hisz. *Responsable de la seguridad*. W praktyce dominowało podejście oparte na opcjonalności/fakultatywności omawianej instytucji (Francja, Szwecja, Luksemburg, Malta, Estonia, Hiszpania, Litwa, Łotwa). Obowiązek powołania inspektorów ochrony danych osobowych w przypadku zaistnienia przewidzianych w przepisach przesłanek wprowadzono w niektórych tylko państwach, między innymi w Niemczech, Słowenii, Chorwacji, Słowacji. Istniały w końcu i ustawodawstwa krajowe, które przed wejściem w życie RODO w ogóle nie przewidywały tej instytucji (np. Czechy, Grecja, Wielka Brytania, Rumunia). Wśród państw członkowskich, które zdecydowały się na wprowadzenie przedmiotowej regulacji w ustawodawstwie krajowym, wyraźnie dominowało podejście kwantytatywne (ilościowe), tj. uzależniające obowiązek powołania stosownego inspektora ochrony danych od liczby zatrudnionych osób (np. w Słowenii 50; w Chorwacji 20, w Słowacji 5). Alternatywne podejście regulacyjne (np. Belgia, Węgry, Holandia) bazowało natomiast na enumeratywnym wyliczeniu podmiotów objętych obowiązkiem powołania inspektorów ochrony danych osobowych (notabene głównie podmiotów z sektora publicznego lub podmiotów powiązanych z sektorem publicznym) [66].

Mając powyższe na uwadze oraz dotychczasową praktykę i brak jednoznacznych wymogów w tym zakresie w polskim porządku prawnym należy stwierdzić, że najlepszym rozwiązaniem byłoby wskazanie obowiązku wyznaczenia IOD poprzez literalne wskazanie podmiotów z sektora publicznego lub podmiotów powiązanych z sektorem publicznym. Z kolei w przypadku sektora prywatnego uzależniające obowiązek powołania IOD od liczby zatrudnionych osób, co szczegółowo zostanie omówione w drugim rozdziale niniejszej pracy. Należy tutaj również zaznaczyć brak regulacji. Nie ma też mechanizmów weryfikujących umiejętności kandydatów na to stanowisko

W konsekwencji wejścia w życie RODO, zawierającego przepisy dotyczące wyznaczenia statusu, jak i zadań inspektora ochrony danych, inicjatywy regulacyjne w omawianym obszarze widocznie osłabły. Na dzień dzisiejszy tylko niektóre państwa członkowskie Unii Europejskiej zdecydowały się na bardziej precyzyjne uregulowanie instytucji inspektora ochrony danych w porządku krajowym (np. Francja, Hiszpania, Słowacja, Węgry, Chorwacja oraz Niemcy). Zdecydowana większość państw członkowskich po wejściu

66 M. Otto, *Pozycja prawna inspektora ochrony danych – zarys prawnoporównawczy,* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019, str. 262-263

w życie RODO w swoim ustawodawstwie krajowym w zakresie odnoszącym się do inspektora ochrony danych *explicite* odsyła do stosownych postanowień RODO [67]. Należy tu podkreślić brak w polskim porządku prawnym zarówno szczegółowych przepisów dotyczących kwalifikacji i wymogów na stanowisku IOD, jak również mechanizmów weryfikujących umiejętności kandydatów na to stanowisko, co z pewnością usprawniłoby zapewnienie fachowej pomocy i nadzoru nad procesem przetwarzania danych osobowych w danej instytucji. Powyższa kwestia została szczegółowo omówiona w rozdziale drugim niniejszej pracy.

W kontekście przekształcenia ABI w inspektora ochrony danych należy zwrócić uwagę na zmiany na kilku płaszczyznach. Po pierwsze, przechodzimy od systemu, w którym wiele obowiązków z zakresu ochrony danych osobowych było szczegółowo określonych i często miało charakter formalny, do systemu opartego na zasadzie rozliczalności i podejścia opartego na ryzyku, w którym o sposobie realizacji poszczególnych obowiązków będą musieli zadecydować sami administratorzy danych i podmioty przetwarzające. Wpływa to bezpośrednio na charakter i zakres zadań inspektorów. Po drugie przechodzimy od systemu, w którym wyznaczenie fachowca z zakresu ochrony danych osobowych było dobrowolne, do systemu, w którym dla wielu podmiotów (w tym zarówno administratorów, jak i podmiotów przetwarzających) będzie to obowiązkiem. Po trzecie – w porównaniu z administratorami bezpieczeństwa informacji – inspektorzy ochrony danych zyskują więcej gwarancji niezależności oraz uprawnienia do żądania różnych form wsparcia ze strony organizacji, w których zostaną wyznaczeni. Nie funkcjonuje już ogólnokrajowy rejestr administratorów bezpieczeństwa informacji. Zamiast obowiązku zgłaszania powołania i odwołania ABI do rejestracji GIODO podmioty, które wyznaczą inspektora ochrony danych osobowych, są zobowiązane powiadomić o jego danych kontaktowych zarówno osoby, których dane dotyczą, jak i organ nadzorczy [68].

Nie sposób nie wspomnieć również o gwarancjach niezależności IOD i jego pozycji prawnej wynikających z RODO. Przede wszystkim inspektor ochrony danych musi mieć możliwość korzystania z zasobów niezbędnych dla wykonywania swoich obowiązków, a także mieć zagwarantowany dostęp do danych osobowych oraz operacji ich przetwarzania. Dodatkowo trzeba mu zapewnić zasoby konieczne do utrzymania jego fachowej wiedzy, a zatem przede wszystkim odpowiednie szkolenia. Inspektor ochrony danych nie może też

67 M. Otto, *Pozycja prawna inspektora ochrony danych – zarys prawnoporównawczy,* op. cit., str. 263

68 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych,* op. cit.

otrzymywać instrukcji dotyczących wykonywanych przez niego zadań, a za ich realizację nie może być karany lub odwoływany. Ważną gwarancją dla właściwego wykonywania obowiązków jest wymóg, by inspektor podlegał najwyższemu kierownictwu administratora lub podmiotu przetwarzającego [69].

I.4. Zasady wyznaczenia IOD, a powołanie ABI

Obowiązek, wyznaczenia IOD jest definiowany poprzez:

1) kategorię przetwarzanych danych;
2) cel przetwarzania danych na dużą skalę;
3) zawsze gdy jest mowa o jednostce publicznej [70].

W przeciwieństwie do ustawy o ochronie danych osobowych, która nie nakładała ogólnego obowiązku powołania ABI przez administratora danych, RODO przewiduje trzy przypadki, w których istnieje obowiązek powołania IOD [71].

Podstawową różnicą między przepisami UODO i RODO w zakresie uregulowania funkcji ABI i IOD jest to, że zgodnie z prawem polskim powołanie ABI było fakultatywne, a na podstawie RODO – w pewnych sytuacjach obowiązkowe. Znaczące jest, że obowiązek ten dotyczyć może nie tylko administratorów danych, ale także podmiotów przetwarzających, co w przepisach rozporządzenia 2016/679 jest wprost wskazane. Na negatywną ocenę zasługuje posługiwanie się pojęciami nieostrymi w przesłankach obligatoryjnego wyznaczenia inspektora. Nie jest bowiem oczywiste, w jakich okolicznościach inspektor powinien zostać wyznaczony, a jego niewyznaczenie może skutkować nałożeniem bardzo wysokiej kary finansowej [72].

Artykuł 37 ust. 1 RODO wskazuje na obowiązek wyznaczenia Inspektora Ochrony Danych (zwanego dalej IOD) przez Administratora danych (zwanego dalej ADO) i podmiot przetwarzający, zawsze gdy:

„a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości,

69 D. Lubasz, W. Chomiczewski, C*ompliance w zakresie ochrony danych osobowych*, [w:] B. Jagura (red.) op. cit.

70 S. Hady-Głowiak, *ABI, IOD jako wyspecjalizowany audytor ds. bezpieczeństwa informacji*, op. cit., str. 56

71 K. Hamelusz , *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

72 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań, op. cit.*

b) 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,
c) 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". Z kolei art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych [73] (zwanej dalej UODO) precyzuje, że „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."

Ogólne rozporządzenie nakłada na niektórych ADO obowiązek powoływania IOD, co stanowi istotną zmianę w porównaniu z pełną fakultatywnością powoływania ABI. Powyższe wskazuje na brak jednoznacznie określonych kategorii administratorów i podmiotów przetwarzających zobligowanych do wyznaczenia IOD. Należy również wskazać z góry ograniczony katalog organów i podmiotów publicznych obowiązanych do jego wyznaczenia. wskazany w UODO.

Wobec tego każdy podmiot – niezależnie od tego, czy skorzystał wcześniej z możliwości powołania ABI, czy nie – zobowiązany jest dokonać analizy, czy w świetle przepisów RODO ciąży na nim taki obowiązek. Należy zgodzić się ze stanowiskiem, że nawet w sytuacji, gdy z przepisów nie wynika obowiązek wyznaczenia inspektora, administratorom i podmiotom przetwarzającym zaleca się udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia tego obowiązku. Ocenę taką trzeba powtarzać w razie potrzeby, w zależności od zmieniającej się sytuacji podmiotu, mającej wpływ na poszczególne przesłanki wskazane w powyższym przepisie, np. wówczas, gdy administrator albo podmiot przetwarzający zaczyna świadczyć nowe usługi [74]. Szczegółowe rozwiązania i analiza w tym zakresie zostanie przedstawiona w rozdziale drugim niniejszej pracy.

Ponadto użycie pojęć ogólnych i niezdefiniowanych, np. „główna działalność", „regularne i systematyczne monitorowanie osób", „duża skala", nie ułatwia wykładni powyższych

73 Dz. U. z 2019 r., poz. 1781

74 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit.

przesłanek. Wymagana jest każdorazowa precyzyjna analiza stanu faktycznego, na podstawie którego ma dochodzić do powołania IOD [75].

Przesłanki te mają charakter nieostry i ich interpretacja może rodzić wątpliwości. Aby ustalić, że przetwarzanie danych osobowych należy do głównej działalności ADO lub podmiotu przetwarzającego, który działa w sektorze prywatnym, należy ustalić, iż stanowi ono „jego zasadnicze, a nie poboczne czynności [76].

GR Art. 29 w swoich Wytycznych dotyczących inspektora ochrony danych dostarczyła wskazówek dotyczących interpretacji użytych w art. 37 ust. 1 RODO pojęć (tj. podmiot i organ publiczny, główna działalność, duża skala, systematyczne i regularne monitorowanie osób), ułatwiających przeprowadzenie analizy w zakresie ustalenia poszczególnych normatywnych przesłanek istnienia lub braku tego obowiązku [77]. Pojęcia te zostaną szczegółowo omówione w kolejnym rozdziale.

Nie sposób nie wspomnieć o art. 46 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości [78] (zwana dalej OchrDanychZwPrzestU), który precyzuje, iż Administrator wyznacza inspektora ochrony danych. IOD może być osoba, która:1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;2) posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1 oraz nie była skazana prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej. Należy tutaj zauważyć istotne przesłanki zastosowane już poprzednio w treści art. 36a ust. 5 u.o.d.o. Powyższe wskazuje na istotną nieudolność ustawodawcy, który w jednej ustawie OchrDanychZwPrzestU wskazuje bardzo istotne wymogi na stanowisku IOD (nieskazanie, pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych) jednocześnie je pomijając w obowiązującej UODO (mimo dotychczasowej praktyki w tym zakresie za rządów poprzedniej u.o.d.o.), która dotyczy zarówno podmiotów publicznych, jak i prywatnych. Ww. wymogi są szczególnie istotne z punktu widzenia osób, którym powierza

75 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

76 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 73

77 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 12

78 Dz. U. z 2019, poz. 125

się wykonywanie zadań z zakresu ochrony danych osobowych w organizacji.

Obowiązek wyznaczenia inspektora na gruncie RODO będzie dotyczył również podmiotów przetwarzających. Dotychczas obowiązujące przepisy u.o.d.o. przewidywały, że administratora bezpieczeństwa informacji mógł powołać administrator danych. Nie oznacza to jednak, że podmioty przetwarzające (podmioty z art. 31 u.o.d.o.) nie powołują takich osób, ponieważ często korzystają one z podwójnego statusu: zarówno podmiotu przetwarzającego, jak i administratora danych (np. przetwarzając dane swoich pracowników). Na gruncie RODO ocenę w zakresie obowiązku wyznaczenia inspektora należy przeprowadzać osobno dla każdej z tych ról. Mogą bowiem wystąpić sytuacje, kiedy administrator nie będzie zobowiązany do wyznaczenia inspektora, natomiast obowiązek taki będzie ciążył na podmiocie przetwarzającym [79].

Pod rządami ogólnego rozporządzenia na pewne ułatwienie w zakresie ustanawiania IOD mogą liczyć spółki należące do grupy przedsiębiorstw. O ile spełniony zostanie wymóg w zakresie łatwego dostępu do IOD, wystarczające będzie powołanie jednego, wspólnego inspektora ochrony danych osobowych dla wszystkich spółek wchodzących w skład grupy. Podobne rozwiązanie zostało również dopuszczone w sektorze publicznym – dla kilku organów lub podmiotów publicznych może zostać wyznaczony jeden, wspólny IOD, przy czym podejmując taką decyzję, należy uwzględnić strukturę organizacyjną i wielkość tych podmiotów [80].

Dla podmiotów, które korzystały z pomocy ABI, zarówno tych zobowiązanych do powołania inspektora ochrony danych, jak i tych, które takiego obowiązku mieć nie będą, a mimo to na takie wyznaczenie się zdecydują, pierwszym kandydatem do pełnienia funkcji inspektora powinna być osoba pełniąca obecnie funkcję ABI. Szczególnie, gdy dotychczas rzetelnie wywiązywała się ona ze swoich obowiązków, zdobywała w dziedzinie ochrony danych osobowych cenne doświadczenie oraz wiedzę o procesach przetwarzania i innych szczegółach funkcjonowania danego podmiotu. Niemniej w tym zakresie administrator danych lub podmiot przetwarzający musi podjąć wyraźną decyzję. Decyzja ta powinna mieć właściwą formę, zależną od rodzaju podmiotu będącego administratorem danych, czy podmiotem przetwarzającym (np. zarządzenie dyrektora szkoły, uchwała wspólników spółki z o.o.) i być

79 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit.

80 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 74-75

wyraźnie zakomunikowana wszystkim zatrudnionym w danej organizacji. Zanim jednak to nastąpi, konieczne będzie jeszcze upewnienie się, czy wszystkie warunki określone wobec funkcji inspektora zostały spełnione [81]. Jak wcześniej wspomniano zagadnienia i rozwiązania w tym zakresie zostaną przedstawione w kolejnym rozdziale niniejszej pracy.

I.5. Zadania i kompetencje Inspektora Ochrony Danych jako następcy ABI

W przepisach o ochronie danych osobowych określone zostały zadania, jakie realizować powinien IOD, oraz wskazany został ogólnie sposób realizacji tych zadań. Zadania IOD można podzielić na cztery ogólne grupy:

1) zadania informacyjne i doradcze,
2) zadania monitorujące i nadzorcze,
3) zadania w zakresie współpracy z organem nadzorczym,
4) inne zadania [82].

Zadania inspektora ochrony danych zostały znacznie rozbudowane w stosunku do ABI i określone w artykule 39 RODO. Zgodnie z art. 39 ust. 1 „Inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, 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;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

81 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit.

82 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu, op. cit.*, str. 150

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach."

Z kolei ust. 2 precyzuje, że „Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania."

Zgodnie z art. 35 ust. 2 ogólnego rozporządzenia ADO ma obowiązek konsultowania się z IOD w przedmiocie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ocena poprzedzająca rozpoczęcie przetwarzania to nowy obowiązek nałożony na ADO i ma być realizowany, gdy „dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych [83].

IOD nie zgłasza zbiorów danych do GIODO, gdyż ten obowiązek został zniesiony w całości. Nie sporządza dla administratora sprawozdania ze zgodności przetwarzania danych osobowych u administratora, tak samo jak nie zapewnia zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych. Oczywiście do IOD są przypisane zadania edukacyjne oraz doradcze, ale rozciągają się one na wszystkich pracowników administratora [84]. Należy podkreślić, że te zadania IOD te zostały znacznie rozbudowane i doprecyzowane w przepisach RODO jako działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

Zadanie polegające na informowaniu administratora, podmiotu przetwarzającego oraz osób przetwarzających dane osobowe o ich obowiązkach wynikających z przepisów o ochronie danych, a także doradzanie im w tej sprawie, porównać można do obowiązku ABI w zakresie zapewniania zapoznania osób upoważnionych do przetwarzania danych z prawem ochrony danych osobowych [85]. Tego rodzaju działania wpisują się w ogólny zamysł prawodawcy, aby IOD służył administratorowi i podmiotowi przetwarzającemu wsparciem oraz fachową wiedzą w zakresie ochrony danych osobowych [86].

---

83 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 78

84 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

85 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań, op. cit.*

86 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu, op. cit.*, str. 150

Jeżeli chodzi o zadanie dotyczące monitorowania przestrzegania prawa ochrony danych osobowych oraz polityk administratora lub przetwarzającego w dziedzinie ochrony danych osobowych, w tym działania zwiększające świadomość, szkolenia osób zajmujących się przetwarzaniem danych oraz powiązane z tym audyty to stanowi ono pewne uzupełnienie zadania opisanego wyżej. Wynika z niego również pośrednio obowiązek przeprowadzania szkoleń oraz podejmowania działań popularyzujących wiedzę z zakresu ochrony danych osobowych. Zadanie to jest nieco zbliżone do obowiązku ABI w zakresie sprawdzania zgodności przetwarzania danych z prawem oraz opracowywanie sprawozdań w tym zakresie. Można się spodziewać, że w ramach audytu inspektor będzie przygotowywał raport dla administratora lub podmiotu przetwarzającego, który porównać można do sprawozdania. Należy jednak podkreślić, że wskazane zadania ABI w tym zakresie były [87] ustawowo uregulowane. Nie można jednak zgodzić się z twierdzeniem, że były one wiele bardziej precyzyjnie uregulowane niż zbliżone zadania IOD na podstawie ogólnego rozporządzenia. Ponadto RODO wskazało nie tylko na zwiększenie świadomości personelu, ale na stałe monitorowanie tego procesu oraz minimalizację ryzyka w tym zakresie poprzez zadania audytowe.

Sformułowanie „monitorowanie" rozumieć można jako prowadzenie stałej obserwacji i kontroli zgodności procesów przetwarzania danych z przepisami o ochronie danych. Jeżeli IOD, monitorując przestrzeganie przepisów, dojdzie do wniosku, że przepisy te nie są przestrzegane (stwierdzi nieprawidłowości w tym zakresie), powinien podjąć działania nadzorcze, tzn. działania władcze zmierzające do usunięcia nieprawidłowości i doprowadzenia do (przywrócenia) stanu zgodnego z prawem [88].

Porównując obecne zadania ABI z tymi, jakie realizować mają inspektorzy ochrony danych (zgodnie z art. 39 ust. 1 RODO), stwierdzić trzeba, że zadania inspektorów, oprócz dwóch dotychczasowych ról wyrażających się w obowiązkach monitorowania przestrzegania przepisów o ochronie danych osobowych oraz obowiązkach edukacyjno-doradczych, obejmować będą również trzecią, wyraźnie wskazaną w przepisach RODO rolę pośrednika. Inspektorzy, zgodnie z art. 39 ust. 1 pkt e i art. 38 ust. 4 RODO, mają pełnić rolę punktu

87 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań, op. cit.*, str. 82.

88 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu, op. cit.*, str. 151

kontaktowego, pośredniczyć między administratorem danych i podmiotem przetwarzającym, a osobami, których dane dotyczą oraz organem nadzorczym [89].

W zakresie współpracy z organem nadzoru może wynikać obowiązek odpowiadania na wszelkie zapytania organu nadzoru, w szczególności w kontekście prowadzenia przez organ nadzorczy postępowań kontrolnych, postępowań w związku ze skargą osoby, której dane dotyczą, czy też w ramach uprzednich konsultacji. Zgodnie z u.o.d.o., ABI nie wykonywał podobnych zadań. Co prawda ABI przeprowadzał, na wniosek GIODO, sprawdzenie zgodności z prawem przetwarzania danych przez administratora. Niemniej jednak sprawozdanie z takiego sprawdzenia było przekazywane GIODO za pośrednictwem administratora danych. W innym wypadku GIODO nie mogło zwrócić się bezpośrednio do ABI, ale do administratora, który z kolei mógł upoważnić ABI do kontaktowania się z GIODO w danej sprawie. Jest to istotna różnica między regulacjami dotyczącymi ABI a inspektora, bowiem zadania inspektora w tym zakresie są mniej skonkretyzowane, a jednocześnie musi on być przygotowany na otrzymywanie różnego rodzaju zapytań bezpośrednio od organu nadzoru [90].

Pomimo że zadania, które ma spełniać IOD, są podobne do zadań znanych ABI, to jednak sposób ich wykonania i pryncypia działalności samego IOD uległy zasadniczej zmianie. RODO w sposób zdecydowanie szerszy określa status oraz zadania osoby odpowiedzialnej za bezpieczeństwo informacji [91].

Wiele zależy od poziomu świadomości zarządzających w odniesieniu do wagi problemu ochrony danych w organizacji. Problemem są też stare przyzwyczajenia i przeświadczenie, że dawny ABI, a obecny IOD jest raczej wykonawcą, mającym rozwiązywać każdy problem dotyczący ochrony danych i odpowiadającym za ochronę danych osobowych w organizacji. Należy podkreślić, że znaczenie funkcji IOD wzrosło w stosunku do wcześniejszej funkcji ABI. Przede wszystkim dotyczy to pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą, uczestnictwa w zgłaszaniu sytuacji naruszenia ochrony danych do Prezesa UODO, jak również uczestnictwa w procesie oceny skutków dla ochrony danych – co nie było określone we wcześniejszych przepisach o ochronie danych obowiązujących w Polsce[92].

89 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 11

90 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań* , op. cit., s. 82

91 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza,* op. cit.

92 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, [w:] M. Kołodziej (red.),

Zadania IOD w organizacji są zatem szerokie. Ma on zarówno pełnić funkcje nadzorcze, doradcze, edukacyjne, jak i wydawać opinie oraz zalecenia, jego obowiązkiem jest również działanie jako punkt kontaktowy i współpraca z organem nadzorczym. W przepisach ogólnego rozporządzenia nie ma jednak szczegółowych przepisów odnoszących się do sposobu realizacji tych obowiązków, a treść wskazanego powyżej art. 39 ust. 1 wydaje się pełna ogólników. Również katalog powinności IOD wynikający z tego przepisu wydaje się niepełny. Nie ma w nim, choćby obowiązku pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą wynikającego art. 38 ust. 4 ogólnego rozporządzenia. Taki zabieg ze strony prawodawcy unijnego może dziwić tym bardziej, że dotyczy on zadań podmiotu, któremu zagwarantowano niezależność w realizacji tych zadań [93].

Należy zgodzić się ze stanowiskiem wyrażonym przez K. Kozieł i Sz. Sieniewicz, że katalog zadań określony w art. 39 RODO jest katalogiem otwartym. Do takiego wniosku może prowadzić przede wszystkim to, że w art. 38 ust. 6 RODO wskazano wprost na możliwość wykonywania przez IOD innych zadań i obowiązków. RODO w niektórych miejscach wprost wskazuje na zadania IOD, które nie wynikają z art. 39 RODO. Przykładem jest tutaj art. 38 ust. 4 RODO, o czym mowa powyżej. Pomimo braku wskazania tego wprost w RODO IOD w praktyce pomaga także administratorowi i podmiotowi przetwarzającemu w prowadzeniu rejestrów odpowiednio czynności przetwarzania danych osobowych (art. 30 ust. 1 RODO) i kategorii czynności przetwarzania danych osobowych (art. 30 ust. 2 RODO). Ponadto lektura innych wersji językowych RODO wskazuje, że zadania określone w art. 39 RODO są jedynie głównymi, podstawowymi zadaniami IOD, a zakres zadań IOD może być w praktyce szerszy [94].

Wobec nowego stanu prawnego opartego na ocenie ryzyka i rozliczalności oraz wobec wyzwań związanych z szybkimi zmianami w metodach przetwarzania i zabezpieczania danych osobowych, inspektorzy mają zapewniać fachowe wsparcie nie tylko administratorom danych, ale też podmiotom przetwarzającym. Takie wsparcie jest konieczne, aby sprostać wyzwaniom związanym z przyjęciem nowej unijnej regulacji, która zwiększa odpowiedzialność administratorów danych i podmiotów przetwarzających oraz wymusza na nich konieczność

Vademecum Inspektora Ochrony Danych, C.H. Beck, Warszawa 2020, str. 2

93 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 77

94 K. Kozieł, S. Sieniewicz, *Weryfikacja kwalifikacji IOD-a i zadań przez niego realizowanych ze wskazaniem środków kontroli,* Lex/el. 2018, dostęp z dnia 09.02.2019 r.

dokonywania samodzielnych ocen w zakresie doboru rozwiązań stosowanych w ramach przetwarzania danych osobowych [95].

Artykuł 37 ust 5 RODO wskazuje, że „IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia powierzonych mu zadań." Nie sposób nie wspomnieć tu o specyfice branży, znajomość RODO i przepisów szczegółowych, a także posiadania stosownego doświadczenia zawodowego, w tym w zakresie realizacji audytów dotyczących w zakresie bezpieczeństwa informacji i ochrony danych osobowych, jak również weryfikacji sposobów zabezpieczenia informacji przetwarzanych zarówno metodą tradycyjną, ale również przy użyciu urządzeń i nośników informacji.

Zgodnie z Wytycznymi GR Art. 29 dotyczącymi inspektorów ochrony danych, poziom wiedzy fachowej musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w danej jednostce. Wyższy poziom wiedzy powinien być wymagany np. w przypadku wyjątkowo skomplikowanych procesów przetwarzania czy też regularnego przekazywania danych osobowych do państw trzecich. Jeśli chodzi o wskazaną w RODO „umiejętność wypełniania zadań", w Wytycznych dotyczących inspektorów ochrony danych wskazuje się, że priorytetem inspektora powinno być zapewnianie przestrzegania rozporządzenia oraz odgrywanie kluczowej roli w zakresie wspierania „kultury ochrony danych". Chodzi o pomaganie w implementacji niezbędnych elementów RODO, w tym zasad przetwarzania danych osobowych, praw osób, których dane dotyczą, ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania, wymogów bezpieczeństwa przetwarzania i zgłaszania naruszeń. Zadania - zarówno ABI, jak i inspektorów - wykraczają poza wdrożenie odpowiednich zabezpieczeń i innych rozwiązań w zakresie bezpieczeństwa przetwarzanych danych. Niemniej inspektorzy, podobnie jak i ABI, powinni być dla administratorów danych i podmiotów przetwarzających fachowym wsparciem również w zakresie doboru odpowiednich do ryzyka środków bezpieczeństwa przetwarzanych danych. Zgodnie z art. 39 ust. 1 lit. c RODO, inspektor ma udzielać zaleceń, co do oceny skutków dla ochrony danych oraz monitorować jej wykonanie zgodnie z art. 35 RODO. Ponadto jest on zobowiązany wykonywać swoje obowiązki z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. RODO wymaga także dokonywania oceny ryzyka, jakie przetwarzanie danych osobowych

95 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 11

może spowodować dla praw i wolności osób, których te dane dotyczą. Umiejętności w zakresie takiej oceny powinny zatem wchodzić w zakres kompetencji inspektora [96].

Podobny wymóg wiedzy w zakresie ochrony danych przewidywał art. 36 a ust. 5 pkt 2 u.o.d.o. Prawodawca europejski nie wprowadził wobec kandydatów na IOD żadnych szczególnych, dodatkowych wymogów formalnych – takich jak choćby uprzednia niekaralność, którą musiała legitymować się osoba pełniąca funkcję ABI [97].

Wobec wymogów na stanowisko ABI wskazywano również na posiadanie pełnej zdolności do czynności prawnych, czy korzystania z pełni praw publicznych. Obecnie w przypadku podmiotów prywatnych ww. wymogi nie są obowiązujące, podobnie, jak również wobec podmiotów świadczących usługę IOD na podstawie umowy cywilnoprawnej. Wobec osób zatrudnionych w ramach umowy o pracę w organach i podmiotach publicznych należy również wskazać na wymogi wynikające m.in. z art. 4 ust 1 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej [98], czy z art. 6 ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych [99]. Wyżej wymienione ustawy wskazują m.in. na wspomniany wcześniej wymóg korzystania z pełni praw publicznych, czy nieskazania prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

RODO mocno akcentuje wymóg posiadania przez inspektora wiedzy i umiejętności, nie reguluje jednak zasad czy trybu weryfikacji spełnienia tego wymogu. Przepisy RODO nie wskazują na konkretny rodzaj czy poziom wykształcenia, legitymowanie się określonym dyplomem czy szczególnym certyfikatem [100].

Wymogi kwalifikacyjne stawiane ABI i inspektorowi są w gruncie rzeczy bardzo podobne i dotyczą posiadania odpowiedniej wiedzy z zakresu ochrony danych osobowych. Żadna z regulacji nie zawiera w tym zakresie kryteriów, według których należy oceniać spełnienie tego wymogu. Znaczącą różnicą jest jednak to, że zgodnie z ogólnym rozporządzeniem, oprócz wiedzy o ochronie danych osobowych inspektor powinien także posiadać umiejętności konieczne do wypełniania swoich zadań. Chodzi tutaj o umiejętności

96 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 13

97 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 75

98 ustawa z dnia 21 listopada 2008 r. o służbie cywilnej Dz. U. z 2020 r., poz. 265, t. j.

99 ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych Dz. U. z 2019 r., poz. 1282, t. j.

100 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 13

związane z przekazywaniem wiedzy na temat ochrony danych, przeprowadzania szkoleń, odpowiedniej organizacji pracy czy też sprawnego komunikowania się z organem nadzorczym lub osobami, których dane dotyczą [101].

Wiedza fachowa w zakresie ochrony danych osobowych ma służyć inspektorowi do profesjonalnego wykonywania zadań wymienionych w art. 39 RODO, czyli informowania, doradzania administratorowi, współpracy z organem nadzorczym, pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, które to działania inspektor ma wykonywać z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania [102].

Wynika z tego, że działalność IOD jest oparta na zasadzie ryzyka w tym sensie, iż IOD musi ocenić, gdzie jego zaangażowanie jest potrzebne bardziej, a gdzie mniej, bo wszystkim naraz nie uda mu się zająć. „To selektywne i pragmatyczne podejście powinno ułatwić [...] doradzenie administratorowi, jaką metodologię należy zastosować przy przeprowadzeniu oceny skutków dla ochrony danych, które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi, jakie szkolenia wewnętrzne przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych, i na które operacje przetwarzania przeznaczyć więcej czasu i zasobów” [103]. Stawiając warunek posiadania odpowiedniej wiedzy na temat ochrony danych osobowych, prawodawca unijny nie uwzględnił przy tym sytuacji, że prawidłowe wykonywanie zadań IOD musi uwzględniać także wiedzę związaną ze specyfiką działania podmiotu (administratora), w którym dane są przetwarzane. Trudno uznać, że wiedza wymagana od osoby zajmującej się ochroną danych w placówce służby zdrowia jest tożsama z wymaganą wiedzą osoby, która ma zajmować się ochroną danych w placówkach edukacyjnych, szkołach wyższych, organach samorządu terytorialnego czy placówkach organizacyjnych pomocy społecznej. Kwestią, która także nie została uregulowana – również w polskiej ustawie o ochronie danych osobowych, która byłaby właściwszym miejscem dla rozstrzygnięcia tej sprawy – jest podstawa do formalnej oceny posiadanych przez kandydata na inspektora ochrony danych kwalifikacji. Brak dookreślenia sposobu uzyskiwania kwalifikacji uprawniającej do zatrudnienia w charakterze inspektora ochrony danych osobowych sprawił,

101 K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, op. cit.

102 E. Kulesza, *Problem niezależności inspektora ochrony danych*, op. cit., str. 119

103 M. Gawroński , M. Kibil , *Zadania Inspektora ochrony danych osobowych*, LEX/el. 2018 (dostęp 09.02.2019 r.)

że pojawiła się znaczna grupa osób pragnących zdobyć poświadczenie posiadania „odpowiednich kwalifikacji", a w wyniku zapotrzebowania na szkolenia pojawiło się wiele podmiotów zajmujących się przygotowaniem do wykonywania zawodu inspektora ochrony danych i wiele form dokształcania. W efekcie takich działań inspektorami ochrony danych wyznaczane są osoby nieposiadające podstawowej wiedzy prawniczej, mające trudności nie tylko w interpretacji, ale i w zrozumieniu podstawowych terminów z RODO, zwłaszcza wobec pojawiających się w tym akcie prawnym pojęć niedookreślonych i niezdefiniowanych [104].

Podsumowując kluczowa również w tym zakresie wydaje się być znajomość specyfiki branży, RODO i przepisów szczegółowych, a także posiadania stosownego doświadczenia zawodowego, w tym w zakresie realizacji audytów dotyczących w zakresie bezpieczeństwa informacji i ochrony danych osobowych, jak również weryfikacji sposobów zabezpieczenia informacji przetwarzanych zarówno metodą tradycyjną, ale również przy użyciu urządzeń i nośników informacji. Zatem wiedza w obszarze bezpieczeństwa teleinformatycznego, a także oceny ryzyka i działań zapewniających i doradczych okazuje się fundamentalna. Szczegółowa analiza i rozwiązania dotyczące wymaganych i pożądanych kompetencji i kwalifikacji IOD zostaną omówione w rozdziale drugim niniejszej pracy.

I.6. Status prawny Inspektora Ochrony Danych, a dotychczasowa pozycja ABI

Pełnienie funkcji IOD nie może być dodatkiem do innych obowiązków pracowniczych. Niestety bardzo często zdarzało, że osoby, które pełniły funkcję ABI, nie miały czasu na rzeczywisty nadzór nad systemem ochrony danych osobowych w danym podmiocie, ponieważ inne obowiązki pracownicze były zbyt czasochłonne. Administratorzy danych oraz podmioty przetwarzające muszą uświadomić sobie, że to w ich interesie leży, aby IOD dysponował odpowiednim czasem do wykonywania swoich funkcji. Inspektor ochrony danych powinien być włączony w opiniowanie wszelkich procesów biznesowych w organizacji, wiążących się z przetwarzaniem danych osobowych. Inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług, czego nie wyklucza obecna u.o.d.o.

Dodatkowo RODO wskazuje administratorowi danych lub podmiotowi przetwarzającemu obowiązek wspierania IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania. IOD musi otrzymać wsparcie niezbędne do utrzymania fachowej wiedzy

104 E. Kulesza, *Problem niezależności inspektora ochrony danych*, op. cit., str. 120

i kompetencji na dobrym poziomie [105]. Zapewniają oni również, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. W ten sposób prawodawca unijny stara się zapewnić samodzielność, która ma być elementem niezależności inspektora ochrony danych. Chodzi o to, aby inspektor ochrony danych nie podlegał naciskom ze strony innych osób i mógł samodzielnie podejmować działania w ramach wykonywania swoich zadań [106].

Zgodnie z art. 36a ust. 8 u.o.d.o., na podmiotach korzystających ze wsparcia ABI ciążył obowiązek zapewniania mu środków niezbędnych do niezależnego wykonywania przez niego zadań. RODO przewiduje obowiązek wspierania inspektora ochrony danych w wypełnianiu przez niego zadań, m.in. poprzez zapewnienie mu zasobów niezbędnych do wykonywania tych zadań. Zarówno u.o.d.o., jak i RODO nie precyzują, jakie środki powinny być zapewnione, niemniej należy je rozumieć szeroko. Zakres oraz rodzaj niezbędnych środków powinien być ustalany indywidualnie z uwzględnieniem specyfiki i (mogących zmieniać się) potrzeb konkretnego podmiotu w zakresie przetwarzania danych osobowych. Innymi słowy, dla każdego ABI inne środki mogą okazać się niezbędne do wykonywania jego zadań. GR Art. 29 w Wytycznych dotyczących inspektorów ochrony danych, w punkcie „niezbędne zasoby", podkreśliła, że środki te należy rozumieć jak najszerzej, przy czym im bardziej skomplikowane procesy przetwarzania danych, tym więcej odpowiednich środków należy przeznaczyć dla inspektora ochrony danych tak, aby ochrona danych była skuteczna i odpowiednia do zakresu przetwarzanych danych [107].

Ponadto administrator oraz podmiot przetwarzający muszą zapewnić, aby inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Jeżeli więc nawet inspektor ochrony danych podjął samodzielnie decyzję z zakresu ochrony danych osobowych, to jego odpowiedzialność może być ograniczona ze względu na to, że nie udostępniono mu wszystkich informacji w sprawie. Przykładem niewyłączenia inspektora w sprawy dotyczące ochrony danych osobowych może być niezaproszenie inspektora na spotkanie dotyczące omówienia bezpieczeństwa informacji w spółce, na którym jego uczestnikom zostały przekazane informacje o zmianach w systemie informatycznym

105 S. Hady-Głowiak, *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, op. cit., str. 57

106 P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 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)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* WKP, Warszawa 2018, str. 433

107 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 15

spółki. Skoro więc IOD nie został poinformowany o zmianach i w konsekwencji nie zareagował odpowiednio w zakresie bezpieczeństwa danych osobowych przetwarzanych elektronicznie, to może być trudno przypisać mu winę (chyba że miał możliwość łatwego zapoznania się z tymi informacjami z innych źródeł, np. firmowego newsletera) [108].

Status IOD w organizacji jest zdecydowanie inny niż status ABI. IOD teoretycznie ma być jednostką niezależną w ramach organizacji, podczas gdy ABI był zależny i podlegał administratorowi i zarządowi. Ta niezależność IOD dotyczy stosunków wewnętrznych u administratora danych, a nie niezależności w ogóle, gdyż IOD ograniczają powszechnie obowiązujące przepisy prawa. Istotne, że IOD powinien być włączony we wszystkie sprawy dotyczące ochrony danych osobowych i mieć zapewnione przez administratora zaplecze niezbędne do wykonywania tych zadań [109].

Komentowany przepis nie zawiera wymogu organizacyjnej odrębności inspektora ochrony danych. Tego rodzaju wymóg przewidywał art. 36a ust. 8 u.o.d.o. z 1997 r. Może w związku z tym zrodzić się wątpliwość, czy niezależność inspektora ochrony danych wymaga wyodrębnienia organizacyjnego, czy też wyodrębnienie tego rodzaju nie jest elementem niezbędnym dla zapewnienia niezależności. Brak wskazania wyraźnego wymogu w tym zakresie skłania do uznania, że wyodrębnienie organizacyjne nie jest konieczne (inspektor może być pracownikiem określonego działu), jednak w zakresie wykonywania zadań inspektora powinien on podlegać bezpośrednio najwyższemu kierownictwu. W praktyce jednak optymalnym rozwiązaniem zazwyczaj jest stworzenie odrębnego organizacyjnie samodzielnego stanowiska (lub zespołu osób), jednak w małych strukturach organizacyjnych może okazać się to niemożliwe bądź niezasadne [110]. Mając powyższe na uwadze nie należy zgodzić się z tezą, że wyodrębnienie organizacyjne IOD nie jest konieczne, bowiem takie działanie może prowadzić do sytuacji, w której bezpośredni przełożony pracownika będącego IOD, będzie naciskał na zrealizowanie wprowadzonych przez IOD zaleceń.

Określenie, kto – w konkretnym przypadku – wchodzi w skład „najwyższego kierownictwa", wymaga uwzględnienia rodzaju podmiotu, będącego administratorem danych lub podmiotem przetwarzającym i obowiązującego w nim systemu zarządzania. Kierownictwem jednostki organizacyjnej może być osoba lub osoby (np. wchodzące w skład

108 M. Sarna, *Inspektor ochrony danych* [w:] pod red. W. Szczygielska, *RODO przewodnik po kluczowych zmianach*, op. cit., 2018, str. 37;

109 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

110 P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych …, op. cit.*, str.435

organu), które kierują jej pracami (np. ministrowie kierujący działami administracji rządowej, dyrektorzy szkół), prowadzą jej sprawy (np. zarząd spółki kapitałowej), albo podejmują zarobkową działalność (np. przedsiębiorcy jednoosobowi), działając jako administrator danych lub podmiot przetwarzający. Podległość najwyższemu kierownictwu jest jedną z gwarancji niezależnej, wysokiej pozycji inspektora ochrony danych w strukturze administratora. Takie umiejscowienie inspektora ma zapewniać najwyższemu kierownictwu bezpośrednią wiedzę na temat porad i zaleceń inspektora. Maksymalnie skraca też drogę raportowania w pilnych przypadkach, wymagających szybkich działań naprawczych, np. w sytuacji naruszenia ochrony danych osobowych [111].

Ponadto RODO idzie dalej precyzując, że IOD nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający [112] za wypełnianie swoich zadań.

Oceniając rolę i zadania inspektora ochrony danych według obecnie obowiązujących przepisów, status inspektora ochrony danych został określony właściwie jako status podmiotu doradczego i wspomagającego administratora (czy podmiotu przetwarzającego dane) w jego działaniach stanowiących przetwarzanie danych, nieposiadającego uprawnień, których wykonywanie mogłoby powodować konflikt z administratorem. Oznacza to, że nie ma potrzeby, aby w szczególny sposób gwarantować niezależność i nieusuwalność inspektora ochrony danych [113].

Oczywiście, RODO wskazuje, że IOD może wykonywać inne zadania i obowiązki, jednak nie powinny one powodować konfliktu interesów, podobnie jak to zostało uregulowane w art. 36a ust. 4 u.o.d.o.[114].

Oznacza to, że inne zadania i obowiązki IOD mogą być traktowane jako dodatkowe i nie powinny utrudniać, bądź uniemożliwiać właściwego wykonywania funkcji IOD [115].

Zatem IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział

111 M. Młotkiewicz, *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, op. cit., str. 14

112 S. Hady-Głowiak, *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, op. cit., str. 57

113 E. Kulesza, *Problem niezależności inspektora ochrony danych*, op. cit., str. 117

114 S. Hady-Głowiak, *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, op. cit., str. 57

115 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu, op. cit.*, str. 149

w określaniu celów i sposobów przetwarzania danych. Administrator może wybrać odpowiednią osobę wśród swoich pracowników, z uwzględnieniem konieczności zapewnienia jej możliwości skutecznego realizowania obowiązków. Powinien także pamiętać o tym, że gdy inspektor wykonuje także inne obowiązki, nie może dochodzić do konfliktu interesów [116].

Za dobrą praktykę należy uznać:

a) zidentyfikowanie (na piśmie) stanowisk skonfliktowanych interesami z rolą IOD w organizacji;

b) opracowanie wewnętrznych zasad i procedur uniemożliwiających łączenie stanowisk będących w konflikcie interesów (do umowy należy wpisać przynajmniej klauzulę ogólną, na podstawie której będą świadczone usługi inspektora ochrony danych);

c) odbieranie oświadczenia IOD o braku konfliktu interesów [117].

Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Mając na uwadze rozmiar i strukturę jednostki oraz zadania, w tym realizowane przez IOD, a także fakt jego zastępstwa w czasie jego usprawiedliwionej nieobecności istnieje konieczność, podobnie, jak to miało miejsce w przypadku ABI, powołania zespołu wspomagającego pracę IOD, w tym zastępcy IOD. Ta ostatnia możliwość została wprowadzona zmianą UODO poprzez dodanie art. 11a pozwalającego na wyznaczenie zastępcy IOD, co przed aktualizacją przepisów nie było możliwe. Przepis ten budzi szereg wątpliwości i może być źródłem problemów. Użyte przez prawodawcę sformułowanie wskazuje na to, że zastępca może wykonywać działania IOD jedynie w czasie jego nieobecności, podczas gdy w praktyce, zwłaszcza w dużych strukturach organizacyjnych, celowe i zasadne jest dokonanie podziału obowiązków między inspektora i jego zastępcę oraz wykonywanie tych zadań w tym samym czasie (nie tylko w czasie nieobecności IOD). W praktyce może to prowadzić do wypaczenia roli zastępcy IOD i ograniczać swobodę działań administratora w tym zakresie [118]. Należy również nadmienić, że wyznaczenie i odwołanie zastępcy IOD należy każdorazowo zgłaszać

116 S. Czub-Kiełczewska, *Okiem IOD-a: status i zadania IOD-a - dobre praktyki*, Lex/el. 2019, dostęp z dnia 16.11.2019 r.

117 M. Gawroński, M. Kibil*, Zadania Inspektora ochrony danych osobowych*, Lex/el. 2018, dostęp z dnia 09.02.2019 r.

118 P. Fajgielski, *Dostosowanie krajowych przepisów do wymogów ogólnego rozporządzenia o ochronie danych* (dodatek MoP 22/2019), Monitor Prawniczy 2019, Nr 22, str. 9

Prezesowi UODO. Rola zastępcy powinna być znacznie szersza i obejmować również współdziałanie z inspektorem wtedy, gdy jest on obecny w jednostce organizacyjnej [119].

Jednym z głównych obowiązków IOD jest współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, co z jednej strony znacznie precyzuje rolę i niezależność Inspektora w jednostce, a z drugiej definiuje jego podległość względem organu nadzorczego. Pełnienie funkcji punktu kontaktowego wiązać się będzie z koniecznością udzielania niezbędnych informacji i wyjaśnień osobom, których dane dotyczą oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia [120].

Przy wykonywaniu tego obowiązku IOD powinien pamiętać o zobowiązaniu do zachowania tajemnicy, jednak zakaz ten nie wyłącza możliwości kontaktowania się z organem nadzorczym w celu uzyskania porady. Co ważne, IOD może konsultować się z organem nadzorczym we wszystkich sprawach, a zatem jest to jego uprawnienie i nie ma takiego przymusu. ABI nie pełnił takiej funkcji, a osoby, których dane były przetwarzane, kontaktowały się bezpośrednio z administratorem [121].

Należy przypomnieć, że prawa osób, których dane są przetwarzane zostały w RODO znacząco wzmocnione i poszerzone, a nieprzestrzeganie praw sankcjonowane jest karą pieniężną sięgającą nawet do 20 000 000 euro. Właśnie w tym zakresie może być konieczne zagwarantowanie niezależności działania IOD w odniesieniu do działań wobec podmiotów danych, takich jak porada, informacja czy wsparcie fachowe, a nawet umożliwienie kontaktu z organem nadzorczym. Powyższe może bowiem ułatwić podmiotowi danych wystąpienie przeciwko administratorowi danych, na przykład poprzez uruchomienie procedury kontroli prawidłowości przetwarzania danych przez organ nadzorczy, czy zgoła doprowadzi do przyznania odszkodowania od administratora danych przez sąd cywilny. Jeśli zatem na gruncie RODO inspektor ochrony danych może stać się „adwokatem" podmiotu danych, powinien być w swoich działaniach niezależny od administratora i mieć swobodę wyboru instrumentów wsparcia osoby, której dane dotyczą, bez obawy, że poniesie konsekwencje za swoje działania zgodne z przepisami [122].

119 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu, op. cit.*, str. 148

120 S. Hady-Głowiak, *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, Kontroler Info nr 8 z 2017 r., str. 58

121 K. Hamelusz, *Zadania IOD względem ABI - analiza prawno-porównawcza*, op. cit.

122 E. Kulesza, Problem niezależności inspektora ochrony danych, op. cit., str. 117

Podkreślić należy, że dane kontaktowe inspektora będą musiały zostać ujawnione w trakcie zbierania danych od osób, których one dotyczą jako jeden z elementów spełnienia obowiązku informacyjnego. W przypadku działań zapewniających zostały one znacznie rozbudowane o konieczność prowadzenia szkoleń personelu i działań zwiększających świadomość, udzielania zaleceń informowania osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie. Ponadto zamiast prowadzenia sprawdzeń pojawił się obowiązek monitorowania przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego i prowadzenia powiązanych z tym audytów. Wszystkie te zadania muszą uwzględniać odpowiednią analizę ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Przepisy RODO wskazują także, iż inspektor ochrony danych może przeprowadzać audyty w zakresie przestrzegania wytycznych ustanowionych w przepisach. W RODO nie sprecyzowano terminów przeprowadzania ewentualnych audytów. Wydaje się jednak, że nie powinny być one być rzadsze niż raz w roku. Okres ten pozwala inspektorowi na ocenę zmian, jakie zachodzą w systemie przetwarzania danych funkcjonującym w organizacji, jak i pozwala na wprowadzenie rekomendacji wydanych przy poprzednim audycie. Europejski ustawodawca przewidział również możliwość wyznaczenia jednego inspektora ochrony danych przez grupę przedsiębiorstw. Warunkiem jest możliwość łatwego nawiązania kontaktu z inspektorem ochrony danych z każdej jednostki organizacyjnej [123].

Jeżeli chodzi o powołanie i odwołanie ABI to Administrator danych obowiązany był zgłosić do rejestracji GIODO jego powołanie i odwołanie w terminie 30 dni od dnia jego powołania lub odwołania. GIODO prowadził ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji. Powyższa kwestia została znacznie uproszczona w RODO, które wskazuje, że Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy [124]. Organ ochrony danych w takich sytuacjach będzie zatem prowadził wewnętrzną ewidencję inspektorów o charakterze pomocniczym [125].

123 S. Hady-Głowiak, *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, op. cit., str. 57

124 A. Kaczmarek, *Wyznaczenie Inspektora Ochrony Danych* [w:] red. B. Marcinkowski, *Ustawa o ochronie danych osobowych, Komentarz*, Wolters Kluwer Warszawa 2018, str. 44

125 D. Lubasz, *Wyznaczenie Inspektora Ochrony Danych,* [w:] D. Lubasz (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2019, str. 86

Ze względu na fakt, że IOD ma pełnić funkcję punktu kontaktowego dla osób, których dane dotyczą, jego dane kontaktowe (osobowe) będą podlegały publikacji. Informacje te będą także musiały być przekazywane podmiotom danych w związku z realizacją obowiązku informacyjnego zarówno przy zbieraniu danych od osoby, której dane dotyczą, jak i w razie pozyskania ich w inny sposób. Imię i nazwisko oraz dane kontaktowe IOD będą również umieszczane w rejestrze czynności przetwarzania danych, obowiązkowo prowadzonym przez wybranych administratorów. Informacje identyfikujące IOD stanowią także element zgłoszenia organowi nadzorczemu przypadku naruszenia ochrony danych osobowych [126].

Podobnie jak w przypadku ABI na gruncie poprzednio obowiązującej ustawy, administrator danych oraz podmiot przetwarzający zobowiązani są zawiadomić Prezesa Urzędu o wyznaczeniu Inspektora. Zawiadomienie to powinno zostać wysłane w terminie 14 dni od wyznaczenia Inspektora i powinno wskazywać imię, nazwisko oraz adres poczty elektronicznej oraz adres inspektora. W zawiadomieniu ponadto powinno znajdować się: imię i nazwisko oraz adres zamieszkania/ nazwa firmy oraz adres prowadzenia działalności gospodarczej administratora, pełną nazwę oraz adres siedziby, numer identyfikacyjny REGON. Zawiadomienie o odwołaniu Inspektora składa się do Prezesa Urzędu w terminie 14 dni od zmiany ww. danych. W przeciwieństwie do poprzednio obowiązującej ustawy zgłoszenie Inspektora może odbyć się jedynie elektronicznie (poprzednio dopuszczano zgłoszenia papierowe) za pośrednictwem formularza dostępnego w Internecie. Zgłoszenie musi być opatrzone kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym na e PUAP. [127]

Podmiot który wyznaczył Inspektora udostępnia dane inspektora w postaci imienia, nazwiska, adresu poczty elektronicznej, lub numeru telefonu inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Ponadto, wspólny IOD może zostać wyznaczony dla kilku organów lub podmiotów publicznych, jednak z uwzględnieniem ich struktury organizacyjnej i wielkości. Należy zauważyć, że odmiennie niż w przypadku powołania jednego IOD dla grupy przedsiębiorstw art. 38 ust. 3 RODO nie wprowadza wymogu łatwego nawiązania kontaktu z inspektorem.

126 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 79

127 A. Kaczmarek, *Wyznaczenie Inspektora Ochrony Danych* [w:] red. B. Marcinkowski, *Ustawa o ochronie danych osobowych, op. cit.*, str. 44-45

Uznać jednak należy, że ze względu na zadania nakładane na IOD bezpośrednio przez przepisy RODO te same wymogi komunikacyjne powinny być spełnione także w tym przypadku, co potwierdza w swoich wytycznych Grupa Art. 29 [128].

Doświadczenie audytowe w sektorze publicznym wskazuje, iż takie podmioty mają problemy z zabezpieczeniem organizacyjnym i technicznym danych osobowych. Dlatego też należy ostrożnie podchodzić do wyznaczenia jednego inspektora ochrony danych dla kilku podmiotów publicznych, gdyż może to powodować fikcyjny nadzór nad systemem ochrony danych w tych podmiotach [129]. Wskazane powyżej rozwiązania przyjęte w ogólnym rozporządzeniu spowodują, że znaczenie IOD, w porównaniu z rolą ABI w organizacjach, jeszcze wzrośnie, a jego status w ramach struktur ADO ulegnie dodatkowemu wzmocnieniu. Ten zabieg prawny – w zamiarze prawodawcy unijnego – powinien doprowadzić do zapewnienia większego poziomu ochrony danych osobowych. Jednocześnie nieco odmienny charakter IOD w porównaniu do ABI powoduje konieczność weryfikacji pełnienia dotychczasowych obowiązków przez osoby zajmujące się ochroną danych w ramach organizacji [130].

I.7. Funkcjonowanie IOD w ujęciu empirycznym

Podsumowując należy zwrócić uwagę na pewne elementy statystyk. W celu ich pozyskania zwrócono się do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych o przekazanie informacji w zakresie:

- liczby zarejestrowanych ABI przed zmianą przepisów o ODO,
- liczby obecnie zgłoszonych IOD do PUODO,
- wysokości nałożonych kar pieniężnych z podziałem na poszczególne lata w jednostkach, gdzie funkcjonował ABI, z uwzględnieniem rodzaju naruszenia,
- wysokości nałożonych kar po zmianie przepisów ODO w jednostkach, gdzie funkcjonuje IOD z uwzględnieniem rodzaju naruszenia,
- liczby skierowanych skarg do GIODO za poszczególne lata przed zmianą przepisów o ODO wraz z liczbą przeprowadzonych kontroli za poszczególne lata (z wyszczególnieniem jednostek, gdzie funkcjonował ABI),

128 J. Łuczak, Inspektor ochrony danych w sektorze publicznym, Lex/ el. 2018, dostęp z dnia 04.04.2019 r.

129 S. Hady-Głowiak, *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, op. cit., str. 57

130 T. A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* op. cit., str. 82

- liczby skierowanych skarg do PUODO za poszczególne lata po zmianie przepisów o ODO wraz z liczbą przeprowadzonych kontroli za ostatni okres (z wyszczególnieniem jednostek, gdzie funkcjonował IOD),
- liczby zgłoszonych naruszeń do PUODO po zmianie przepisów ustawy i sposobu reakcji organu - liczby podmiotów od których przyjęto wyjaśnienia i na tym zakończono czynności oraz podmiotów u których organ przeprowadził kontrolę lub podjął decyzję o jej przeprowadzeniu (z wyszczególnieniem jednostek, gdzie funkcjonował IOD).

Zwrócono się również o wskazanie rodzaju/branży podmiotów z uwzględnieniem podziału na jednostki publiczne i prywatne.

Z odpowiedzi przekazanej przez UODO [131] wynika, że do 24 maja 2018 r. ogólna liczba ABI wpisanych do jawnego, ogólnopolskiego rejestru ABI wyniosła 28 206. Jednakże organ zaznaczył, że liczba ta odzwierciedla zarejestrowane zgłoszenia powołania ABI, a nie liczbę osób, które pełniły tę funkcję, ponieważ w części przypadków zgłoszenia pochodziły od administratorów, którzy powołali do pełnienia tej funkcji tę samą osobę. Z kolei w odniesieniu do liczby zgłoszonych IOD organ wskazał, że od dnia 25 maja 2018 r. do Urzędu wpłynęło kilkadziesiąt tysięcy pism związanych z powołaniem inspektorów ochrony danych. Organ przy tym zaznaczył, że zgodnie z obowiązującymi przepisami nie prowadzi ewidencji w tym zakresie.

W odpowiedzi na pozostałe pytania organ wskazał, że :

- od 25.05.2018 r. do 31.12.2018 r. do UODO wpłynęło 5714 skarg i wszczęto 43 postępowania kontrolne,
- od 1.01.2019 r. do 26.04.2019 r. do UODO wpłynęło 2239 skarg i wszczęto 41 postępowań kontrolnych.
- od 25.05.2018 r. do 31.03.2019 r. do UODO zgłoszono 3799 naruszeń ochrony danych osobowych. Najwięcej naruszeń pochodzi z sektora ubezpieczeniowego i telekomunikacyjnego.

Podsumowując w 2017 r. było około 2,9 tys. skarg. Rok później było ich już ponad 5,5 tys., ale tylko po 25 maja 2018 roku, gdy zaczęliśmy stosować RODO wpłynęło ich prawie 4,5 tys. [132]. Rok 2019 to nieco ponad 9,3 tys. skarg. W roku 2020, co prawda liczba skarg zmalała, jednak nadal utrzymywała się wysoko – 6,4 tys. W 2019 roku UODO otrzymał ponad 6 tys. zgłoszeń naruszeń. W całym 2020 roku wpłynęło ich łącznie ponad 7,5 tys., na co wpływ miało przeorganizowanie działalności administratorów, którzy na skutek pandemii niejednokrotnie

131 Pismo UODO sygn. Z0.0143.104.2019.AK.2 z dnia 3 czerwca 2019 roku

132 M. Rzemka, *Urząd bliżej obywateli*, Newsletter UODO dla Inspektorów Ochrony Danych, nr 9/2019, str. 2

musieli rozpocząć prace w trybie zdalnym oraz dostarczać towary i usługi za pośrednictwem Internetu. Ponadto w minionych trzech latach odnotować należy znaczny wzrost liczby wpływających do UODO pytań prawnych dotyczących stosowania RODO, jak i zgłoszeń naruszeń ochrony danych, dokonywanych przez administratorów. To świadczy o tym, że administratorzy danych osobowych, inspektorzy ochrony danych, jak i sami obywatele bardzo szybko identyfikują problemy i oczekują wskazówek [133].

Według szacunkowych wyliczeń International Association of Privacy Professionals (IAPP) w konsekwencji ukonstytuowania statusu, jak i zadań inspektorów ochrony danych w RODO, w Europie zaistniała potrzeba powołania 28 000 inspektorów ochrony danych osobowych. W skali całego globu liczbę tę szacuje się na 75 000 [1] . Zapotrzebowanie na inspektorów ochrony danych jest przy tym szczególnie wysokie w takich branżach, jak: nowe technologie, marketing cyfrowy, finanse, służba zdrowia i handel detaliczny [134].

Z powyższych statystyk jednoznacznie wynika, że organ nadzorczy nie posiada wiedzy i nie prowadzi bieżących działań nadzorczych w zakresie spełnienia przez podmioty obowiązku ustawowego w zakresie wyznaczenia IOD. Z kolei liczba skarg i przeprowadzonych kontroli od dnia 25.05.2018 r., znacząco wzrosła w stosunku do poprzednich, gdzie GIODO realizował około 10 % kontroli. Należy przy tym podkreślić jednoznacznie zapotrzebowanie na fachowych IOD nie tylko w sektorze publicznym, ale również w sektorze prywatnym, a w szczególności w obszarze teleinformatycznym (telekomunikacja i nowe technologie), finansów, służby zdrowia oraz ubezpieczeniowym.

Przeprowadzono także badanie dotyczące kształtowania się i funkcjonowania instytucji IOD w wybranych jednostkach administracji samorządu terytorialnego. Wśród jednostek objętych badaniem należy wyróżnić m.in. Starostwo Powiatowe w Bochni, Jarosławiu, Krośnie, Tarnowie, Krakowie, Zakopanem, Urząd Gminy Nowy Targ, Urząd Gminy Tarnów, Urząd Miasta Jarosław, Urząd Miasta Krosno, Urząd Miasta Rzeszowa, Urząd Miasta Stary Sącz oraz Urząd Miasta Nowy Sącz. Do każdej z jednostek skierowano w drodze informacji publicznej ankietę zawierającą 15 pytań, a jej wyniki zostaną szczegółowo omówione w kolejnych rozdziałach niniejszej rozprawy stanowiąc niezbędny element rozważań funkcjonowania IOD w praktyce od instytucji ABI do obecnego stanu prawnego. Pozwolą one również na wskazanie występujących nieprawidłowości oraz wskazanie prawidłowych rozwiązań prawnych w tym zakresie.

133 *Za nami trzy lata RODO*, https://uodo.gov.pl/pl/138/2059 , dostęp z dnia 4.06.2021 r.

134 M. Otto, *Pozycja prawna inspektora ochrony danych – zarys prawnoporównawczy,* op. cit., str. 261

Z przeprowadzonych badań wynika jednoznacznie, że funkcja ABI była sprawowana we wszystkich badanych jednostkach. W większości badanych jednostek funkcję IOD pełnią osoby, które dotychczas wykonywały funkcję ABI. Powyższe pozwala na wysunięcie wniosku, iż osoby te posiadają wymagane doświadczenie zawodowe do sprawnego wykonywania zadań na danym stanowisku. W 8 z 13 badanych jednostek ABI, a obecnie IOD wykonuje czynności na innych stanowiskach, takich, jak sekretarz powiatu, naczelnik wydziału organizacyjnego, informatyk, czy kierownik wydziału ds. informatyki, co jednoznacznie może powodować konflikt interesów. IOD nie może zajmować w organizacji funkcji pociągającej za sobą określanie sposobów i celów przetwarzania danych, co ww. stanowiska potwierdzają. Zdaniem jednostek badanych w żadnym z tych przypadków nie istnieje konflikt interesów, co budzi poważne wątpliwości w zakresie braku świadomości kierowników tych jednostek. Należy zadać również pytanie, czy w jednostkach tych jest zapewniony odpowiedni stopień bezpieczeństwa przetwarzania danych osobowych i informacji prawnie chronionych. Po wejściu w życie RODO inspektorzy ochrony danych zostali wyznaczeni oraz zgłoszeni do Prezesa Ochrony Danych Osobowych. We wszystkich badanych jednostkach, na stronie internetowej jednostki zostały udostępnione dane IOD w postaci imienia, nazwiska, adresu poczty elektronicznej, lub numeru telefonu inspektora, niezwłocznie po jego wyznaczeniu. W 11 z badanych jednostek, które objęto wyżej wymienionym badaniem przeprowadzonym przez autora niniejszej pracy można stwierdzić, że IOD zatrudniony był najczęściej na podstawie umowy o pracę, a jedynie w jednym podmiocie na podstawie umowy cywilnoprawnej. Jedna z jednostek nie wskazała podstawy zatrudnienia IOD. We wszystkich badanych jednostkach stanowisko IOD zostało wyodrębnione w strukturze organizacyjnej jednostki jako samodzielne stanowisko podległe bezpośrednio Kierownikowi jednostki. Powyższe budzi poważne wątpliwości w jednostkach administracji publicznej, które często nie realizują powyższego z uwagi choćby na brak przesłanek ustawowych, co w jednostkach samorządu terytorialnego jest realizowane, jak wskazano powyżej.

Niepokój budzi fakt, że w niektórych z badanych jednostek IOD oprócz zajmowanego stanowiska, pełni również tą funkcję w innych podmiotach. W większości badanych jednostek IOD wykonuje swoje zadania w ramach pełnego etatu.

W 11 badanych jednostkach nie zgłoszono żadnego przypadku naruszenia do PUODO po zmianie przepisów ustawy, natomiast w dwóch jednostkach zgłoszono po jednym przypadku. Ponadto w większości badanych jednostek IOD prowadzi planowe audyty/sprawdzenia oraz doraźne wynikające z konkretnie zaistniałej sytuacji. IOD prowadzi szkolenia z poszczególnymi pracownikami indywidualnie, bądź w małych grupach- zawsze

przed dopuszczeniem do pracy nowo przyjętego pracownika i co dwa lata dla pozostałych pracowników. Ponadto IOD kontaktuje się z pracownikami z własnej inicjatywy bądź na prośbę pracownika w celu rozwiązania konkretnego problemu z zakresu ochrony danych. Wyniki ankiety wskazały co najmniej 2 przypadki nieprawidłowości w związku z funkcjonowaniem IOD, o których mowa powyżej. Pozostałe elementy zostaną szczegółowo omówione na konkretnych przykładach w kolejnych rozdziałach niniejszej pracy.

II. Status IOD w instytucji w ujęciu prawnym i pragmatycznym

II.1. Zasady prawidłowego wyznaczania i usytuowania IOD w instytucji w ujęciu sektorowym.

Zgodnie z zasadami wynikającymi z art. 37 ust. 1 RODO, o czym wspomniano w poprzednim rozdziale, Administrator i podmiot przetwarzający ma obowiązek wyznaczyć inspektora ochrony danych zawsze, gdy:

1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

2) główna działalność administratora 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;

3) główna działalność administratora polega na przetwarzaniu na dużą skalę danych osobowych wrażliwych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Ustawa z 10 maja 2018 r. odmiennie od ustawy o ochronie danych osobowych z 1997 r. i regulacji dotyczących powołania administratora bezpieczeństwa informacji (ABI), nakłada ogólny obowiązek powołania IOD na administratora danych i podmiot przetwarzający, jeżeli spełniają oni przesłanki wskazane w art. 37 RODO. Należy podkreślić, że nowe regulacje (RODO i UODO) rozszerzyły obowiązek powołania Inspektora na podmioty przetwarzające, co stanowi nowość w porównaniu ze starą ustawą. Obowiązek powołania Inspektora dotyczy zarówno podmiotów ze sfery prywatnej i publicznej [135].

Z treści art. 8. UODO wynika, że „Administrator i podmiot przetwarzający są obowiązani do wyznaczenia inspektora ochrony danych, zwanego dalej "inspektorem", w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679.”

135 A. Kaczmarek, *Wyznaczenie Inspektora Ochrony Danych* op. cit., str. 38

Można wyrazić wątpliwość co do zasadności wprowadzenia do krajowej regulacji prawnej tego rodzaju przepisu, gdyż komentowany artykuł nie niesie ze sobą nowej treści normatywnej, a zawarte w tym artykule odesłanie w żaden sposób nie uszczegóławia ani nie modyfikuje ogólnych norm określonych w unijnym rozporządzeniu, nie ma więc znaczenia prawnego [136].

Pierwsza przesłanka powołania Inspektora ma charakter podmiotowy (art. 37 ustęp 1 lit. a RODO), a dwie pozostałe – przedmiotowy (art. 37 ust. 1 lit. b i c RODO). Rozporządzenie nie zdefiniowało pojęcia „organ" i „podmiot publiczny" [137].

Jednym z istotnych problemów jest brak jednoznacznie określonych kategorii administratorów i podmiotów przetwarzających zobligowanych do wyznaczenia IOD, a także bardzo wąski katalog organów i podmiotów publicznych obowiązanych do jego wyznaczenia. wskazany w UODO. Powyższe wskazuje jednoznacznie na brak jednolitego stanowiska ustawodawcy w tym zakresie, mając na uwadze choćby realizację zadań w interesie publicznym oraz wytyczne GR art. 29 wskazujące wykazanie istnienia obowiązku wyznaczenia IOD albo jego braku.

Mając na uwadze wskazane wyżej regulacje i w celu dalszych rozważań konieczne jest wyjaśnienie pojęcia "organu lub podmiotu publicznego", na które wskazuje RODO. Grupa Robocza Art. 29 ds. ochrony danych (zwana dalej GR Art. 29) w wytycznych dotyczących Inspektorów Ochrony Danych stoi na stanowisku, że takie pojęcie powinno zostać określone na poziomie przepisów krajowych. Taki obowiązek będzie miał miejsce w przypadku wszystkich organów i podmiotów publicznych (niezależnie od zakresu przetwarzanych danych), jak również w stosunku do podmiotów, które w ramach swojej głównej działalności regularnie i na dużą skalę monitorują osoby lub jeżeli działalność podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych [138]. Warto podkreślić, że GR Art. 29 odsyłała w Wytycznych do akcesoryjnego wykorzystania definicji „organów sektora publicznego" zawartej w art. 2 dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego [139]. W świetle tego przepisu, organem sektora publicznego są państwowe,

136 P. Fajgielski, *Komentarz do ustawy o ochronie danych osobowych*, op. cit., str. 735

137 A. Kaczmarek, *Wyznaczenie Inspektora Ochrony Danych*, op. cit., str. 40

138 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 5, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

139 Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego Dz. Urz. UE L 345, str.90, ze zm.

regionalne lub lokalne władze, podmioty prawa publicznego oraz stowarzyszenia utworzone przez jedną lub kilka władz albo jeden lub kilka takich podmiotów prawa publicznego. Podmiot prawa publicznego został zdefiniowany jako jakikolwiek organ posiadający osobowość prawną, ustanowiony w szczególnym celu zaspakajania potrzeb w interesie ogólnym, który nie ma charakteru przemysłowego lub handlowego, finansowany w przeważającej części przez państwo, władze regionalne lub lokalne, czy też inne podmioty prawa publicznego. Z kolei w polskim porządku prawnym pojęcie organów publicznych i podmiotów publicznych przed wejściem w życie komentowanej ustawy było przede wszystkim przedmiotem ogólnych definicji normatywnych zawartych odpowiednio w art. 5 paragraf 2 pkt 3 k.p.a. oraz art. 9 ustawy z dnia 27.8.2009 r. o finansach publicznych [140], co korespondowało z powyższymi definicjami z dyrektywy 2003/98/WE [141]. Pojęcie jednostki sektora finansów publicznych [142] zostało zdefiniowane w art. 9 u.f.p. [143] Mając powyższe na uwadze do powołania inspektora zobowiązane są takie podmioty jak np. jednostki samorządu terytorialnego, organy władzy publicznej, ZUS, NFZ, uczelnie publiczne, PAN. Do kategorii organów i podmiotów

140 Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych Dz. U. z 2019 r. poz. 869 z późn. zm., zwana dalej u.o.f.p.

141 D. Lubasz, *Wyznaczenie Inspektora Ochrony Danych,* op. cit., str. 81

142 1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;

2) jednostki samorządu terytorialnego oraz ich związki;

3) związki metropolitalne;

4) jednostki budżetowe;

5) samorządowe zakłady budżetowe;

6) agencje wykonawcze;

7) instytucje gospodarki budżetowej;

8) państwowe fundusze celowe;

9) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;

10) Narodowy Fundusz Zdrowia;

11) samodzielne publiczne zakłady opieki zdrowotnej;

12) uczelnie publiczne;

13) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;

14) państwowe i samorządowe instytucje kultury;

15) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

143 Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych Dz. U. z 2019 r. poz. 869 z późn. zm.

publicznych prawodawca zaliczył również instytuty badawcze. W myśl art. 1 ust. 1 ustawy z dnia 30.4.2010 r. o instytutach badawczych [144], instytutem badawczym jest państwowa jednostka organizacyjna, wyodrębniona pod względem prawnym, organizacyjnym i ekonomiczno-finansowym, która prowadzi badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie i zastosowanie w praktyce [145].

Podmiotem publicznym obowiązanym do wyznaczenia IOD, zgodnie z art. 9 ustawy, jest również Narodowy Bank Polski, który jest bankiem centralnym Rzeczypospolitej Polskiej, a jego status i zadania określone są w ustawie z 29.8.1997 r. o Narodowym Banku Polskim [146].

Pomimo ogólnych definicji systemowych ustawodawca polski zdecydował się jednak uregulować autonomicznie pojęcia organów i podmiotów publicznych w UODO, pozostawiając odwołanie do u.f.p. z pominięciem regulacji k.p.a. Jak słusznie wskazuje się w doktrynie, pojęcie sektora finansów publicznych i pojęcie sektora publicznego nie jest jednak tożsame [147]. Z tego też względu należy podkreślić brak konsekwencji ustawodawcy w tym zakresie w aktualnym brzmieniu UODO i znacznie ogranicza krąg podmiotów publicznych obowiązanych do wyznaczenia IOD.

Ponadto należy zauważyć, że zadanie może być realizowane w interesie publicznym lub może być sprawowana władza publiczna nie tylko przez organy lub podmioty publiczne. Zadanie może być również realizowane przez inne osoby fizyczne i prawne podlegające prawu publicznemu lub prywatnemu, czy w sektorach - zgodnie z krajowymi regulacjami każdego państwa członkowskiego - takich jak np. transport publiczny, dostarczanie wody i energii, infrastruktura drogowa, radiofonia i telewizja publiczna, budynki użyteczności publicznej albo przez organy powołane dla zawodów regulowanych. W tych przypadkach sytuacja osób, których dane dotyczą może być bardzo podobna do sytuacji przetwarzania ich danych przez organy lub podmioty publiczne. W szczególności dane mogą być przetwarzane w podobnych celach, a możliwość wpływu osób, których dane dotyczą, na charakter tego przetwarzania może być ograniczona bądź wyłączona, co może wymagać dodatkowej ochrony, jaką daje powołanie IOD. Działalność IOD powinna obejmować również wszelkie operacje przetwarzania prowadzone przez jednostkę, w tym te niezwiązane z zadaniami realizowanymi w interesie publicznym [148] (np. zarządzanie bazą danych pracowników). GR Art. 29 podkreśla jednak,

144 Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych Dz. U. z 2019 r. poz. 1350 z późn. zm.

145 A. Kaczmarek, *Wyznaczenie Inspektora Ochrony Danych*, op. cit., str. 42

146 Ustawa z dnia 29.8.1997 r. o Narodowym Banku Polskim Dz. U. z 2019 r., poz. 1810 z późn. zm.

147 D. Lubasz, *Wyznaczenie Inspektora Ochrony Danych,* op. cit, str. 83

148 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający*, [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.),

że choć dla takich podmiotów obowiązek nie wynika z przepisów, to właśnie wobec istnienia pierwiastka publicznego w procesie przetwarzania, co może wymagać dodatkowej ochrony, jaką daje powołanie IOD, warto by administratorzy rozważyli zasadność wyznaczenia inspektora [149].

Mając powyższe na uwadze należy podkreślić, że wskazany w UODO katalog organów i podmiotów publicznych obowiązanych do wyznaczenia IOD jest bardzo wąski, ponieważ nie dotyczy choćby państwowych jednostek organizacyjnych nieposiadających osobowości prawnej, niebędących przedsiębiorstwem, czy instytucji lub jednostek organizacyjnych wykonujących zadania w interesie publicznym, zatem w takiej sytuacji analiza dobrowolnego powołania IOD wydaje się jedynym prawidłowym rozwiązaniem. Dodatkowo warto zauważyć, że obowiązek wyznaczenia inspektora spoczywać może zarówno na administratorze, jak i na podmiocie przetwarzającym, zależnie od tego, kto spełnia przesłanki obowiązkowego wyznaczenia IOD. W braku jednoznacznie określonych kategorii administratorów i podmiotów przetwarzających zobligowanych do wyznaczenia IOD kluczowe jest wskazanie istnienia obowiązku albo wykazanie jego braku. W tej sytuacji, zgodnie z wytycznymi GR Art. 29, każdy podmiot powinien przeprowadzić analizę, która pozwoli ustalić istnienie bądź nie obowiązku wyznaczenia IOD, albo – po ustaleniu braku obowiązku – należy rozważyć, czy w konkretnych okolicznościach wyznaczenie IOD nie jest zasadne. W celu podjęcia odpowiedniej decyzji administrator powinien przeprowadzić analizę oraz udokumentować ją. Po trzecie, treść komentowanego przepisu jednoznacznie wskazuje, że pozostali administratorzy (niewskazani w nim) mogą powoływać IOD, bowiem art. 37 RODO nie wprowadza zakazu wyznaczenia inspektora ochrony danych w przypadkach niemieszczących się w ust. 1 analizowanego przepisu [150].

W związku z bardzo ograniczonym katalogiem organów i podmiotów publicznych wskazanych w UODO obowiązanych do wyznaczenia IOD każda instytucja lub jednostka organizacyjna wykonująca zadania w interesie publicznym, a także prywatne jednostki realizujące zadania w interesie publicznym lub sprawujące władzę publiczną powinny każdorazowo przeprowadzić analizę wykazującą istnienie lub brak obowiązku wyznaczenia IOD i udokumentować ją. Rozwiązanie przyjęte w tym zakresie w polskim porządku prawnym pozostawia wiele do życzenia z uwagi na wskazanie bardzo wąskiego katalogu podmiotów

---

RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, WKP, Warszawa 2018, str. 774

149 D. Lubasz, *Wyznaczenie Inspektora Ochrony Danych, op. cit.*, str. 83

150 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 770

obowiązanych do wyznaczenia IOD w porównaniu z dotychczasową praktyką obowiązującą w innych państwach członkowskich. W ustawodawstwach poszczególnych państw członkowskich z jednej strony wskazywano w ustawodawstwie krajowym obowiązek powołania IOD w zależności od liczby zatrudnionych osób, a z drugiej strony wskazywano podmioty objęte obowiązkiem powołania inspektorów ochrony danych osobowych, o czym wspomniano w rozdziale I.3. Mając powyższe na uwadze najlepszym rozwiązaniem byłoby jednoznaczne wskazanie przez ustawodawcę obowiązku wyznaczenia IOD przez podmioty z sektora publicznego, w tym podmioty powiązane z sektorem publicznym, a w przypadku sektora prywatnego uzależniające obowiązek powołania stosownego inspektora ochrony danych od liczby zatrudnionych osób.

Należy również nawiązać do przeprowadzonych badań dotyczących kształtowania się i funkcjonowania instytucji IOD w wybranych jednostkach administracji samorządu terytorialnego, o których wspomniano w I rozdziale niniejszej pracy. Spośród jednostek objętych badaniem wszystkie z nich były obowiązane do wyznaczenia IOD, zatem przeprowadzenie analizy, która pozwoliłaby ustalić istnienie, bądź brak jego wyznaczenia okazało się zbyteczne. Funkcja ABI była sprawowana we wszystkich badanych jednostkach. W 12 z badanych jednostek funkcję IOD pełnią osoby, które dotychczas wykonywały funkcję ABI. W 1 przypadku na stanowisku IOD wyznaczono osobę, która nie pełniła wcześniej funkcji ABI. Z doświadczenia i praktyki wynika również, że analiza istnienia, bądź braku konieczności obowiązku wyznaczenia IOD jest prowadzona m.in. przez państwowe jednostki organizacyjne nieposiadające osobowości prawnej.

Druga przesłanka dotyczy sytuacji, gdy 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. Zdaniem Grupy Roboczej Art. 29 (Wytyczne WP 243) przetwarzanie danych osobowych jest „główną działalnością administratora", jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Główną działalnością będzie działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane. Z kolei o tym, czy przetwarzanie następuje na dużą skalę, powinny świadczyć takie czynniki, jak:

– liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa;
– zakres przetwarzanych danych osobowych;
– okres, przez jaki dane są przetwarzane;
– zakres geograficzny przetwarzania danych osobowych.

Natomiast pojęcie „regularne” powinno być rozumiane jako:

– stałe albo występujące w określonych odstępach czasu przez ustalony okres;
– cykliczne albo powtarzające się w określonym terminie;
– odbywające się stale lub okresowo.

Monitorowanie systematyczne oznacza zaś monitorowanie zgodnie z określonym systemem; zaaranżowane, zorganizowane lub metodyczne; odbywające się w ramach generalnego planu zbierania danych; przeprowadzone w ramach określonej strategii. W wytycznych podano też przykłady regularnego i systematycznego monitorowania osób oraz przetwarzania danych na dużą skalę, tj. obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie poczty elektronicznej; działania marketingowe oparte na danych itd.

Trzecią przesłanką jest sytuacja, gdy główna działalność administratora polega na przetwarzaniu na dużą skalę danych osobowych wrażliwych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Jak wskazano w Wytycznych 243, chociaż przepis używa słowa „i”, nie ma powodu, dla którego obie przesłanki powinny być stosowane jednocześnie. Zastosowanie powinna mieć alternatywa nierozłączna „lub”. Wystarczy zatem, gdy główna działalność ADO polega na przetwarzaniu na dużą skalę danych osobowych wrażliwych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Powyższe wskazówki nie dają oczywiście jednoznacznej odpowiedzi na pytanie, kiedy administrator lub podmiot przetwarzający powinni wyznaczyć IOD [151].

Do wyznaczenia inspektora są zobowiązane również podmioty, które w ramach swojej głównej działalności regularnie i na dużą skalę monitorują osoby, czyli także profilują, zwłaszcza przy działalności marketingowej, sprzedażowej. Nie jest dokładnie określone i zdefiniowane pojęcie dużej skali, ale większość firm marketingu bezpośredniego, banki, firmy ubezpieczeniowe, dostawcy usług telefonicznych lub internetowych, przetwarzanie związane z geolokalizacją, spersonalizowaną reklamą, będzie zobowiązana wyznaczyć IOD. W podmiotach, których działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, czyli na przykład i między innymi dotyczących stanu zdrowia, trzeba będzie obowiązkowo wyznaczyć IOD [152]. "Głównej działalności" nie należy interpretować w sposób wyłączający działalność w zakresie przetwarzania danych nierozerwalnie związaną z działalnością główną administratora lub podmiotu

151 A. Kręcisz – Sarna, *Kiedy w podmiocie trzeba powołać IOD,* Oficyna Prawa Polskiego, nr 62/2019, str. 21

152 P. Glen, *IOD – kosztowny obowiązek czy luksus,* Oficyna Prawa Polskiego, nr 58/2019, str. 14

przetwarzającego. Dla przykładu działalnością główną szpitali będzie zapewnianie opieki medycznej. Natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna. Ponadto każda placówka medyczna, spełniająca wymóg dużej skali przetwarzania danych osobowych, będzie zobowiązana do powołania Inspektora Ochrony Danych. "dużej skali" przetwarzania. Warto również w przypadku „dużej skali" przetwarzania odwołać się do projektu Medycznego Kodeksu Branżowego, zgodnie z którym powołanie IOD nie będzie konieczne:

1. co do zasady, indywidualnych praktykach lekarskich i pielęgniarskich, chyba że nie spełniają wymogów określonych w pkt 2 i 3;
2. placówkach udzielających świadczeń ambulatoryjnych, w tym AOS, które w ostatnich trzech miesiącach zrealizowały świadczenia dla nie więcej niż 600 pacjentów;
3. placówkach wyłącznie udzielających świadczenia w ramach POZ i nieposiadających więcej niż 2750 przypisanych pacjentów w ostatnich 3 miesiącach;
4. placówkach udzielających stacjonarnych i całodobowych świadczeń zdrowotnych: szpitalnych, które udzielały świadczeń zdrowotnych dla nie więcej niż 100 pacjentów oraz innych niż szpitalne, które udzielały świadczeń zdrowotnych dla nie więcej niż 150 pacjentów [153]. Zatem każda placówka medyczna, spełniająca wymóg dużej skali przetwarzania danych osobowych, będzie zobowiązana do powołania Inspektora Ochrony Danych, tym samym szpitale.

Kolejnym przykładem może być spółka świadcząca usługi ochrony mienia, prowadząca monitoring w szeregu prywatnych centrów handlowych i przestrzeni publicznej. Jej działalnością główną jest ochrona, natomiast związane z tym bezpośrednio jest przetwarzanie danych osobowych, co oznacza, że takie spółki również muszą powołać IOD. Z drugiej strony wszystkie podmioty, spółki i inne organizacje prowadzą określone działania wspierające, np. prowadząc listę płac albo korzystając ze standardowej obsługi IT. Są to przykłady niezbędnych działań wspierających prowadzenie działalności głównej. Mimo że działania te są konieczne lub niezbędne, zazwyczaj uznawane są za raczej za działania dodatkowe niż za główną działalność [154]. Należy podkreślić, iż nawet jeśli administrator spełnia warunki wyznaczenia

153 M. Łokaj, *Czy każda placówka medyczna będzie zobowiązana do posiadania Inspektora Ochrony Danych osobowych (IOD)?*, Lex/el. 2017, dostęp z dnia 3.04.2019 r.

154 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu

IOD, to podmiot przetwarzający na rzecz tego administratora takiego obowiązku mieć nie musi. Wyznaczenie przez niego IOD może jednak być spełnione w ramach dobrej praktyki.

Inaczej rzecz ma się wówczas, gdy administrator lub podmiot przetwarzający co prawda nie jest zobowiązany do wyznaczenia IOD, ale jest zainteresowany jego powołaniem, ponieważ uznaje potrzebę wskazania osoby do wypełniania zadań związanych z ochroną danych osobowych. Mamy wówczas do czynienia nie z wyznaczeniem IOD, ale ze wskazaniem pracownika albo zewnętrznego konsultanta, którzy będą zajmować się kwestiami ochrony danych osobowych w organizacji, ale nie będą pełnili funkcji IOD, a więc nie muszą podlegać wymogom wskazanym w analizowanych przepisach. W przypadku powołania takiej osoby istotne jest, aby nazwa stanowiska, status pracownika, pozycja i jego zadania nie wprowadzały w błąd. W związku z tym Grupa art. 29 zaleca poinformowanie pracowników organizacji, jak również organów ochrony danych, osób, których dane dotyczą, i ogółu społeczeństwa, iż osoba zatrudniona nie jest IOD w świetle przepisów rozporządzenia 2016/679 [155].

Przed przyjęciem RODO, GR Art. 29 stała na stanowisku, że IOD jest warunkiem rozliczalności, a powołanie IOD może ułatwić przestrzeganie przepisów jak również przyczynić się do wzrostu konkurencyjności przedsiębiorstwa. Prócz zapewnienia przestrzegania przepisów poprzez wprowadzenie mechanizmów rozliczania (np. ułatwienie dokonania oceny skutków dla ochrony danych lub przeprowadzania audytów) IOD odgrywają rolę pośredników pomiędzy zainteresowanymi stronami (np. organem ochrony danych osobowych, osobami, których dane dotyczą albo jednostkami w ramach przedsiębiorstwa) [156]. Dla porównania zrewidowane ustawodawstwo krajowe obowiązujące w Niemczech wyraźnie przewiduje obowiązek wyznaczenia inspektorów ochrony danych w stosunku do organów publicznych, które przetwarzają dane osobowe w sposób zautomatyzowany, a także podmiotów prywatnych. Należy tu mieć na uwadze sytuacje, jeżeli co najmniej 10 osób jest stale zatrudnionych przy automatycznym przetwarzaniu danych osobowych lub niezależnie od liczby osób zatrudnionych przy automatycznym przetwarzaniu, gdy:
– administrator lub podmiot przetwarzający podejmuje się przetwarzania podlegającego ocenie skutków dla ochrony danych (art. 35 RODO),

13 grudnia 2016 r. z późn. zm., str. 21, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

155 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 771

156 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 5, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

– działalność administratora obejmuje przetwarzanie danych do celów sprzedaży danych (tzw. brokerzy danych), przekazania danych anonimowo lub badania rynku lub opinii [157]. Mając powyższe na uwadze dobrą praktyką będzie obowiązek wyznaczenia IOD w zależności od liczby zatrudnionych osób i zaproponowane wcześniej rozwiązanie wskazania tego obowiązku w ustawodawstwie krajowym.

Zgodzić się należy z E. Bielak-Jomaa, że art. 37 RODO w istocie pozbawia IOD kompetencji związanych z ochroną danych w obszarze działań orzeczniczych, nie dając w istocie podstawy do zwolnienia sądów jako szczególnej kategorii administratorów będących podmiotami publicznymi z obowiązku powołania IOD. Zatem także w sądach IOD powinni zostać powołani, przy czym będą oni realizować swoje obowiązki w odniesieniu do przetwarzania danych przez administratora w każdej sferze poza związaną ze sprawowaniem wymiaru sprawiedliwości [158].

Do wyłączenia obowiązku wyznaczenia inspektora ochrony danych nie wystarczy uznanie danego organu za organ sądowy, lecz ma ono zastosowanie jedynie do przetwarzania danych w kontekście przetwarzania danych w ramach sprawowania wymiaru sprawiedliwości. W istocie nie mamy więc tutaj do czynienia z wyłączeniem podmiotowym, lecz z określeniem obszarów, w których powołany inspektor ochrony danych nie będzie miał kompetencji do wykonywania swoich zadań. Z zakresu kompetencji IOD będą wyłączone jedynie operacje przetwarzania danych ściśle mieszczące się w ramach czynności orzeczniczych (np. w odniesieniu do postępowania dowodowego), gdyż *ratio* tego wyłączenia jest zapewnienie gwarancji niezawisłości sędziowskiej. W pozostałym zakresie sądy mają obowiązek wyznaczenia IOD [159].

Przepis art. 10 UODO wprowadza obowiązek zawiadomienia o wyznaczeniu IOD Prezesa Urzędu Ochrony Danych Osobowych, który prowadzi wewnętrzną ewidencję zawiadomień. Obowiązek ten spoczywa na podmiocie wyznaczającym: administratorze lub procesorze i powinien być spełniony w terminie 14 dni od dnia wyznaczenia IOD [160]. Obowiązek ustawowy koresponduje z wymogami art. 37 ust. 7 RODO i ogranicza się zatem do zawiadamiania PUODO o danych kontaktowych inspektora, z czym nie wiąże się jakikolwiek skutek prawny związany ze skutecznością jego wyznaczenia (brak konstytutywnego charakteru

157 M. Otto, *Pozycja prawna inspektora ochrony danych – zarys prawnoporównawczy,* op. cit., str. 265 - 266

158 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

159 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 775

160 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit., str. 9

zgłoszenia). Czynność przyjęcia zawiadomienia ma charakter materialno-techniczny nieskutkujący wydaniem żadnego rozstrzygnięcia administracyjnego [161].

Jednocześnie przepisy nie precyzują, czy w umowie o świadczenie usługi IOD (zawieranej przez administratora lub procesora z podmiotem delegującym) ta konkretna osoba musi być wskazana. Należy przyjąć, że nie ma takiego wymogu, chociaż jest to z pewnością rekomendowane. W takiej umowie należy określić mechanizm wyznaczania konkretnej osoby fizycznej pełniącej funkcję IOD. Konkretyzacja tej osoby może nastąpić w ramach realizacji umowy [162].

ADO musi publikować na swojej stronie internetowej aktualne dane kontaktowe IOD – w tym jego imię, nazwisko oraz adres e-mail lub numer telefonu. Po drugie, powinien w uporządkowany sposób podawać dane kontaktowe IOD, w ramach realizacji obowiązków informacyjnych przy zbieraniu danych zgodnie z art. 13 i 14 RODO [163]. Jeśli dany podmiot nie prowadzi własnej strony internetowej, to takiej publikacji powinien dokonać w sposób ogólnie dostępny w miejscu prowadzenia działalności. Rozwiązanie to wydaje się niezgodne z RODO. Artykuł 37 ust. 7 RODO nie wymaga bowiem publikowania imienia i nazwiska inspektora, a jedynie podania jego danych kontaktowych, czyli np. adresu korespondencyjnego, numeru telefonu kontaktowego lub dedykowanego adresu e-mail. Zgodnie z Wytycznymi GR Art. 29 wskazanie dodatkowych informacji może być dobrą praktyką, ale decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć powinno od administratora lub podmiotu przetwarzającego i IOD [164]. Brak opublikowania wymaganych danych IOD czy publikacja niepełnych danych (np. bez imienia i nazwiska) jest naruszeniem wymogów RODO oraz UODO – co niestety często można zauważyć [165]. Jednakże w przypadku jednostek samorządu terytorialnego objętych badaniem ankietowym, o którym mowa wszystkie udostępniły na swojej stronie internetowej dane IOD w postaci imienia, nazwiska, adresu poczty elektronicznej lub numeru telefonu inspektora, niezwłocznie po jego wyznaczeniu. Mając powyższe na uwadze należy tutaj przytoczyć zasadę pierwszeństwa prawa UE przed przepisami konstytucyjnymi państw członkowskich wynikającą z wyroku Trybunału Sprawiedliwości z dnia 17 grudnia 1970 r. 11/70. Tym samym prawidłowym rozwiązaniem będzie usunięcie niezgodności przepisów prawa krajowego

161 D. Lubasz, *Wyznaczenie Inspektora Ochrony Danych, op. cit.,* str. 87

162 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym,* Wolters Kluwer, Warszawa 2018, str. 245

163 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 12

164 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit.

165 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 9

z art. 37 ust. 7 RODO, a dobrą praktyką publikowanie dodatkowych informacji przez ADO ułatwiających kontakt z IOD.

II.2. Wyznaczenie jednego IOD dla wielu podmiotów.

Nałożenie na organy i podmioty publiczne obowiązku wyznaczenia IOD spowodowało zwiększenie zapotrzebowania na osoby mogące pełnić tę funkcję oraz ukazało deficyt osób merytorycznie przygotowanych do pełnienia tej funkcji na rynku pracy. Swego rodzaju złagodzeniem problemów wynikających z niedostatków kadrowych w tym zakresie jest również możliwość sprawowania funkcji inspektora ochrony danych przez jedną osobę dla wielu administratorów (lub podmiotów przetwarzających) [166].

RODO przewiduje możliwość wyznaczenia przez organy lub podmioty publiczne wspólnego IOD dla kilku takich podmiotów lub organów, przy czym w procesie tym musi zostać uwzględniona struktura organizacyjna i wielkość administratorów [167].

W praktyce jest to konstrukcja dość często wykorzystywana, choć niekiedy nasuwa wątpliwości, co do faktycznej możliwości wykonywania zadań przez IOD dla wszystkich obsługiwanych w ten sposób podmiotów (np. jeden inspektor wspólny dla wszystkich bądź bardzo wielu jednostek organizacyjnych podległych dużej gminie miejskiej) [168]. Nadinterpretacja tego przepisu przez organy administracji publicznej powodowana często chęcią uzyskania nadmiernych oszczędności prowadzi najczęściej do naruszeń przepisów i wpływa na właściwe i rzetelne wypełnianie przez IOD jego podstawowych zadań, a co za tym idzie brak efektywności i skuteczności zadań realizowanych przez organ administracji publicznej. RODO nie wskazuje, w jaki sposób podmioty te ustalają między sobą właściwość w tym zakresie, czy i pod jakimi warunkami mogą odstąpić od podjętej wcześniej decyzji o wyznaczeniu wspólnego IOD [169]. Główną rolę w zakresie wyznaczenia wspólnego IOD dla kilku takich podmiotów lub organów odgrywać powinna przede wszystkim dostępność IOD, bowiem częste nadinterpretacje tego przepisu prowadzą do stworzenia fikcyjnego stanowiska oraz braku możliwości faktycznej realizacji zadań przez IOD i sprzyjają naruszeniom przepisów o ochronie danych osobowych przez jednostki sektora finansów publicznych. Biorąc pod uwagę fakt, iż IOD posiada wiele zadań, administrator albo podmiot przetwarzający musi

166 P. Fajgielski, *Inspektor Ochrony Danych w sektorze publicznym,* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019, str. 157

167 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

168 P. Fajgielski, *Inspektor Ochrony Danych w sektorze publicznym,*, op. cit., str. 157

169 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 775

mieć pewność, że jeden IOD, z zespołem, jeśli jest to niezbędne, pozytywnie wypełni swoje obowiązki pomimo wyznaczenia go dla kilku podmiotów i organów publicznych [170]. Ponadto nie jest jasne, czy będzie on reprezentantem każdego z administratorów w każdej sprawie, czy też prezentować będzie wspólne stanowisko wszystkich. Jeden inspektor wyznaczony np. dla kilku ministerstw nie zawsze będzie mógł realizować swoje zadania w sposób właściwy, biorąc pod uwagę różne cele i zakres działań różnych ministerstw. Analiza art. 37–39 wskazuje na to, że wyznaczenie jednego inspektora możliwe będzie, jeżeli administrator będzie miał pewność, że jeden IOD pozytywnie wypełni swoje obowiązki pomimo wyznaczenia go dla kilku podmiotów i organów publicznych. W tym przypadku administratorzy powinni więc przeanalizować możliwości faktycznego działania we wszystkich podmiotach po to, aby upewnić się, że będzie on mógł wypełniać swoje obowiązki w sposób prawidłowy. To oznacza, że ani liczba tych podmiotów nie może być zbyt duża, ani ich struktura i organizacja w zasadniczy sposób nie mogą różnić się od siebie, a wspólny inspektor powinien być wyznaczony przez organy, które są ze sobą powiązane. Należy również pamiętać, że administratorzy, ponosząc odpowiedzialność za procesy prawidłowego przetwarzania danych, powinni być najbardziej zainteresowani w zapewnieniu właściwych narzędzi i mechanizmów współpracy z IOD oraz w zapewnieniu im niezależności. Pierwszorzędne znaczenie ma więc fakt, że IOD pełniący funkcję na rzecz kilku podmiotów publicznych musi znać nie tylko przepisy i procedury ochrony danych, ale także przepisy procedur administracyjnych oraz przepisy dotyczące przetwarzania danych przez organy lub podmioty w zakresie wykonywanych przez nie zadań publicznych, a także właściwe przepisy ustrojowe. Poszczególne organy/podmioty muszą mieć zapewniony łatwy kontakt z inspektorem ochrony danych [171].

Mając powyższe na uwadze w badaniu ankietowym, o którym mowa w I rozdziale pracy w 7 spośród 13 jednostek samorządu terytorialnego objętych badaniem IOD prowadzi jednocześnie obsługę innych podmiotów, a w 4 z nich osoba ta wykonuje również inne zadania. Powyższe stanowi potwierdzenie tezy, iż chęć uzyskania nadmiernych oszczędności może powodować brak rzeczywistego nadzoru IOD nad przestrzeganiem przepisów z zakresu ochrony danych osobowych, co wpływa na jakość oraz rzetelne wypełnianie podstawowych zadań w tym zakresie. Powyższe wskazuje na brak możliwości rzetelnej realizacji nałożonych

170 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 12, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

171 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający,* op. cit., str. 777

na IOD zadań ustawowych, co w konsekwencji prowadzi do naruszeń przepisów o ochronie danych osobowych. Prawidłowym rozwiązaniem dla każdego ADO przed wyznaczeniem jednego IOD dla kilku podmiotów i organów publicznych będzie przeprowadzenie wnikliwej analizy zapewniającej spełnienie kryterium dostępności i łatwego kontaktu z inspektorem oraz co najważniejsze pełną realizację przez IOD swoich obowiązków ustawowych.

Przepisy RODO (art. 37 ust. 6) dopuszczają możliwość sprawowania funkcji inspektora ochrony danych przez osobę, która nie jest pracownikiem administratora (podmiotu przetwarzającego), a wykonuje zadania inspektora na podstawie umowy o świadczenie usług (umowy zlecenia). Na tym tle zrodziła się w praktyce wątpliwość, czy ta sama osoba może pełnić funkcje IOD na podstawie umowy o świadczenie usług dla wielu różnych podmiotów. Niekiedy neguje się taką możliwość uzasadniając, że skoro prawodawca wyraźnie przewidział możliwość wyznaczenia wspólnego inspektora ochrony danych dla kilku organów lub dla grupy przedsiębiorstw, a nie zawarł w RODO przepisu odnoszącego się do pełnienia funkcji inspektora ochrony danych dla różnych podmiotów, to takiej możliwości nie ma. Tego rodzaju interpretacja nie wydaje się właściwa, wnioskowanie *acontrario* z braku przepisów może prowadzić do błędnej wykładni. Fakt braku szczególnego unormowania pełnienia funkcji inspektora ochrony danych dla różnych podmiotów nie powinien być uznawany za podstawę formułowania zakazu w tym zakresie, gdyż w przepisach RODO tego rodzaju zakaz nie został ustanowiony. Z kolei przepisy wskazujące na możliwość pełnienia funkcji inspektora ochrony danych na podstawie umowy o świadczenie usług wskazują, że prawodawca dopuszcza taką możliwość, z zastrzeżeniem jednak, że pełnienie funkcji IOD nie powinno prowadzić do konfliktu interesów [172].

Reasumując, prawodawca unijny nie wprowadza obowiązku powołania dla kilku organów/podmiotów publicznych jednego inspektora ochrony danych. Powołanie jednego IOD traktuje jako uprawnienie uzasadnione ekonomicznie i racjonalne z punktu widzenia zapewnienia prawidłowego przetwarzania danych osobowych przez podmioty publiczne, jeżeli spełnione są wskazane w przepisach rozporządzenia 2016/679 warunki. W RODO brak jest regulacji dotyczących sposobu powoływania oraz odwoływania wspólnego IOD. Prawodawca europejski nie wyznaczył także formalnej granicy, przez ile podmiotów może zostać powołany ten sam IOD, jednak wyznaczenie inspektora dla kilku podmiotów nie może negatywnie wpływać na wykonywanie powierzonych mu zadań. Powinien on zatem móc wywiązywać się w pełni ze wszystkich obowiązków związanych z ochroną danych osobowych, u każdego

172 P. Fajgielski, *Inspektor Ochrony Danych w sektorze publicznym,* op. cit., str. 158

z administratorów. Uznać należy, że może on w tym zakresie korzystać ze wsparcia podległego mu zespołu czy zastępców IOD, jeśli tacy zostaną wyznaczeni w strukturze administratora, zgodnie z dokumentacją wewnętrzną (np. polityką ochrony danych) [173]. Zapewnieniu efektywności służyć mają uprawnienia i pozycja IOD. Inspektor zaś działa w interesie każdego z administratorów oddzielnie. Co istotne, aby zapewnić zgodność działania organizacji z przepisami z zakresu ochrony danych osobowych, w szczególności w przypadku incydentów bezpieczeństwa czy innego rodzaju naruszenia praw podmiotów danych, rekomendowane jest choćby ramowe określenie czasu reakcji IOD na określone kategorie zdarzeń. Wskazane jest także umożliwienie inspektorowi ochrony danych pozostawania w kontakcie z pracownikami administratora poza godzinami pracy IOD, np. poprzez dostęp do skrzynki mailowej lub skorzystanie z telefonu służbowego. W przypadku naruszenia ochrony danych osobowych, zgodnie z treścią art. 33 ust. 1 RODO, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu [174]. Dlatego administratorzy przed podjęciem decyzji o wyznaczeniu jednego inspektora dla kilku organów powinni odpowiedzialnie rozważyć, czy z uwagi na charakter działalności, cele i zadania, które organ/podmiot publiczny realizuje, wyznaczenie jednego IOD będzie spełniało standardy jego niezależności i zapewni efektywność jego działań, tak aby wpierać administratora i monitorować prawidłowość procesów przetwarzania danych osobowych [175].

Na zasadzie analogii skonstruowana została dobrowolność wyznaczenia IOD dla kliku podmiotów w ramach podmiotów publicznych oraz w grupie przedsiębiorstw [176].

Należy zauważyć, że odmiennie niż w przypadku powołania jednego IOD dla grupy przedsiębiorstw art. 38 ust. 3 RODO nie wprowadza wymogu łatwego nawiązania kontaktu z inspektorem. Uznać jednak należy, że ze względu na zadania nakładane na IOD bezpośrednio przez przepisy RODO te same wymogi komunikacyjne powinny być spełnione także w tym przypadku, co potwierdza w swoich wytycznych Grupa art. 29. RODO nie wprowadza wymogu

173 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

174 K. Kozieł, S. Sieniewicz, *Weryfikacja kwalifikacji IOD-a i zadań przez niego realizowanych ze wskazaniem środków kontroli,* Lex/el. 2018, dostęp z dnia 18.05.2019 r.

175 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 777

176 M. Czaplińska, *IOD dla grupy przedsiębiorstw, komentarz praktyczny*, LEX/el. 2018, dostęp z dnia 4.04.2019 r.

powołania jednego IOD dla tych samych organów i podmiotów publicznych (organów i podmiotów tego samego rodzaju) [177].

Artykuł 37 (2) stanowi, iż grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile "można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej". Pojęcie łatwości kontaktu odnosi się do zadań IOD związanych z komunikacją z osobami, których dane dotyczą i obowiązkami punktu kontaktowego dla organu nadzorczego, jak również funkcjonowaniem wewnątrz podmiotu, biorąc pod uwagę fakt, iż jednym z zadań IOD jest "informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia". Warto zauważyć, że pojęcie łatwości kontaktu – przy uwzględnieniu zadań IOD – odnosić się będzie, po pierwsze, do sprawnego komunikowania się z inspektorem ochrony danych, a więc udostępnienia jego danych kontaktowych zarówno wszystkim administratorom zrzeszonym w grupie przedsiębiorstw, jak i osobom, których dane dotyczą. Osoby te mają prawo kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących. Po drugie, łatwość nawiązania kontaktu zrealizowana może być poprzez zapewnienie odpowiedniego organizacyjnego i technicznego wsparcia inspektorowi. Łatwość odnosi się bowiem także do możliwości sprawnego działania, co oznacza również, że komunikacja musi odbywać się w języku lub językach używanych przez organy nadzorcze i osoby, których dane dotyczą [178].

Zgodnie z powyższym IOD, przy pomocy zespołu, jeśli to niezbędne, powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą i współpracy z właściwym organem nadzorczym [179].

RODO nie daje wskazówek co do tego, w jaki sposób IOD ma być zatrudniony przez spółki z grupy. Może być on pracownikiem każdej ze spółek zatrudnionym na część etatu bądź świadczyć dla nich pracę w ramach umów cywilnoprawnych. Spółki z grupy mogą podpisać wspólne porozumienie dotyczące wyznaczenia jednego IOD. Mogą być również wprowadzone odpowiednie postanowienia do polityki ochrony danych w grupie kapitałowej. W porozumieniu należy ustalić, jak będą rozliczane koszty dotyczące IOD w grupie. Jeżeli będzie on zatrudniony przez jedną ze spółek, np. spółkę matkę, to zapewni ona oprócz wynagrodzenia również

177 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

178 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 785

179 M. Czaplińska*, IOD dla grupy przedsiębiorstw, komentarz praktyczny*, op. cit.

niezbędne środki do wykonywania funkcji IOD. Należy zatem ustalić, czy w związku z tym pozostałe spółki-córki zostaną obciążone kosztami administracyjnymi w tym zakresie. Należy pamiętać, że każda ze spółek ma obowiązek odrębnie powiadomić Prezesa UODO o wyznaczeniu IOD, zgodnie z wymaganiami art. 10 UODO oraz opublikować informację o wyznaczonym IOD zgodnie z art. 11 UODO [180].

Zatem w celu dopełnienia formalności związanych z wyznaczeniem IOD dla grupy przedsiębiorstw podmioty z grupy powinny zawrzeć umowę formułującą deklarację, że jedna ze spółek dokona wyznaczenia IOD dla grupy przedsiębiorstw, którą stanowią, zawierając w tym celu umowę z IOD, której postanowienia w zakresie wykonywania zadań przez IOD oraz obowiązków wynikających z RODO będą wiązać wszystkie strony umowy. Istotne pozostaje złożenie przez podmioty z grupy oświadczenia, że z IOD wyznaczonym dla grupy przedsiębiorstw będzie można łatwo nawiązać kontakt z każdej ze spółek będących stroną umowy, wskazując jednocześnie sposób realizacji tego postanowienia umownego [181].

Innym rozwiązaniem, które spotykam w grupach kapitałowych, jest wyznaczanie odrębnych IOD dla każdej ze spółek i powołanie wspólnego zespołu inspektorów dla grupy kapitałowej, którego przewodniczącym zwykle jest IOD w spółce matce. Taki zespół ustala wspólne standardy i wytyczne dotyczące zapewnienia przestrzegania przepisów RODO w grupie [182].

W ramach wspólnego wyznaczenia IOD strony takiej umowy winny także oświadczyć, że każda z nich osobno dopełni obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD na zasadach określonych w art. 10 ustawy z 10.05.2018 r. o ochronie danych osobowych. Z punktu widzenia IOD powołanego dla całej grupy istotne jest, że jego działania dotyczyły monitorowania przestrzegania przepisów RODO i polityk funkcjonujących dla poszczególnych przedsiębiorstw [183].

Powołanie wspólnego IDO możliwe będzie, np. w ramach placówek medycznych prowadzonych w formie spółek prawa handlowego tworzących jedną grupę kapitałową. Z kolei w odniesieniu do placówek publicznych można zastosować rozwiązanie, zgodnie z którym jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla

180 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 7-8

181 M. Czaplińska, *IOD dla grupy przedsiębiorstw, komentarz praktyczny*, op. cit.

182 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 8

183 M. Czaplińska*, IOD dla grupy przedsiębiorstw, komentarz praktyczny*, op. cit.

kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych [184].

Niezależnie od przyjętych wyżej wymienionych rozwiązań do prawidłowego wykonywania funkcji IOD zarówno dla kilku podmiotów i organów publicznych, czy w grupie przedsiębiorstw niezbędne jest również:

- wykluczenie możliwości wystąpienia konfliktu interesów,
- zapewnienie standardów niezależności i efektywność działań IOD w zakresie monitorowania prawidłowości procesów przetwarzania danych osobowych i skutecznej reakcji IOD w przypadku incydentów bezpieczeństwa czy innego rodzaju naruszenia praw podmiotów danych,
- utworzenie rozwiązań umożliwiających zapewnienie łatwego kontaktu z inspektorem zarówno wszystkim administratorom zrzeszonym w grupie przedsiębiorstw, jak i osobom, których dane dotyczą oraz realizację obowiązków punktu kontaktowego dla organu nadzorczego,
- zapewnienie odpowiedniego organizacyjnego i technicznego wsparcia IOD w realizacji zadań poprzez utworzenie zespołu czy zastępców IOD w ramach w struktury organizacyjnej administratora.

II.3. Kompetencje i kwalifikacje IOD

Inspektor ochrony danych nie jest zawodem regulowanym. Nie ma też mechanizmów weryfikujących umiejętności kandydatów na to stanowisko. Często administratorzy nie potrafią zaakceptować rzeczywistego celu powołania IOD, czyli profesjonalnego doradcy ds. ochrony danych osobowych, pełniącego nadzór nad systemem ich przetwarzania i ochrony, a nie osoby odpowiedzialnej za tworzenie i utrzymanie tego systemu w organizacji. Brakuje też wyraźnego doprecyzowania, czy IOD to tylko nowe zadanie w zakresie obowiązków pracownika lub współpracownika, nowa funkcja w organizacji (a w rzeczywistości – czy to następca ABI, działającego według zasad wynikających z u.o.d.o., znowelizowanej w 2014 r.), czy też nowe, nadal tworzące się w świadomości pracodawców stanowisko o charakterze eksperckim, dla którego nie przewidziano odpowiednich nawiązań w przepisach dotyczących klasyfikacji zawodów i stanowisk w organizacjach [185].

184 M. Łokaj, *Kiedy kilka publicznych placówek medycznych będzie mogło mieć wspólnego IDO?,* Lex/el. 2017, dostęp z dnia 4.04.2019 r.

185 M. Kołodziej, *Podstawy prawne powołania inspektora ochrony danych,* op. cit., str. 28

Najważniejszą kwestią w zakresie funkcjonowania IOD i realizacji przez niego zadań jest brak jednoznacznych przesłanek prawnych określających wymogi na tym stanowisku. Zgodzić się należy z twierdzeniem, że rozporządzenie nie dostarcza jednak szczegółowych wytycznych w zakresie wymaganych kompetencji oraz sposobów ich weryfikacji, co w praktyce może budzić wątpliwości [186].

Należy przy tym mieć na uwadze zarówno specyfikę branży, znajomość RODO i przepisów szczegółowych, doświadczenie zawodowe w realizacji audytów w zakresie bezpieczeństwa informacji oraz wiedzę praktyczną dotyczącą najlepszych praktyk zabezpieczeń w zakresie przetwarzania informacji chronionych (metodą tradycyjną oraz za pomocą urządzeń takich jak komputer stacjonarny, laptop, smartphone, tablet, czy zewnętrznych nośników danych).

Ostatecznie pożądanym obszarem świadomości, wiedzy i umiejętności IOD są kwestie dotyczące spraw organizacyjnych i proceduralnych. Jest to na pewno umiejętność analizowania ryzyka, tworzenia i stosowania polityk, procedur i instrukcji, a w obszarze kompetencji miękkich – zdolność do zbierania wiedzy o potencjalnych kierunkach ataku w organizacji, przykładowych profili możliwych napastników oraz budowania kultury bezpieczeństwa w organizacji [187]. Powyższe zapewni organizacji fachową pomoc i doradztwo w zakresie zapewnienia ciągłości działania jednostki.

I tak zgodnie z art. 37 ust. 5 RODO Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39. Z kolei z rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania, wynika, że zawód ten został sklasyfikowany pod pozycją audytor/kontroler w ramach specjalistów do spraw administracji i rozwoju. Próby skonkretyzowania tych kryteriów odnajdziemy zarówno w praktyce stosowania przepisów krajowych o ochronie danych osobowych, jak i przepisów unijnych. Przykładem są przepisy dotyczące stanowisk i szczegółowych zasad wynagradzania urzędników i innych pracowników sądów i prokuratury, wprowadzające stanowisko inspektora ochrony danych w sądach powszechnych i wojskowych.

---

186 K. Kozieł, S. Sieniewicz, *Weryfikacja kwalifikacji IOD-a i zadań przez niego realizowanych ze wskazaniem środków kontroli*, Lex/el. 2018, Lex/el. 2018, dostęp z dnia 18.05.2019 r.

187 M. Gruszczyński, T. Wącirz, *Cechy dobrego inspektora ochrony danych* [[w:] M. Kołodziej (red.), *Vademecum Inspektora Ochrony Danych*, C.H. Beck, Warszawa 2020, str. 55

Co ciekawe w tym wypadku wymaga się jedynie dodatkowo, żeby IOD miał ukończone studia drugiego stopnia. Innym przykładem jest wykaz stanowisk urzędniczych w Biurze Krajowej Rady Radiofonii i Telewizji. Od osoby zatrudnionej na stanowisku IOD wymaga się wykształcenia wyższego magisterskiego oraz 7 lat pracy (w tym na stanowisku kierowniczym) [188] . Dobrą praktyką może być uwzględnienie wytycznych dla inspektorów ochrony danych w instytucjach EU, w których zalecane jest wymaganie od IOD co najmniej siedmiu lat odpowiedniego doświadczenia, aby dana osoba mogła pełnić funkcję inspektora ochrony danych w instytucji lub organie, w których ochrona danych jest związana z podstawową ich działalnością lub które mają istotny wolumen operacji przetwarzania danych osobowych [189].

Konieczne kwalifikacje zawodowe i specjalistyczna wiedza obejmują:

1) doświadczenie w zakresie unijnych przepisów o ochronie prywatności i ochrony danych osobowych;

2) wiedzę dotyczącą zastosowań technologii informacyjno-komunikacyjnych i bezpieczeństwa teleinformatycznego;

3) dobre zrozumienie sposobu, w jaki funkcjonuje instytucja lub organ, tego, jak są w niej przetwarzane dane osobowe;

4) umiejętność interpretacji odpowiednich przepisów dotyczących ochrony danych w tych instytucjach lub organach. Prawidłowa realizacja zadań przez IOD będzie często wymagała w praktyce posiadania przez nich wiedzy z bardzo różnych dziedzin, nie tylko z zakresu przepisów prawa o ochronie danych osobowych – znajomości funkcjonowania systemów teleinformatycznych, wiedzy z zakresu przeprowadzania szkoleń, metodologii prowadzenia kontroli i opracowywania specjalistycznej dokumentacji, ale także – a może nawet przede wszystkim – umiejętności współpracy z ludźmi w ramach konsultacji z innymi jednostkami w danej instytucji i poza nią [190]. Istotność roli przypisanej IOD w ramach modelu ochrony danych osobowych wynika z faktu, że została ona zaprojektowana jako swoisty gwarant właściwego przestrzegania przepisów o ochronie danych osobowych, dlatego też IOD musi spełniać wymagania dotyczące kwalifikacji zawodowych, wiedzy, doświadczenia, umiejętności, warunku dokształcania się [191]. Motyw 97 przewiduje, że niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych

188 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 5

189 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit., str. 7

190 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający,* op. cit., str. 788

191 M. Czaplińska, *IOD dla grupy przedsiębiorstw, komentarz praktyczny*, op. cit.

operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe. Należy zauważyć, że określony w RODO poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Dla przykładu, w przypadku wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnych kategorii, IOD może potrzebować wyższego poziomu wiedzy i wsparcia. Ponadto inaczej sytuacja przedstawiać się będzie w przypadku podmiotów regularnie przekazujących dane do państw trzecich niż w przypadku, gdy przekazywanie takie ma charakter okazjonalny. W związku z tym wybór IOD powinien być dokonany z zachowaniem należytej staranności i brać pod uwagę charakter przetwarzania danych w ramach podmiotu [192]. Osoba zatrudniona na stanowisku IOD powinna na bieżąco zapewniać i doradzać najwyższemu kierownictwu w podejmowaniu decyzji (cechować się znajomością specyfiki branży, w której funkcjonuje administrator danych/podmiot przetwarzający, np. jednostki oświatowe, służba zdrowia, itp.) i prowadzić systematyczny monitoring przestrzegania przepisów ODO (zarówno przepisów prawa krajowego, jak i europejskiego), m.in. w obszarach takich, jak zamówienia publiczne, proces zatrudnienia, właściwe stosowanie monitoringu wizyjnego, nadzorowanie procesów udostępniania i powierzania danych osobowych. Nie sposób przy tym nie zauważyć, że wiedza wymagana od osoby zajmującej się ochroną danych w placówkach medycznych będzie tożsama z wiedzą osoby pełniącą funkcję IOD w innych branżach, jak placówki oświatowe, czy podmioty publiczne. Dobry IOD powinien oprzeć swoje działania na rzetelnym audycie zerowym w organizacji i prześledzeniu wszystkich procesów związanych z przetwarzaniem danych osobowych. Taki audyt zerowy pozwoli inspektorowi zorientować się nie tylko w organizacji i przebiegu procesów przetwarzania, poznać personel administratora, ale również ocenić poziom systemu ochrony prywatności i przygotować plan działań na kolejne miesiące [193]. Należy zauważyć brak u dotychczasowych ABI i obecnych IOD kompetencji do prowadzenia audytów w oparciu o metodykę ISO/IEC 27001 zarówno w obszarze bezpieczeństwa zasobów ludzkich, zgodności z regulacjami prawnymi, organizacji bezpieczeństwa informacji, a także zadań związanych z identyfikacją, przeglądem zagrożeń i naruszeń danych osobowych i w obszarze bezpieczeństwa teleinformatycznego (wymagana znajomość systemów informatycznych oraz

192 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 12, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

193 M. Gruszczyński, T. Wącirz, *Cechy dobrego inspektora ochrony danych,* op. cit., str. 51

ich zabezpieczeń). Inspektor ochrony danych realizuje zadania z pogranicza prawa oraz technologii teleinformatycznych. Sama znajomość przepisów nie wystarczy, by IOD pełnił swoją funkcję w sposób prawidłowy, zwłaszcza że technologia i zagrożenia związane z cyberbezpieczeństwem rozwijają się tak dynamicznie, że prawo i wytyczne za tym nie nadążają (chociażby ze względu na długi proces legislacyjny). Inspektor powinien śledzić rozwiązania technologiczne oraz dobre praktyki w zakresie bezpieczeństwa infrastruktury teleinformatycznej, zwłaszcza w obszarach dotyczących aktualizacji oprogramowania, metod autoryzacji i uwierzytelniania, stosowania silnych haseł, identyfikacji użytkowników, czy analizy anomalii i incydentów. Inspektor powinien mieć świadomość tego, jakie są metody działania cyberprzestępców i sposoby przeprowadzania tego typu ataków oraz w jakie obszary organizacji najczęściej są wymierzane. W omawianym obszarze IOD powinien zwrócić uwagę np. na: zasady szyfrowania i ochronę przed ransomware, oraz ataki i zagrożenia IT. W obszarach technologicznych, w zakresie przedmiotu, IOD powinien mieć przynajmniej podstawową wiedzę i świadomość dotyczącą technicznych środków, takich jak:

1) narzędzia zabezpieczeń stacji roboczych i przechowywania haseł,
2) rozwiązania polegające na mikrosegmentacji i segmentacji,
3) narzędzia służące zarządzaniu aktualizacjami i poprawkami,
4) narzędzia szyfrowania danych,
5) rozwiązania zapewniające backup – sprzętowe i programowe,
6) rozwiązania służące wspieraniu analizy incydentów,
7) narzędzia służące analizie szkodliwego oprogramowania[194]. Podsumowując należy stwierdzić, że choć artykuł 37 ust. 5 nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę wyznaczając IOD, to jednak istotne jest, by inspektor posiadał odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość RODO. Istotne jest także, aby przy dokonywaniu wyboru wziąć pod uwagę konieczność unikania konfliktu interesu oraz zweryfikować faktycznie posiadaną wiedzę potencjalnego kandydata. Wskazane jest przeprowadzenie testu wiedzy, uwzględniającego przepisy szczególne, istotne dla administratora [195]. Jednakże sam test wiedzy w tym wypadku nie zweryfikuje kompetencji i umiejętności IOD, co do rzetelnego i fachowego wypełniania przez niego zadań. Należy wziąć

194 M. Gruszczyński, T. Wącirz, *Cechy dobrego inspektora ochrony danych, op. cit.*, str. 54

195 S. Czub-Kiełczewska, *Okiem IOD-a: status i zadania IOD-a - dobre praktyki,* op. cit.

pod uwagę przede wszystkim znajomość specyfiki branży i zbadać umiejętność wydawania zaleceń oraz przeprowadzania zadań audytowych, czy analizy ryzyka.

Do pełnienia funkcji IOD przydatne są w szczególności następujące kompetencje:

1) umiejętności z zakresu prowadzenia audytu wewnętrznego,

2) wiedza z zakresu szacowania ryzyka,

3) wiedza dotycząca funkcjonowania systemu informatycznego,

4) umiejętności związane z opracowywaniem dokumentacji dotyczącej ochrony danych,

5) umiejętności związane z prowadzeniem szkoleń [196]. Dlatego umiejętność obrony własnej opinii, prawidłowego argumentowania i prezentowania problematyki ochrony danych może być niezwykle istotnym elementem w pracy IOD. Trzeba pamiętać, że IOD jest również osobą, która zajmuje się podnoszeniem wiedzy pracowników administratora. To on powinien prowadzić regularne szkolenia wewnątrz organizacji[197]. Propagowanie odpowiednich i regularnych szkoleń dla inspektorów ochrony danych przez organy nadzorcze również może być przydatne. Nie należy jednak zgodzić się ze stanowiskiem, iż do potwierdzenia wiedzy z ochrony danych mogą być przydatne różnego rodzaju dyplomy, zaświadczenia czy certyfikaty ukończenia specjalistycznych szkoleń, warsztatów, kursów czy studiów w zakresie przetwarzania danych zgodnie z RODO czy wykonywania zadań IOD [198]. Potwierdza to stanowisko Prezesa UODO wskazujące, iż wymagany od inspektora poziom wiedzy fachowej nie jest jednoznacznie określony, ale zgodnie z wytycznymi dotyczącymi IOD musi być on współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Należy również dodać, iż zarówno większość programów studiów podyplomowych na uczelniach wyższych, jak również szkoleń specjalistycznych proponowanych na rynku skupia się w większości na zagadnieniach dotyczących przepisów z zakresu ochrony danych osobowych i prawnego otoczenia funkcjonowania IOD, co nie pozwala na nabycie faktycznej wiedzy i umiejętności do rzetelnego i fachowego wykonywania zadań na tym stanowisku. Zagadnienia, o których mowa powyżej powinny stanowić jedynie 30% wymaganych zagadnień programowych. Wśród pozostałych zagadnień należy wymienić m.in. planowanie i realizacji kontroli, sprawdzeń i audytów w zakresie związanym z zabezpieczeniem informacji oraz infrastruktury informatycznej, projektowanie i kontrolę obszaru bezpieczeństwa fizycznego i środowiskowego. Nie sposób nie wspomnieć również

196 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 5

197 M. Gruszczyński, T. Wącirz, *Cechy dobrego inspektora ochrony op. cit.*, str. 53

198 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 5

o zagadnieniach związanych z zarządzaniem ryzykiem w obrębie ochrony danych osobowych, czy o systemowym podejście do zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy ISO/IEC 27001:2013, itp. Powyższe wynika z braku dostatecznej ilości osób fachowo zajmujących się przedmiotową tematyką. IOD powinien również posiadać odpowiednią wiedzę na temat operacji przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych. W przypadku organów i podmiotów publicznych IOD powinien również posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki. Priorytetem IOD powinno być zapewnienie przestrzegania rozporządzenia. IOD odgrywa kluczową rolę w zakresie wspierania "kultury ochrony danych" w ramach podmiotu oraz pomaga w implementacji niezbędnych elementów RODO, w tym zasad przetwarzania danych osobowych, praw osób, których dane dotyczą, ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania, wymogów bezpieczeństwa przetwarzania i zgłoszenia naruszeń [199]. Punktem wyjścia dla każdego IOD może być prawidłowo opracowany rejestr czynności przetwarzania. Prawidłowe opracowanie takiego rejestru pozwoli IOD na dogłębne poznanie procesów, w jakich przetwarzane są dane osobowe w organizacji. Wychodząc od przesłanki legalności przetwarzanych danych, należałoby zająć się podstawami prawnymi w tych właśnie procesach. W wielu przypadkach to właśnie tam pojawi się katalog przepisów, które będą podstawami prawnymi przetwarzania i o które, poza RODO, inspektor powinien uzupełnić swoją wiedzę. Dobry IOD w toku wykonywania swoich obowiązków powinien umieć zweryfikować, czy przepisy dają administratorowi danych osobowych przesłankę legalności przetwarzania danych osobowych w realizowanym procesie. Należy zauważyć, że akty prawne, na podstawie których administrator ma przesłankę legalności przetwarzania, będą definiować również kwestie związane z retencją danych. Poza rejestrem czynności przetwarzania jednym z narzędzi rekomendowanych inspektorom jest dokument tabeli ról. Określa on:

1) właścicieli procesów w organizacji,
2) osoby informowane,
3) osoby konsultowane,
4) poziomy uprawnień i dostępu do informacji zgodnie z zasadą minimalnej wiedzy koniecznej (*need to know). Inspektor* będzie w stanie sprawnie funkcjonować w organizacji oraz wypełniać

199 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 13, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

swoje obowiązki, jeśli pozna strukturę organizacyjną i procesy zachodzące w środowisku administratora [200].

Wymóg uaktualniania wiedzy i zapewnienia na to środków finansowych jest zupełnie uzasadniony, biorąc pod uwagę wyzwania związane z szybkim postępem technologicznym, globalizacją, rosnącą w dużym tempie skalą zbierania i wymiany danych. Jednym słowem – fachowa wiedza, przekładająca się na konkretne umiejętności praktyczne, jest nie tylko kryterium wyboru danej osoby do pełnienia funkcji inspektora ochrony danych, ale tak naprawdę fundamentem, na którym zbudować można w danej organizacji cały system skutecznej ochrony danych osobowych [201]. Ponadto należy pamiętać, iż zgodnie z art. 53 UODO Prezes Urzędu udostępnia w BIP:

1)standardowe klauzule umowne, o których mowa w art. 28 ust. 8 RODO,

2)zatwierdzone kodeksy postępowania,

3)przyjęte standardowe klauzule ochrony danych (wg art. 46 ust 2 lit. d),

4)rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Jednakże wskazany przepis jak na razie jest traktowany trochę po macoszemu, jednakże IOD powinien na bieżąco śledzić wytyczne zarówno polskiego, jak i europejskiego organu nadzorczego.

Najistotniejsze w pełnieniu funkcji IOD jest nie tylko posiadanie odpowiednich kwalifikacji zawodowych zgodnie z art. 37 ust. 5 RODO, lecz również odpowiednia postawa osoby pełniącej tę funkcję. Chodzi o postawę etyczną tej osoby, która daje gwarancję, że prawo do prywatności osób, których dane są przetwarzane, będzie przestrzegane. Osoba taka powinna chronić prywatność osób nie tylko w pracy, ale również na co dzień. Nie możemy zapominać, że prawo do prywatności to jedno z podstawowych praw każdego człowieka – zawarte również w art. 12 Powszechnej Deklaracji Praw Człowieka [202].

W państwach członkowskich, które obecnie regulują kryteria powołania inspektora, mogą być one ukształtowane różnorodnie. Tym samym wymogi na stanowisku IOD powinny zostać szczegółowo uregulowane w ustawodawstwie krajowym, podobnie, jak to ma miejsce w innych krajach członkowskich. Dla przykładu w myśl § 4f ust. 2 BDSG [203] IOD może być tylko taka osoba, która posiada specjalistyczną wiedzę i daje rękojmię właściwego

200 M. Gruszczyński, T. Wącirz, *Cechy dobrego inspektora ochrony danych, op. cit.*, str. 51-53

201 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 789

202 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 3

203 Bundesdatenschutzgesetz, zwana dalej BDSG – niemiecka ustawa o ochronie danych osobowych

wykonywania swoich obowiązków. Wymagany poziom wiedzy specjalistycznej ustala się w szczególności w zależności od zakresu przetwarzania danych przez administratora i związanych z tym wymogów ich ochrony. Ze względu na wątpliwości w praktyce działalności administratorów z sektora prywatnego niemieckie organy ochrony danych osobowych zrzeszone w tzw. Kręgu Düsseldorfskim przyjęły w 2010 r. rezolucję, w której wyjaśniono w szczególności rozumienie kryteriów fachowości, które musi spełniać inspektor ochrony danych. W konsekwencji inspektor powinien mieć podstawową wiedzę o przepisach o ochronie danych osobowych, w tym wiedzę dotyczącą zarówno regulacji na poziomie konstytucyjnym, jak i na poziomie federalnego ustawodawstwa o ochronie danych osobowych. Wiedza ta musi również obejmować organizacyjne i techniczne środki zabezpieczenia. Ponadto inspektor ochrony danych w zależności od wielkości administratora oraz sektora, w którym ten administrator działa, a także charakteru przetwarzanych danych i wdrożonych środków technicznych ich przetwarzania powinien mieć również pełną wiedzę o mających zastosowanie przepisach sektorowych. Jednocześnie od inspektora ochrony danych wymaga się także wiedzy o technologiach informacyjno-komunikacyjnych oraz różnych kwestiach dotyczących bezpieczeństwa danych. Inspektor ochrony danych powinien mieć również podstawową wiedzę o działalności administratora w odniesieniu do zarządzania zasobami ludzkimi, księgowością, sprzedażą czy marketingiem, a zarazem powinien znać strukturę organizacyjną administratora. Jednocześnie powinien mieć praktyczną wiedzę o wdrażaniu mechanizmów zarządzania ochroną danych osobowych (m.in. chodzi o przeprowadzanie audytów, ocenę ryzyka, czy współpracę z radami zakładowymi, które w niemieckim systemie ochrony danych osobowych również odgrywają pewną rolę w dziedzinie ochrony danych osobowych). Należy dodać, że w świetle omawianej rezolucji niezbędną wiedzę i umiejętności IOD co do zasady powinien posiadać już przed powołaniem na to stanowisko [204].

Z kolei we Francji, aby zostać IOD, trzeba przejść trzydziestopięciogodzinne szkolenie zakończone egzaminem, które uprawnia do tego, by zostać inspektorem podstawowego szczebla na trzy lata. Jeśli chcesz być inspektorem o szczebel wyżej, to musisz przejść kurs państwowy, który trwa już 90 godzin. Przy czym we Francji, tak jak u nas, inspektorem może być człowiek z ulicy. Tyle że administrator we Francji ma wiedzę i wskazówkę, że jeśli ktoś przeszedł taki, nazwijmy to, państwowy kurs i uzyskał uprawnienia to ma odpowiednie przygotowanie [205]. Pomimo, iż rozwiązania przyjęte we Francji stanowią istotny krok naprzód

204 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający,* op. cit., str. 788

205 https://prawo.gazetaprawna.pl/artykuly/1445350,jaroslaw-felinski-nie-kazdy-powinien-byc-inspektorem-

w celu zdobycia przez IOD odpowiednich kwalifikacji zawodowych to nie sposób nie zgodzić się ze wskazanym wyżej stanowiskiem, które nie potwierdza posiadania przez IOD odpowiedniego doświadczenia zawodowego. Francuska Komisja ds. Wolności oraz Informatyki (CNIL) wydała pierwsze zezwolenie 12 lipca 2019 r. spółce Afnor na okres 5 lat zgodnie z ramami akredytacji dotyczącymi certyfikacji umiejętności inspektora ochrony danych (IOD) przyjętymi we wrześniu 2018 r. Zgodnie ze wskazaną ustawą uprawniony do tego CNIL przyjął 20 września 2018 r. dwa standardy certyfikacji umiejętności IOD:
- system odniesienia do certyfikacji, który określa w szczególności warunki dopuszczalności wniosków oraz listę 17 umiejętności i know-how, które mają zostać certyfikowane,
- wzorzec akredytacji, który określa kryteria mające zastosowanie do jednostek, które chcą uzyskać upoważnienie CNIL do poświadczania umiejętności inspektora ochrony danych na podstawie wzorca certyfikacji opracowanego przez CNIL. Jest to dobrowolny mechanizm, który pozwala każdemu specjaliście udowodnić, że spełnia wymogi dotyczące umiejętności i wiedzy DPO określone w rozporządzeniu. Będąc kluczowym graczem w zakresie przestrzegania RODO, IOD musi w szczególności posiadać specjalistyczną wiedzę na temat przepisów i praktyk dotyczących ochrony danych. Certyfikat jest wektorem zaufania zarówno dla organizacji korzystającej z tych certyfikowanych osób, jak i dla jej użytkowników, klientów, dostawców, agentów czy pracowników [206].

Z informacji znajdujących się na stronach internetowych słowackiego organu nadzorczego wynika, że funkcję IOD może sprawować osoba, która zdała egzamin państwowy. Egzamin jest bezpłatny, a przerwa dłuższa niż dwa lata w wykonywaniu tej funkcji wymaga ponownego przeprowadzenia egzaminu [207].

Hiszpański organ ochrony danych wskazuje, że IOD, aby mógł realizować swoje funkcje, musi mieć odpowiednią wiedzę i umiejętności, aby:
a)zbierać informacje w celu zidentyfikowania czynności przetwarzania,
b)analizować i sprawdzać zgodność działań związanych z przetwarzaniem,
c)informować, doradzać i wydawać zalecenia administratorowi lub przetwarzającemu,
d)zbierać informacje w celu nadzorowania rejestru czynności przetwarzania,
e)zapewniać doradztwo w zakresie stosowania zasady *privacy by design* i *privacy by default,*

ochrony-danych.html, dostęp z dnia 19.11.2020 r.

206 https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-delivre-son-premier-agrement, dostęp z dnia 19.11.2020 r.

207 https://dataprotection.gov.sk/uoou/sk/content/zodpovedna-osoba-ss-23-nasl , dostęp z dnia 19.11.2020 r.

f)doradzać:

– czy należy przeprowadzić ocenę skutków dla ochrony danych czy też nie,
– jaka metodologia powinna być stosowana przy przeprowadzaniu oceny skutków dla ochrony danych,
– czy ocena skutków dla ochrony danych powinna być przeprowadzana wewnętrznie czy zlecona na zewnątrz,
– jakie zabezpieczenia (w tym środki techniczne i organizacyjne) należy zastosować w celu minimalizacji ryzyka dla praw i interesów osób, których dane dotyczą,
– czy ocena skutków została przeprowadzona prawidłowo,

g)priorytetyzować swoją działalność i koncentrować wysiłki na kwestiach, które wiążą się z większym ryzykiem dla ochrony danych,

h)doradzać administratorowi danych:

– jaką metodologię należy zastosować w odniesieniu do oceny skutków dla ochrony danych,
– które obszary powinny podlegać wewnętrznemu lub zewnętrznemu audytowi ochrony danych,
– w zakresie prowadzenia wewnętrznych szkoleń [208].

Na stronie Hiszpańskiego organu ochrony danych pojawiły się kryteria pozwalające na możliwość uzyskania certyfikacji IOD, które będą przyznawane przez podmioty certyfikujące należycie akredytowane przez ENAC [209]. Certyfikacja nie jest obowiązkowa, a program jest systemem certyfikacji, który umożliwia zaświadczenie, że IOD posiadają kwalifikacje zawodowe i wiedzę wymagane do wykonywania zawodu. Jedynymi podmiotami, które mogą certyfikować IOD to te, które zostały akredytowane przez ENAC zgodnie z normą UNE-EN ISO / IEC 17024: 2012 oraz systemem certyfikacji delegatów ds. ochrony danych. Podmioty zainteresowane uzyskaniem akredytacji do certyfikacji DPD powinny skontaktować się z ENAC i poprosić o informacje o tym, jak rozpocząć proces akredytacji [210].

Mając na uwadze praktykę i rozwiązania przyjęte w poszczególnych krajach członkowskich oraz brak szczegółowych wymogów i regulacji dotyczących zawodu IOD w polskim porządku prawnym, jak również mechanizmów weryfikujących umiejętności kandydatów na to stanowisko zasadnym wydaje się ich unormowanie na gruncie przepisów

208 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym, op. cit.*, str. 243

209 Entidad Nacional de Acreditación – stowarzyszenie koordynujące i zarządzające systemem ewaluacji zgodnie z kryteriami ustalonymi przez UE.

210https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion , dostęp z dnia 19.11.2020 r.

krajowych. Zasadnym rozwiązaniem wydaje się wprowadzenie obowiązku ukończenia studiów podyplomowych z zakresu bezpieczeństwa informacji i ochrony danych osobowych kończących się egzaminem zawodowym oraz obowiązek odbycia co najmniej dwuletniej praktyki pod nadzorem doświadczonego IOD. Program studiów, jak wspomniano wcześniej powinien być oparty nie tylko na zagadnieniach dotyczących przepisów z zakresu ochrony danych osobowych i prawnego otoczenia funkcjonowania IOD, ale również w zakresie planowania i realizacji kontroli, sprawdzeń i audytów w zakresie związanym z zabezpieczeniem informacji oraz infrastruktury informatycznej, projektowania i kontroli obszaru bezpieczeństwa fizycznego i środowiskowego. Kluczowe będą również zagadnienia związane z zarządzaniem ryzykiem w obrębie ochrony danych osobowych, czy systemowe podejście do zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy ISO/IEC 27001:2013. Zamiast obowiązku ukończenia studiów podyplomowych należy również dopuścić możliwość uzyskania certyfikacji IOD, które będą przyznawane przez podmioty certyfikujące akredytowane przez Prezesa UODO. Odbycie dwuletniej praktyki powinno być odpowiednio udokumentowane i określone w ustawie poprzez potwierdzenie przez kierownika jednostki wykonywania czynności, o których mowa w art. 39 ust. 1 i 2 RODO pod nadzorem IOD, podobnie jak to ma miejsce w przypadku audytorów wewnętrznych określonych w art. 286 u.o.f.p. [211]. Nieodzownym elementem kwalifikującym

211 Art. 286. [Wymagania kwalifikacyjne na audytora wewnętrznego]

1. Audytorem wewnętrznym może być osoba, która:

1) ma obywatelstwo państwa członkowskiego Unii Europejskiej lub innego państwa, którego obywatelom, na podstawie umów międzynarodowych lub przepisów prawa wspólnotowego, przysługuje prawo podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej;

2) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;

3) nie była karana za umyślne przestępstwo lub umyślne przestępstwo skarbowe;

4) posiada wyższe wykształcenie;

5) posiada następujące kwalifikacje do przeprowadzania audytu wewnętrznego:

a) jeden z certyfikatów: Certified Internal Auditor (CIA), Certified Government Auditing Professional (CGAP), Certified Information Systems Auditor (CISA), Association of Chartered Certified Accountants (ACCA), Certified Fraud Examiner (CFE), Certification in Control Self Assessment (CCSA), Certified Financial Services Auditor (CFSA) lub Chartered Financial Analyst (CFA), lub

b) złożyła, w latach 2003-2006, z wynikiem pozytywnym egzamin na audytora wewnętrznego przed Komisją Egzaminacyjną powołaną przez Ministra Finansów, lub

c) uprawnienia biegłego rewidenta, lub

d) dwuletnią praktykę w zakresie audytu wewnętrznego i legitymuje się dyplomem ukończenia studiów podyplomowych w zakresie audytu wewnętrznego, wydanym przez jednostkę organizacyjną, która w dniu

do wykonywania funkcji IOD są również: rzetelne podejście i wysoki poziom etyki zawodowej [212].

II. 4. Niezależność IOD w instytucji a rola ADO.

W porównaniu z dotychczas obowiązującymi przepisami RODO wprowadza daleko idące organizacyjne, finansowe i funkcjonalne gwarancje niezależności IOD i zdecydowanie umacnia jego pozycję [213].

Obowiązkiem kierownika jednostki jest zapewnienie IOD nie tylko odpowiedniego wsparcia w wypełnianiu zadań. Ma on także zapewnić mu warunki niezbędne do niezależnego i skutecznego ich wykonywania, do których należą:

- bezpośrednia podległość kierownikowi jednostki,
- udział we wszystkich sprawach związanych z ochroną danych osobowych,
- nieotrzymywanie instrukcji dotyczących wykonywania zadań,
- brak możliwości odwołania lub ukarania za wypełnianie przez IOD jego zadań,
- nieotrzymywanie innych zadań i obowiązków, które mogłyby powodować konflikt interesów [214].

Obowiązki te należy rozumieć szeroko – chodzi o wszystkie sprawy, które mogą mieć wpływ na przetwarzanie danych osobowych, a więc IOD powinien być włączany na przykład

---

wydania dyplomu była uprawniona, zgodnie z odrębnymi ustawami, do nadawania stopnia naukowego doktora nauk ekonomicznych lub prawnych.

2. Za praktykę w zakresie audytu wewnętrznego, o której mowa w ust. 1 pkt 5 lit. d, uważa się udokumentowane przez kierownika jednostki wykonywanie czynności, w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;

2) realizacją czynności w zakresie audytu gospodarowania środkami pochodzącymi z budżetu Unii Europejskiej oraz niepodlegającymi zwrotowi środkami z pomocy udzielanej przez państwa członkowskie Europejskiego Porozumienia o Wolnym Handlu (EFTA), o którym mowa w ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2018 r. poz. 508, z późn. zm.);

3) nadzorowaniem lub wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2019 r. poz. 489)

212 Poradnik Prezesa Urzędu Ochrony Danych Osobowych, https://sip.lex.pl/#/publication/151350208/prezes-urzedu-ochrony-danych-osobowych-wyznaczenie-i-status-iod-wytyczne-puodo?cm=SREST.

213 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

214 Zasady współpracy audytora wewnętrznego i IOD określone przez Ministerstwo Finansów i Prezesa UODO, https://uodo.gov.pl/pl/138/445 dostęp z dnia 4.04.2019 r.

w organizację nowej akcji promocyjnej firmy, programu lojalnościowego czy w reorganizację instytucji, ponieważ mogą one mieć wpływ na sposób przetwarzania danych osobowych pracowników [215].

W praktyce najczęściej spotykanym rozwiązaniem jest powierzanie funkcji IOD osobom zatrudnionym na innych stanowiskach. Nie ma tu reguły – wyznaczani IOD są zatrudniani na różnych stanowiskach. Dobrze jest, aby osoba wyznaczona do pełnienia funkcji IOD wykonywała zadania zbieżne z ochroną danych osobowych, np. związane z bezpieczeństwem innych rodzajów informacji, czy z audytem wewnętrznym. Kluczową kwestią jest zapewnienie niezależności w wykonywaniu zadań IOD, dlatego tak istotne jest to, aby inne zadania, które wykonuje inspektor, nie kolidowały z wykonywaniem zadań IOD określonych w RODO. W takiej sytuacji istotna jest też podległość służbowa. Jeżeli przełożony osoby wyznaczonej do pełnienia funkcji IOD nie będzie zapewniać możliwości wykonywania przez nią zadań, to takie wyznaczenie będzie w tym wypadku fikcją [216]. Podobnie będzie w sytuacji, gdy bezpośredni przełożony pracownika będącego IOD, np. kierownik kadr będzie naciskał na zrealizowanie wprowadzonych przez IOD zaleceń.

Inspektor ochrony danych powinien być również osobą usytuowaną poza strukturą działu compliance. Z pewnością nie powinien łączyć swojej funkcji z zadaniami oficera compliance. O ile bowiem w zakresie funkcji prewencyjnej systemu compliance, której zadaniem będzie zapewnienie zgodności działań struktury z przepisami o ochronie danych osobowych, interesy inspektora ochrony danych oraz działu compliance będą zbieżne, o tyle w zakresie funkcji śledczej systemu compliance tak już nie będzie. Dział compliance może być zainteresowany zastosowaniem mechanizmów, które z punktu widzenia inspektora ochrony danych będą mogły stanowić naruszenie zasad przetwarzania danych z uwagi przykładowo na zbyt dużą ingerencję w prawo do prywatności. Dlatego funkcja inspektora ochrony danych powinna znajdować się organizacyjnie poza systemem compliance i być od niego niezależna [217].

Istotną nieprawidłowością z punktu widzenia funkcjonowania IOD w administracji publicznej jest wyznaczanie na tym stanowisku z jednej strony osób zajmujących samodzielne

215 A. Mednis, *Odpowiedzialność Inspektora Ochrony Danych,* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019, str.143

216 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 4

217 D. Lubasz, W. Chomiczewski, C*ompliance w zakresie ochrony danych osobowych*, [w:] B. Jagura (red.), B. Makowicz (red.), Systemy zarządzania zgodnością. Compliance w praktyce, WKP 2020, dostęp z dnia 4.06.2021 r.

lub kierownicze stanowiska, których zadania i obowiązki mogą powodować konflikt interesów. Z drugiej strony występuje sytuacja, gdzie bezpośrednia podległość IOD najwyższemu kierownictwu administratora lub podmiotu przetwarzającego jest pozorna, co uniemożliwia mu właściwe funkcjonowanie i realizację zadań. Przykładem takich nieprawidłowości jest wyznaczanie na stanowisku IOD osób, które w strukturze organizacyjnej jednostki zajmują równocześnie stanowisko, gdzie bezpośrednim przełożonym takiego pracownika jest naczelnik lub dyrektor departamentu podległy jednocześnie temu samemu Administratorowi, już nie mówiąc o wykonywaniu przez IOD zadań biorących udział w określaniu celów i sposobów przetwarzania danych. Powyższe nieprawidłowości potwierdzają wyniki badania ankietowego, gdzie jak wskazano w poprzednim rozdziale w 8 z 13 badanych jednostek ABI, a obecnie IOD wykonuje czynności na innych stanowiskach. Należy tu wymienić stanowiska samodzielne bezpośrednio podległe Kierownikowi jednostki takie, jak Kierownik Referatu/Wydziału oraz Główny Specjalista i stanowiska niższe, jak archiwista zakładowy, podinspektor, czy stanowisko ds. elektronicznych technik pracy i zintegrowanego systemu zarządzania. Tylko w 4 jednostkach zatrudnienie na stanowisku IOD nie powoduje konfliktu interesów, gdzie w 2 spośród wymienionych stanowisk podlegają bezpośrednio Kierownikowi jednostki. IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych, co ww. przypadki potwierdzają. Zdaniem jednostek badanych w żadnym z tych przypadków nie istnieje konflikt interesów, co budzi poważne wątpliwości w zakresie braku świadomości kierowników tych jednostek. Jednym z powodów takich błędnych interpretacji może być brak odpowiednich działań legislacyjnych uwzględniających stanowisko Inspektora Ochrony Danych w tabeli grup stanowisk urzędniczych, wymienionych w załączniku nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 29 stycznia 2016 r. w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej [218].

Należy wskazać, że Inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego, czy wykonywać zadania na podstawie umowy o świadczenie

218 Rozporządzenie Prezesa Rady Ministrów z dnia 29 stycznia 2016 r. w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej Dz. U. z 2018 r., poz. 807 z późn. zm.

usług, czego nie wyklucza obecna UODO. Dodatkowo RODO wskazuje administratorowi danych lub podmiotowi przetwarzającemu obowiązek wspierania IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Zapewniają oni również, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Powyższe wskazuje na pełną niezależność IOD i daje gwarancję bezstronności w wykonywaniu przez niego zadań. Ponadto RODO idzie dalej precyzując, że IOD nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego [219].

Wsparcie IOD może polegać m.in. na zapewnieniu:

1)zasobów finansowych, infrastruktury (lokali, obiektów, sprzęt) oraz personelu;

2)dostępu do zasobów, np. IT, dotyczących bezpieczeństwa itp., tak aby IOD otrzymał niezbędne wsparcie oraz informacje;

3)zespołu IOD. W takich przypadkach wewnętrzna struktura zespołu i zadania oraz odpowiedzialność każdego z jego członków powinna być jasno sprecyzowana. Podobnie jest, gdy funkcja IOD jest wykonywana przez zewnętrznego usługodawcę [220].

Należy zgodzić się ze stanowiskiem wyrażonym przez M. Byczkowskiego, iż w rzeczywistości IOD dowiaduje się więc o wielu sprawach, procesach czy projektach często w ostatniej chwili albo podczas okresowego audytu zgodności procesów przetwarzania danych z RODO. Aby zapewnić realizację tego obowiązku, potrzebna jest ciągła akcja informacyjna i szkoleniowa. Inspektor powinien realizować ją z poparciem kierownictwa administratora lub podmiotu przetwarzającego [221].

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny, co oznacza, że IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Stanowiska niekompatybilne z funkcją IOD (powodujące konflikt interesów) to m.in.: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT). Dotyczy to również niższych stanowisk, jeżeli biorą udział w określaniu celów i sposobów

219 S. Hady-Głowiak, *ABI, IOD jako wyspecjalizowany audytor ds. bezpieczeństwa informacji,* op. cit., str. 57

220 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym,* op. cit., str. 246

221 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 9

przetwarzania danych [222]. W szczególności funkcji IOD nie powinien sprawować pracownik rozliczany z wyniku finansowego, który efekt biznesowy mógłby przedkładać ponad potrzebę ochrony prywatności [223]. Ponadto, konflikt interesów może powstać, gdy zewnętrzny IOD zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych [224]. Szczególne wątpliwości co do niezależnej opinii IOD może rodzić sytuacja, gdy ta sama osoba fizyczna będzie inspektorem zarówno u administratora, jak i procesora (tj. względem tych samych kategorii danych osobowych), ponieważ IOD powinien monitorować przestrzeganie przepisów o ochronie danych także u procesora [225].

Artykuł 38 ust. 3 RODO wyznacza pewien zakres gwarancji, których celem jest umożliwianie IOD wykonywania obowiązków z odpowiednim stopniem niezależności w ramach organizacji. Administrator lub podmiot przetwarzający mają w szczególności zapewnić, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. IOD ma wprawdzie możliwość wykonywania innych zadań i obowiązków w ramach współpracy z danym podmiotem, jednak „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów" (art. 38 ust. 6 RODO) [226].

Ponadto w ramach wypełniania zadań zgodnie z art. 39 IOD nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte czy celu jaki powinien zostać osiągnięty, czy też faktu, czy należy skontaktować się z organem nadzorczym. Nie może również zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, np. określonej wykładni przepisów [227].
Rozwiązaniem zgodnym w RODO jest podleganie IOD bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (art. 38 ust. 3 zdanie ostatnie RODO). Takie rozwiązanie jest rekomendowane także przez stowarzyszenie IOD (*Network of IODs)* dla instytucji i organów UE. Wytyczne te stanowią, że jedną z najlepszych praktyk

222 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit., str. 7

223 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym, op. cit.*, str. 255

224 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 17, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

225 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym,* op. cit., str. 256

226 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit., str. 7

227 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 16, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

pomagającą zapewnić niezależność IOD jest zapewnienie, aby raportował on bezpośrednio do szefa instytucji lub organu, który powinien być odpowiedzialny za weryfikację wykonywania obowiązków przez IOD zgodnie z rozporządzeniem. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami IOD ten powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i osobom podejmującym decyzję [228].

Jednocześnie po raz kolejny należy podkreślić, że osoba pełniąca funkcję IOD, także w zakresie wykonywania zadań dodatkowych powinna podlegać bezpośrednio najwyższemu kierownictwu administratora (np. w urzędzie wojewódzkim IOD będzie bezpośrednio podlegał wojewodzie, w urzędzie gminy – wójtowi, a w szkole wyższej – rektorowi) [229]. Inspektor ma w ten sposób zapewnioną możliwość przedstawiania swoich opinii i stanowisk wobec procesów przetwarzania danych w organizacji bezpośrednio kierownictwu danej organizacji. Cała organizacja, a nie tylko IOD, powinna chronić dane osobowe, inspektor niejako „z boku" kontroluje sposób ochrony danych przez organizację. Prawodawca unijny uznał w ten sposób wagę ochrony danych osobowych, szczególnie w przypadkach wymienionych w art. 37 ust. 1 RODO, i przewidział „dodatkową parę oczu" w postaci niezależnej funkcji inspektora [230]. W odniesieniu do zakazu nakładania na inspektora dodatkowych zadań, mogących spowodować konflikt interesów, należy dodać, że wymóg ten zobowiązuje kierownictwo podmiotu publicznego w każdej konkretnej sytuacji do starannego przeanalizowania, czy jakiekolwiek inne zadania funkcje, jakimi zamierzałby obarczyć inspektora, nie utrudniłyby mu właściwego wykonywania jego określonych w art. 39 RODO obowiązków. W tym zakresie brane muszą być pod uwagę rozmaite i liczne czynniki, np. ilość czasu potrzebnego na wykonywanie poszczególnych obowiązków, stopień skomplikowania i ważności zadań, rezerwa czasowa na nieplanowane zadania, ilość i rodzaj danych osobowych oraz procesów i systemów informatycznych służących do ich przetwarzania [231]. Zatem mając na uwadze oraz gwarancje niezależności, bezstronności i bezpośredniej podległości kierownikowi jednostki oraz wsparcie i zasoby niezbędne do wykonania zadań i utrzymania fachowej wiedzy przez IOD wynikające z RODO niepokojący jest fakt, iż do Urzędu Ochrony Danych Osobowych,

228 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit., str. 7

229 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

230 A. Mednis, *Odpowiedzialność Inspektora Ochrony Danych,* op. cit., str.141

231 Prezes UODO, W tabeli grup stanowisk urzędników Służby Cywilnej konieczne jest dodanie stanowiska IOD, https://uodo.gov.pl/pl/138/923, dostęp z dnia 3 kwietnia 2019 r.

zgłaszane są częste niewłaściwe praktyki przypisywania IOD obowiązków w formie dodatkowych zadań już zatrudnionym pracownikom.

Nie można zatem wpływać w żaden sposób na IOD w celu załatwienia przez niego danej sprawy w określony sposób (np. w sprawie stanowiska inspektora w konsultacjach oceny skutków przetwarzania). Inspektor nie może zostać odwołany ani ukarany za wypełnianie swoich zadań. Zakaz nie dotyczy niewłaściwego wypełniania tych zadań ani zadań dodatkowych niedotyczących ochrony danych. Inspektor może wykonywać inne zadania i obowiązki, z zastrzeżeniem, że nie mogą one powodować konfliktu interesów [232].

W doktrynie wyrażono pogląd wykluczający wykonywanie przez IOD jakichkolwiek zadań (wymogów) wyraźnie nałożonych na administratora (lub procesora). Jak się wskazuje w doktrynie, na gruncie RODO wyłączona zatem będzie możliwość przeniesienia na IOD ciężaru podejmowania decyzji, który został nałożony wprost na administratora lub procesora. Wydaje się, iż jest to zbyt daleko idący pogląd. Natomiast wykluczyć należy możliwość nałożenia na IOD obowiązków, które mogłyby podważyć jego niezależną pozycję, w tym także poprzez włączenie go w proces decyzyjny – o celach i środkach przetwarzania danych [233].

Nieprawidłowe są również praktyki dotyczące prób pomijania stanowiska IOD w strukturze organizacyjnej podmiotu, czy oczywistego naruszenia zasady bezpośredniej podległości IOD najwyższemu kierownictwu, o których mowa powyżej. Powyższe jednoznacznie potwierdza zasadność i konieczność uwzględnienia stanowiska „inspektora ochrony danych" w tabeli grup stanowisk urzędniczych w służbie cywilnej i stanowisko Prezesa Urzędu Ochrony Danych Osobowych w tym zakresie. Sytuacja ta może niekorzystnie wpływać na poziom ochrony danych osobowych, przestrzeganie obowiązujących w tym zakresie ww. przepisów oraz prawidłowe wypełnianie przez IOD jego podstawowych zadań. Warto wskazać, że przykładem dostosowania przepisów innych aktów normatywnych do regulacji w zakresie ochrony danych osobowych jest rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 22 marca 2011 r. w sprawie stanowisk i wymaganych kwalifikacji urzędników sądowych i innych pracowników oraz szczegółowych zasad wynagradzania referendarzy sądowych, starszych referendarzy sądowych, asystentów sędziów, starszych asystentów sędziów, urzędników oraz innych pracowników wojewódzkich sądów administracyjnych [234]. W załączniku nr 1, tabela A, odnośnie stanowisk, zaszeregowań

232 A. Mednis, *Odpowiedzialność Inspektora Ochrony Danych,* op. cit., str.142

233 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym,* op. cit., str. 250

234Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 22 marca 2011 r. w sprawie stanowisk

i kwalifikacji urzędników sądowych i innych pracowników wojewódzkich sądów administracyjnych, na mocy nowelizacji z dnia 26 października 2018 r., dodano stanowisko inspektora ochrony danych (l.p. 8 w tabeli). Innym przykładem wprowadzenia stanowiska inspektora ochrony danych do wykazu stanowisk były zmienione na wniosek Prezesa UODO przepisy rozporządzenia Prezesa Rady Ministrów z dnia 15 maja 2018 r. w sprawie wynagradzania pracowników samorządowych [235]. W chwili obecnej załącznik nr 1 do tego rozporządzenia określający wykaz stanowisk obejmuje stanowisko inspektora ochrony danych. Szef Służby Cywilnej wskazany w RODO obowiązek wyznaczenia w podmiotach publicznych inspektora ochrony danych nie stanowi jednocześnie konieczności tworzenia nowych stanowisk. W opinii Szef Służby Cywilnej powołuje się m.in. na art.38 ust. 6 RODO, który stanowi, że IOD może wykonywać inne obowiązki. Obecnie obowiązujący wykaz stanowisk pozwala na dostosowanie struktury zatrudnienia do ilości obowiązków wynikających z ochrony danych osobowych. Ponadto zdaniem Szefa Służby Cywilnej obowiązek utworzenia nowych stanowisk znacząco wpłynie na wzrost zatrudnienia. Nie można się zgodzić z tak przyjętą argumentacją. Z uwagi na dużą liczbę i charakter zadań inspektorów trudno sobie wyobrazić, że w wielu przypadkach instytucji publicznych (w tym np.: ministerstwach, urzędach centralnych czy urzędach wojewódzkich zatrudniających kilkaset pracowników) nie ma możliwości powierzenia takich zadań pracownikowi zatrudnionemu na wyodrębnionym w tym celu stanowisku. Prezes UODO podkreślił również, że IOD powinien wykonywać swoje działania w sposób skuteczny i niezależny [236]. Mając powyższe na uwadze nie sposób nie wspomnieć o art. 38 RODO, który stanowi, iż administrator oraz podmiot przetwarzający zapewniają, "by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych." Określenie „właściwie” odnosić można do właściwości rzeczowej inspektora, która obejmuje wszelkie kwestie związane z przetwarzaniem i ochroną danych osobowych, natomiast sformułowanie „niezwłocznie” wskazuje, że inspektor powinien być zaangażowany w sprawy w najkrótszym możliwym czasie

---

i wymaganych kwalifikacji urzędników sądowych i innych pracowników oraz szczegółowych zasad wynagradzania referendarzy sądowych, starszych referendarzy sądowych, asystentów sędziów, starszych asystentów sędziów, urzędników oraz innych pracowników wojewódzkich sądów administracyjnych Dz. U. z 2011 r., Nr 72, poz. 384 z późn. zm.

235 Rozporządzenie Prezesa Rady Ministrów z dnia 15 maja 2018 r. w sprawie wynagradzania pracowników samorządowych Dz. U. z 2018 r., poz. 936 z późn. zm.

236 Stanowisko Prezesa UODO w sprawie tabeli grup stanowisk urzędników Służby Cywilnej, https://uodo.gov.pl/pl/138/1193, dostęp z dnia 3 kwietnia 2019 r.

[237]. W wytycznych Grupy Roboczej Art. 29 dotyczących wyznaczania IOD wprost czytamy, że w związku z tym organizacja powinna zapewnić między innymi udział IOD w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji, uczestnictwo IOD przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych. Niezbędne informacje powinny zostać udostępnione IOD odpowiednio wcześniej, umożliwiając Inspektorowi zajęcie stanowiska. Oprócz kontaktów zdalnych nieodzowne więc będą osobiste wizyty inspektora u administratora [238]. Stanowisko IOD powinno być zawsze brane pod uwagę. GR Art. 29 zaleca, w ramach dobrych praktyk, dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem IOD. I tak w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi powinien istnieć obowiązek natychmiastowej konsultacji się z IOD. W określonych przypadkach administrator lub podmiot przetwarzający powinni stworzyć wytyczne ochrony danych osobowych, które wskazywałyby przypadki wymagające konsultacji z IOD [239]. Niedopełnienie lub nienależyte wypełnienie omawianego obowiązku może przybrać postać pomijania IOD w sprawach związanych z przetwarzaniem i ochroną danych lub informowania go ze znacznym opóźnieniem, co może prowadzić do naruszeń przepisów o ochronie danych [240]. W polityce lub procedurach należy wprowadzić obowiązek zapraszania IOD na spotkania organizowane przez najwyższe kierownictwo oraz poszczególne komórki organizacyjne administratora lub podmiotu przetwarzającego, podczas których są omawiane kwestie lub podejmowane decyzje związane z przetwarzaniem danych osobowych w ramach bieżących lub projektowanych procesów realizowanych w organizacji. Powyższe rozwiązanie nie jest w mojej ocenie wystarczające. Należy rozszerzyć udział IOD do wszelkich czynności, jak udział w Komisjach (np. w Komisji przetargowej), Zespołach i innych czynnościach, gdzie mamy do czynienia z przetwarzaniem danych osobowych, jak np. brakowanie dokumentacji, czy utylizacja sprzętu. Istotne jest to, aby przy wykonywaniu tych zadań IOD wzbudzał zarówno zaufanie, jak i respekt [241].

237 P. Fajgielski, *Ogólne Rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Wolters Kluwer, Warszawa 2018, str. 431

238 P. Glen, *IOD – kosztowny obowiązek czy luksus, op. cit.*, str. 15

239 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 15, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

240 P. Fajgielski, *Ogólne Rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* op. cit., str. 431

241 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 10

Podmiot powołujący IOD powinien określić (np. w polityce ochrony danych), jakie uprawnienia będą przysługiwać IOD. Oczywiście muszą one służyć realizacji zadań IOD.
Szczegółowe kompetencje IOD mogą obejmować:
1)stały dostęp do wszystkich pomieszczeń, sprzętu, nośników i instalacji służących do przetwarzania danych osobowych;
2)możliwość żądania od pracowników i współpracowników organizacji dostępu do informacji, dokumentów, pomieszczeń, nośników danych itp.;
3)możliwość prowadzenia wewnętrznych postępowań w sprawach związanych z ochroną danych osobowych oraz wnioskowania o uzyskanie zewnętrznej opinii prawnej.
W piśmiennictwie wyrażono pogląd, iż wewnątrzorganizacyjne kompetencje IOD można porównać do uprawnień podmiotów kierujących komórką audytu wewnętrznego. Można je porównać również do osób kierujących komórką do spraw zapewnienia zgodności zgodnie z zasadami ładu korporacyjnego dla podmiotów nadzorowanych przyjętymi przez Komisję Nadzoru Finansowego [242].

Przy ocenie skutków dla ochrony danych RODO wprost wskazuje na zaangażowanie IOD i stanowi, że administrator powinien konsultować się z inspektorem przy okazji dokonywania takiej oceny. Informowanie IOD i konsultowanie się z nim w początkowych fazach wspomoże zapewnienie zgodności z RODO i uwzględniania ochrony danych w fazie projektowania. W związku z tym angażowanie IOD powinno być standardową procedurą w organizacji. Ponadto ważne jest, aby IOD był postrzegany jako partner w dyskusji i włączany w prace grup roboczych poświęconych procesom związanym z przetwarzaniem danych osobowych w ramach organizacji [243].

Dla porównania, zgodnie z BDSG niemieccy inspektorzy nie mogą otrzymywać żadnych instrukcji dotyczących wykonywanych przez nich zadań, a o swojej działalności raportują bezpośrednio do najwyższego szczebla zarządczego danego organu czy podmiotu. Co do zasady inspektorzy ochrony danych mogą wykonywać inne zadania i obowiązki. Niemniej jednak administrator lub podmiot przetwarzający zobowiązani są dopilnować, aby wszelka dodatkowa działalność inspektorów nie prowadziła do konfliktu interesów. Inspektorzy ochrony danych objęci są przy tym tzw. zatrudnieniem chronionym, tj. nie mogą zostać zwolnieni, chyba że pracodawca przedstawi fakty, które przemawiają za natychmiastowym wypowiedzeniem umowy o pracę. Dodatkowo w stosunku do

242 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym, op. cit.*, str. 255

243 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

inspektorów ochrony danych obejmujących nowe stanowiska w pełnym wymiarze w innym miejscu struktury organizacyjnej, niezwiązanym z ochroną danych osobowych, ochrona zatrudniania rozciąga się na rok po zaprzestaniu pełnienia funkcji inspektora. BDSG utrzymuje jednocześnie niemiecką zasadę zachowania przywilejów, tzn. jeśli inspektor ochrony danych przy wykonywaniu swoich zadań poweźmie informacje o jakiejkolwiek sprawie, w ramach której kierownictwo podmiotu lub inny pracownik podmiotu mógłby skorzystać z przywileju tajemnicy adwokackiej lub przedsiębiorstwa, wówczas może on również z takowego przywileju skorzystać [244].

Z punktu widzenia rozmiaru i struktury jednostki oraz zadań, w szczególności audytowych realizowanych przez IOD, a także konieczności jego zastępstwa w czasie jego usprawiedliwionej nieobecności w pracy bardzo ważnym elementem jest to, aby ADO zadbał o powołanie zespołu wspomagającego pracę IOD, w tym zastępcę IOD. Słuszne wydaje się być stwierdzenie, że ich właściwa realizacja będzie możliwa dopiero po wprowadzeniu określonych rozwiązań organizacyjnych, np. utworzeniu odrębnego zespołu bezpośrednio podlegającego IOD, którego działania będzie nadzorował [245]. W przepisach prawa lub wytycznych GR Art. 29 nie zostały wskazane żadne ograniczenia co do tego, w jakim zakresie IOD może delegować swoje kompetencje na pracowników zespołu. Nie ulega jednak wątpliwości, iż w stosunkach zewnętrznych związanych z pełnioną przez IOD funkcją, zawsze powinien on występować osobiście. Podobnie rzecz ma się z podejmowaniem decyzji, co do przeprowadzenia kontroli w kwestii zgodności z RODO przetwarzania danych osobowych oraz wyrażania opinii co do działań rekomendowanych administratorowi. Szczegółowy podział kompetencji i obowiązków powinien określać regulamin zespołu IOD lub inne wewnętrzne regulacje w danej organizacji [246].

Podsumowując należy stwierdzić, że gwarancje niezależności IOD wynikające z RODO zostały jasno i precyzyjnie określone, jednak częsta ich nadinterpretacja przez ADO oraz brak stosownych działań legislacyjnych spowodowane chęcią uzyskania nadmiernych oszczędności prowadzą do występowania licznych nieprawidłowości. Nieprawidłowości te z jednej strony są wynikiem niewłaściwych praktyk polegających na przypisywaniu IOD obowiązków w formie dodatkowych zadań już zatrudnionym pracownikom i występowania konfliktu interesów oraz brakiem udziału IOD we wszystkich sprawach związanych z ochroną danych osobowych.

244 M. Otto, *Pozycja prawna inspektora ochrony danych – zarys prawnoporównawczy,* op. cit., str. 266

245 J. Łuczak, *Inspektor ochrony danych w sektorze publicznym*, op. cit.

246 G. Bar, *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, op. cit., str. 9

Z kolei z drugiej strony oczywiste pomijanie stanowiska „inspektora ochrony danych" w tabeli grup stanowisk urzędniczych w służbie cywilnej może powodować naruszenie zasady bezpośredniej podległości IOD najwyższemu kierownictwu. Jednym z przedstawionych rozwiązań przeciwdziałania tego typu nieprawidłowościom będzie powierzenie funkcji IOD osobie, której stanowisko nie powoduje konfliktu interesów i nie pociąga za sobą możliwości określania sposobów i celów przetwarzania danych. Osoba wyznaczona do pełnienia funkcji IOD może wykonywać zadania zbieżne z ochroną danych osobowych, np. związane z bezpieczeństwem informacji. Udział IOD we wszystkich sprawach związanych z ochroną danych osobowych powinien obejmować obowiązek zapraszania IOD na spotkania organizowane przez najwyższe kierownictwo oraz poszczególne komórki organizacyjne administratora lub podmiotu przetwarzającego, podczas których są omawiane kwestie lub podejmowane decyzje związane z przetwarzaniem danych osobowych w ramach bieżących lub projektowanych procesów realizowanych w organizacji. Powinien również obejmować uczestnictwo w Komisjach, Zespołach i innych czynnościach, gdzie mamy do czynienia z przetwarzaniem danych osobowych, jak np. brakowanie dokumentacji, czy utylizacja sprzętu. Niezbędne informacje powinny zostać udostępnione IOD odpowiednio wcześniej, umożliwiając Inspektorowi zajęcie stanowiska. Na koniec należy podkreślić, że ustawodawca powinien podjąć pilne kroki legislacyjne w celu uwzględnienia stanowiska IOD w tabeli grup stanowisk urzędniczych, wymienionych w załączniku nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 29 stycznia 2016 r. w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej.

II.5. Odpowiedzialność IOD.

Inspektorem Ochrony Danych może być wyłącznie osoba fizyczna. Inspektor może być pracownikiem Administratora Danych Osobowych – dalej ADO lub podmiotu przetwarzającego, albo wykonywać zadania na podstawie umowy o świadczenie usług. Pracodawca (ADO) wytycza nam, na podstawie jakiej umowy może pełnić funkcję IOD i tak mamy wskazany stosunek pracy albo umowy cywilnoprawnej, zaś celem zatrudnienia ma być tylko i wyłącznie świadczenie usług z zakresu pełnienia funkcji IOD, ale od tej zasady może być wyjątek, a RODO dopuszcza świadczenie pracy, z innego zakresu. Artykuł 37 ust. 6 RODO wskazuje, iż Inspektor Ochrony Danych może wykonywać swoje zadania na podstawie umowy o świadczenie usług, czyli, wcale nie musi być pracownikiem organizacji, oczywiście dużą

zaletą takiego IOD jest, jeśli jest pracownikiem organizacji macierzystej, ponieważ, doświadczenie w organizacji jest nieocenionym dobrem i skarbnicą wiedzy. Trzeba również pamiętać, że IOD ma gwarancję niezależności, ma on pełnić funkcję ekspercko-doradczą oraz być punktem kontaktowym dla organu nadzorczego i osób. Jeśli organizacja zdecyduje się na skorzystanie z funkcji outsourcingu funkcji IOD to musi wiedzieć, że w praktyce działania mogą być wykonywane przez jedna osobę dedykowaną do obsługi organizacji jak i zespół, ale z zastrzeżeniem w umowie o powierzenie danych, że konkretnym "koordynatorem" IOD jest dana osoba. To na koordynatorze spoczywają działania formalno-prawne, a także odpowiedzialność prawna jak za swoje czyny podległych inspektorów realizujących bieżące działania w obsługiwanej organizacji. IOD zatrudniony w ramach stosunku pracy odpowiada za swoje działania zgodnie z zakresem czynności i wykonywaniem zadań na podstawie ustawy z dnia 26.06.1974 r. – Kodeks pracy (dalej k.p.) [247], natomiast IOD współpracujący w oparciu o umowę B2B wg ustaleń stron [248]. Należy zwrócić uwagę czy podmioty świadczące usługi IOD spełniają formalne wymogi prowadzenia działalności, czyli legitymują się odpowiednimi uprawnieniami w zakresie zgłoszenia PKD w ramach swojej działalności [249].

W art. 82 RODO – określone zostały zasady odpowiedzialności odszkodowawczej administratorów i podmiotów przetwarzających wobec osoby, która poniosła szkodę majątkową bądź niemajątkową wskutek naruszenia przepisów RODO. Zgodnie z tym przepisem każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Przepis art. 82 RODO nie zawiera pełnej regulacji zasad odpowiedzialności odszkodowawczej, dlatego też w zakresie nieuregulowanym bądź uregulowanym wybiórczo można zastosować przepisy ustawy z dnia 23.04.1964 r. – Kodeks cywilny[250] – dalej k.c. [251]

To administrator danych, a nie inspektor, ponosi odpowiedzialność za skuteczne zabezpieczenie danych osobowych. Zdarzało się, że uchwałami zarządów czy zarządzeniami organów podmiotów publicznych „przenoszono" odpowiedzialność za zapewnienie poufności

247 Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy Dz. U. z 2020 r., poz. 1320 z późn. zm.

248 A. Dawidowska, *Jaka jest odpowiedzialność inspektora ochrony danych?,* Lex /el. 2018 dostęp z dnia 3.04. 2019 r.

249 M. Kołodziej, *Podstawy prawne powołania inspektora ochrony danych, op. cit.*, str. 41

250 Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny Dz. U. z 2020 r., poz. 1740, t.j.

251 B. Kaczmarek-Templin, *Prawo do odszkodowania na drodze cywilnej za naruszenie ochrony danych zarówno w sektorze publicznym i prywatnym*, LEX/el. 2018

danych osobowych na inspektora ochrony danych. Takie działanie jest nieskuteczne i bezcelowe. Po pierwsze, przepisy wyraźnie wskazują, że to administrator decyduje o celach i sposobach przetwarzania danych, po drugie, inspektor nie ma siły sprawczej administratora danych, która pozwoliłaby mu wypełnić to zobowiązanie. W szczególności nie decyduje o sposobach realizacji budżetu (wydatki na zabezpieczenia, szkolenia, systemy informatyczne) ani o zatrudnieniu specjalistów od bezpieczeństwa informacji, osobowego, teleinformatycznego, prawnego. Inspektor jest odpowiedzialny za nadzór i przygotowywanie niezbędnych zaleceń, a nie za wdrażanie tych zaleceń. Artykuł 38 ust. 3 RODO wskazuje, że „Inspektor nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań". Wskazana treść przepisu ma podkreślić niezależność w wykonywaniu obowiązków IOD. Warto zwrócić uwagę na fakt, że powyższy przepis umożliwia jednak administratorowi odwołanie lub ukaranie inspektora, jeżeli nie wypełnia on swoich obowiązków wskazanych w RODO, ponieważ odnosi się do sposobu wypełniania obowiązków i jego niezależności, a nie zaniechania w tym zakresie[252].

IOD nie ponoszą odpowiedzialności w przypadku niezgodności z RODO. Z rozporządzenia jasno wynika, że to administrator lub podmiot przetwarzający zobowiązany jest do zapewnienia i udowodnienia zgodności przetwarzania danych osobowych z przepisami prawa (artykuł 24^1). Przetwarzanie danych zgodne z rozporządzeniem jest obowiązkiem administratora lub podmiotu przetwarzającego[253].

Kary w świetle RODO niedozwolone są tylko w przypadkach, gdy są nałożone w związku z wypełnianiem przez IOD swoich zadań. Na przykład IOD może uznać określone przetwarzanie za wysoce ryzykowne i zalecić administratorowi lub podmiotowi przetwarzającemu przeprowadzenie oceny skutków dla ochrony danych, ale administrator lub podmiot przetwarzający nie zgadza się z oceną IOD. W takiej sytuacji IOD nie może zostać odwołany ani karany za udzielenie określonego zalecenia. Kary mogą przybrać szereg form i mogą być bezpośrednie albo pośrednie. Mogą polegać na braku albo opóźnieniu awansu, utrudnieniu rozwoju zawodowego, ograniczeniu dostępu do korzyści oferowanych pozostałym pracownikom. Nieistotny jest przy tym fakt nałożenia kary, gdyż sama możliwość jej wykonania i obawa z tym związana może być wystarczająca do utrudnienia IOD wykonywania zadań. Zgodnie z normalnymi regułami, przepisami karnymi i prawa pracy, jak w przypadku

252 S. Czub-Kiełczewska, *Okiem IOD-a: status i zadania IOD-a - dobre praktyki*, op. cit.

253 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 5, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

każdego innego pracownika czy zleceniobiorcy, IOD może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków IOD (np. kradzież, nękanie fizyczne i psychiczne, molestowanie seksualne, ciężkie naruszenie obowiązków). W tym kontekście RODO nie wyjaśnia jak i kiedy IOD może zostać odwołany i zastąpiony inną osobą. Jednak im stabilniejszy kontrakt i szerszy zakres ochrony przed odwołaniem, tym większa szansa na wykonywanie zadań IOD w sposób niezależny. GR Art. 29 zaleca stosowanie takiej polityki [254]. Nie należy również zapominać o zasadach odpowiedzialności i uprawnieniach pracowników wynikających z ustaw szczególnych, bowiem zgodnie z art. 9 § 1 k.p. „ilekroć w Kodeksie pracy jest mowa o prawie pracy, rozumie się przez to przepisy Kodeksu pracy oraz przepisy innych ustaw i aktów wykonawczych, określające prawa i obowiązki pracowników i pracodawców, a także postanowienia układów zbiorowych pracy i innych opartych na ustawie porozumień zbiorowych, regulaminów i statutów określających prawa i obowiązki stron stosunku pracy."

Brak podstawy do odwołania IOD nie oznacza jednak bezwzględnego zakazu jego odwołania. Jedyne ograniczenie w tym zakresie przynosi wspomniany art. 38 ust. 3. Administrator lub podmiot przetwarzający mogą rozwiązać umowę o pracę z osobą pełniącą funkcję IOD, jeśli nie realizuje ona zadań określonych w umowie o pracę, dokumencie określającym zakres obowiązków lub czynności, do których zobowiązała się w umowie cywilnoprawnej. Pamiętać należy także, że IOD będący pracownikiem podlega przepisom prawa pracy, a więc zwolnienie go z pracy nastąpić może w przypadkach przewidzianych w Kodeksie pracy i przepisach szczególnych[255].

Jednocześnie jednak zauważa się, że im stabilniejszy kontrakt i większa ochrona przed odwołaniem, tym większa szansa na realizację zadań inspektora ochrony danych w sposób niezależny. W tym kontekście należy stwierdzić, że zdecydowanie większą stabilność zatrudnienia zapewni IOD stosunek pracy niż więź cywilnoprawna. Wiąże się to przede wszystkim z ochroną pracownika przed wypowiedzeniem lub rozwiązaniem umowy o pracę oraz ze środkami odwoławczymi przysługującymi pracownikowi z tytułu bezzasadnego lub niezgodnego z prawem wypowiedzenia lub rozwiązania niezwłocznego umowy o pracę przez pracodawcę. Tego typu gwarancji nie przewiduje k.c. [256].

254 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 17, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

255 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający,* op. cit., str. 793

256 M. Kuba, *Podstawy prawne zatrudnienia Inspektora Ochrony Danych* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019, str.135

Zgodnie z ogólnymi zasadami dotyczącymi odpowiedzialności deliktowej poszkodowany za każdym razem będzie musiał wykazać zaistnienie szkody, zawinionego działania podmiotu, którego działanie wywołało szkodę, i związku przyczynowego między działaniem a skutkiem w postaci szkody, przy czym działanie wywołujące szkody musi wynikać z naruszenia przepisów RODO (w tym także, jak wynika z motywu 146 RODO, przepisów aktów delegowanych i wykonawczych przyjętych na podstawie RODO oraz przepisów państwa członkowskiego doprecyzowujących RODO). W myśl ogólnej reguły, że „ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne" (art. 6 k.c.), wydaje się, że ciężar dowodu będzie zatem obciążał poszkodowanego. Jednak biorąc pod uwagę zasadę rozliczalności ustanowioną w art. 5 ust. 2 RODO, zgodnie z którą administrator musi być w stanie wykazać przestrzeganie zasad przetwarzania danych osobowych, ciężar w istocie zostanie przerzucony na niego (zaraz po zgłoszeniu przez podmiot danych naruszenia). Zgodnie z motywem 146 RODO: „Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego". Uwzględnienie szkody niemajątkowej, o której mowa w przepisie art. 82 RODO, z całą pewnością musi wiązać się z naruszeniem dobra osobistego. Niezależnie od ADO odpowiedzialny może być także podmiot przetwarzający dane, jednak jego odpowiedzialność jest proporcjonalna do jego uprawnień i obowiązków. Oznacza to, że będzie on ponosił odpowiedzialność wyłącznie wówczas, gdy nie dopełnił swoich obowiązków, które wynikają z RODO (np. nie wdrożył środków bezpieczeństwa lub nie zgłosił administratorowi naruszenia ochrony danych osobowych), lub gdy działał poza zgodnymi z prawem instrukcjami administratora albo wbrew tym instrukcjom [257].

Mając na uwadze odpowiedzialność IOD za skutki niewłaściwego przetwarzania danych osobowych lub za zaniedbania czy błędy w zakresie wykonywanych przez niego obowiązków, zalecane jest rozważenie objęcia go ubezpieczeniem odpowiedzialności cywilnej z tytułu wykonywanej funkcji [258]. Należy tutaj również zaznaczyć, aby podmioty świadczące usługi IOD spełniały formalne wymogi prowadzenia działalności, czyli legitymowały się odpowiednimi uprawnieniami w zakresie zgłoszenia PKD w ramach swojej działalności

257 B. Kaczmarek-Templin, *Prawo do odszkodowania na drodze cywilnej za naruszenie ochrony danych zarówno w sektorze publicznym i prywatnym*, op. cit.

258 M. Kołodziej, *Podstawy prawne powołania inspektora ochrony danych, op. cit.,* str. 42

Podsumowując należy również podkreślić, że zgodnie z art. 38 ust. 3 RODO „Inspektor nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Powyższy przepis umożliwia jednak administratorowi odwołanie lub ukaranie inspektora, jeżeli nie wypełnia on swoich obowiązków wskazanych w RODO, ponieważ odnosi się do sposobu wypełniania obowiązków i jego niezależności, a nie zaniechania w tym zakresie. IOD zatrudniony w ramach stosunku pracy odpowiada za swoje działania zgodnie z zakresem czynności i wykonywaniem zadań na podstawie k.p. i ustaw szczegółowych, natomiast IOD współpracujący w oparciu o umowę B2B wg ustaleń stron. Należy przypomnieć również o niedozwolonych klauzulach w uchwałach zarządów i zarządzeniach podmiotów publicznych polegających na próbie przenoszenia odpowiedzialności za zapewnienie poufności danych osobowych na IOD. Takie działanie jest nieskuteczne i bezcelowe.

II.6. Obsługa klienta zewnętrznego i wewnętrznego przez IOD we wszystkich sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Inspektor jest wyznaczany, aby zapewnić u administratora nadzorowanie poszanowania praw i wolności osób w związku z przepisami o ochronie danych osobowych. Poza wskazanymi powyżej obowiązkami jest on przede wszystkim punktem kontaktowym, do którego mogą one się zwracać w związku z możliwością skorzystania z przysługujących im praw. Bardzo często rolą IOD jest udzielanie osobom, których dane dotyczą, wyjaśnień w zakresie legalności przetwarzania ich danych, a także możliwości usunięcia ich danych. Prezes UODO kontaktuje się z IOD w sprawach dotyczących przetwarzania danych przez administratora. W praktyce bardzo często kieruje do IOD dodatkowe pytania dotyczące zgłoszonego przez administratora naruszenia lub skargi osób, których dane dotyczą, na odmówienie realizacji ich praw. Przyśpiesza to wyjaśnienie sprawy i ułatwia wzajemną komunikację [259]. Zgodnie z u.o.d.o., ABI nie wykonywał podobnych zadań, o czym wspomniano w poprzednim rozdziale.

Zadania dotyczące żądań osób w zakresie realizacji ich uprawnień określonych w RODO powinny zostać opisane w instrukcji postępowania w zakresie realizacji praw osób, których dane dotyczą, wdrażanej przez administratora w ramach dokumentacji polityki ochrony danych. Należy w niej ustalić, poprzez jakie kanały komunikacji będą wpływać wnioski, oraz wskazać komórkę organizacyjną odpowiedzialną za to zadanie. Oczywiście osoby mogą

259 S. Czub-Kiełczewska, *Okiem IOD-a: status i zadania IOD-a - dobre praktyki*, op. cit.

kontaktować się w tych sprawach z IOD za pomocą danych kontaktowych podanych w klauzulach informacyjnych lub zamieszczonych na stronie internetowej administratora danych. W takim wypadku IOD będzie przekierowywać zapytania do wyznaczonych osób w organizacji, określonych w specjalnej instrukcji postępowania w zakresie realizacji praw osób, informując o tym również osoby, których dane dotyczą. Do zadań IOD wynikających z instrukcji będą należały:

1) nadzorowanie i konsultowanie odpowiedzi na wnioski lub żądania wpływające od osób, w tym ocena zasadności wniosku oraz pilnowanie wymaganego czasu przesłaniają odpowiedzi do osoby,

2) przygotowanie wzorów odpowiedzi na zapytania osób w odniesieniu do realizacji poszczególnych praw przyznanych im w RODO,

3) udzielanie wytycznych co do postępowania dla poszczególnych działów, np. IT lub obsługi klienta, w zakresie wykonywania działań związanych z realizacją wniosku, np. dotyczącego usunięcia danych lub przygotowania kopii danych,

4) weryfikacja wykonanych działań dotyczących realizacji wniosków przez właściwe komórki organizacyjne,

5) prowadzenie rejestru wniosków lub nadzór nad jego prowadzeniem oraz przechowywanie dokumentacji dotyczącej wpływających wniosków i udzielanych odpowiedzi.

Przy realizacji powyższych zadań IOD może wspomagać się swoim zespołem, jeżeli taki został powołany przez administratora danych. Zadania IOD dotyczące sytuacji naruszenia ochrony danych, realizowane w związku z przesłanym zawiadomieniem zgodnie z art. 34 ust. 2 RODO powinny zostać opisane w instrukcji postępowania w sytuacji naruszenia ochrony danych, wdrażanej przez administratora w ramach dokumentacji polityki ochrony danych. Należy w niej opisać zadania IOD dotyczące zawiadamiania osób, których dotyczyło naruszenie, w tym wzór takiego zawiadomienia wraz z danymi kontaktowymi do IOD. W tym zakresie IOD będzie odpowiadać za przygotowanie zawiadomienia oraz nadzór nad jego wysłaniem oraz za dalsze kontakty z osobami, których dane dotyczą[260].

Dane kontaktowe IOD powinny zawierać dane umożliwiające osobom, których dane dotyczą, i organom nadzorczym nawiązanie kontaktu w łatwy sposób (adres korespondencyjny, telefon kontaktowy lub dedykowany adres email). Gdy to właściwe, powinny również zostać udostępnione inne środki komunikacji dla ogółu społeczeństwa, np. dedykowania infolinia, formularz kontaktowy z IOD na stronie internetowej organizacji. Wyżej wymieniony przepis

260 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str.24

nie wymaga publikowania imienia i nazwiska IOD. Podczas gdy wskazanie tych informacji może być dobrą praktyką, to decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć będzie od administratora lub podmiotu przetwarzającego i IOD [261]. Pogląd o zasadności rozszerzenia katalogu danych inspektora wskazywanych przez administratora lub podmiot przetwarzający wspiera również GR Art. 29 w Wytycznych dotyczących IOD, podnosząc, że decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych jest konieczne lub pomocne, zależeć będzie od administratora. Jednakże w ramach dobrej praktyki GR Art. 29 zaleca o informowanie o imieniu, nazwisku i danych kontaktowych IOD [262]. Z kolei zgodnie z art. 11 UODO „Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności." Mając powyższe na uwadze należy przypomnieć tutaj, iż zgodnie z zasadą pierwszeństwa prawa UE przed przepisami konstytucyjnymi państw członkowskich wynikającą z wyroku Trybunału Sprawiedliwości z dnia 17 grudnia 1970 r. 11/70, o czym mowa w punkcie II.1 niniejszego rozdziału, prawidłowym rozwiązaniem będzie usunięcie niezgodności treści art. 11 UODO z art. 37 ust. 7 RODO. Z kolei dobrą praktyką jest publikowanie dodatkowych informacji przez ADO ułatwiających kontakt z IOD.

Powiadomienie powinno następować zarówno po wyznaczeniu inspektora, jak i w przypadku zmiany osoby na tym stanowisku oraz w przypadku zmiany jej danych kontaktowych. Komentowany przepis nie wprowadza obowiązku rejestracji inspektorów ochrony danych ani prowadzenia ich jawnego rejestru przez organ ochrony danych. Ustawodawca europejski skoncentrował się na publikowaniu danych kontaktowych przez administratora i podmiot przetwarzający [263].

Przy tym należy zauważyć aktualizację przepisów UODO poprzez dodanie art. 11a pozwalającego na wyznaczenie zastępcy IOD, o czym wspomniano w I rozdziale niniejszej dysertacji. Brak możliwości powołania formalnego zastępcy nie pozwał na faktyczną realizację bieżących zadań przez osobę wspomagającą IOD. Niezwykle istotne jest, by IOD, lub jego zespół, był zaangażowany od najwcześniejszego etapu we wszystkie kwestie związane

261 Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 14, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

262 D. Lubasz, *Wyznaczenie Inspektora Ochrony Danych, op. cit.*, str. 88

263 E. Bielak-Jomaa, *Administrator i podmiot przetwarzający, op. cit.*, str. 792-793

z ochroną danych. Zatem problem ciągłości wykonywania funkcji IOD jest istotny z punktu widzenia realizacji obowiązków administratora lub podmiotu przetwarzającego zgodnie z RODO [264]. Dobrym rozwiązaniem zatem będzie powołanie zastępcy lub zastępców IOD na stałe, jako Zespołu wspierającego realizację przez IOD jego zadań ustawowych i da zapewnienie ciągłości działania w tym zakresie.

Organizacja powinna przygotować szablony potwierdzeń i różnych odpowiedzi w zależności od poszczególnych sytuacji, a nawet od płci osoby wnioskującej o wykonanie prawa do jej danych. Szablony powinny zostać przetłumaczone na wszystkie potrzebne języki, aby ułatwić centralnemu zespołowi obsługi praw osób, odpowiadanie nawet w przypadku braku znajomości danego języka. Szablony można tłumaczyć dowolnym sposobem, ale zawsze warto takie tłumaczenie zweryfikować przy pomocy personelu posługującego się danym językiem[265].

O ile w relacji zewnętrznej aktywność IOD nie zawsze będzie inicjowana przez samego IOD, bowiem to nie on jest dysponentem uprawnień nadzorczych czy praw osób, których dane dotyczą, o tyle w relacjach wewnętrznych jego działania mogą być z reguły inicjowane według zaplanowanego wraz z podmiotem, który dokonał jego wyznaczenia, schematu. Bezsporne jest zatem, że funkcja IOD generuje aktywność osoby wyznaczonej do tej roli przez administratora nie tylko w momentach, jakich wymaga tego RODO. Inspektor ochrony danych musi liczyć się z tym, że dokumentowanie jego działania ma miejsce nie tylko w sytuacji wystąpienia incydentu czy naruszenia, którego skutkiem jest dokonanie oceny, czy kierować zawiadomienie do osoby, której dane dotyczą, czy zgłaszać naruszenie organowi nadzoru. Działalność inspektora ochrony danych nie jest także wymagana tylko i wyłącznie w zakresie aktualizacji prowadzonej zgodnie z RODO dokumentacji czy w ramach współpracy przy realizacji praw osób, których dane dotyczą. Inspektor ochrony danych, będąc podmiotem uprawnionym i zobowiązanym do czuwania nad prawidłowością funkcjonowania systemu ochrony danych, musi mieć zamysł wykonywania swojej pracy w taki sposób, aby nie tylko on, ale i administrator mógł wykazać przed organem nadzoru, że nie pełni swojej roli w sposób bierny. Powyższe obliguje inspektora ochrony danych do zaplanowania sekwencji czynności podejmowanych wobec stosowania systemu ochrony danych we wszystkich obszarach związanych z wdrożeniem RODO. W sferze zainteresowania inspektora ochrony danych będą

264 M. Byczkowski, *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, op. cit., str. 7

265 P. Więckowski, *Organizacja wypełniania obowiązków dotyczących ochrony danych osobowych w grupie przedsiębiorstw* [w:] M. Kołodziej (red.), *Vademecum Inspektora Ochrony Danych*, C.H. Beck, Warszawa 2020, str. 95

musiały się zatem znaleźć działania podejmowane przez administratora w zakresie spełnienia przez niego obowiązków informacyjnych wobec osób, których dane dotyczą, lub pracowników administratora. Obszarem sprawdzeń objętym przez IOD będą na pewno relacje z podmiotami przetwarzającymi, świadczącymi usługi zewnętrzne administratorowi danych. W zależności od stanu faktycznego stosowanych systemów monitorujących działania IOD będą obejmować także kwestie oceny ryzyka w kontekście mechanizmów i potrzeb monitoringu. Dalszym zakresem aktywności winna pozostawać analiza praktyk stosowania zaprojektowanych procedur RODO w relacji z osobami fizycznymi, w tym analiza skuteczności organizacyjnego podziału zadań i sposobu komunikacji wewnątrz organizacji [266]. Należy tu podkreślić istotę działań wewnętrznych poprzez obowiązki udziału IOD we wszystkich sprawach związanych z ochroną danych osobowych, o czym wspomniano w punkcie II.5 niniejszego rozdziału. Jako dobrą praktykę wskazano jego udział IOD w spotkaniach organizowanych przez najwyższe kierownictwo oraz poszczególne komórki organizacyjne administratora lub podmiotu przetwarzającego, podczas których są omawiane kwestie lub podejmowane decyzje związane z przetwarzaniem danych osobowych w ramach bieżących lub projektowanych procesów realizowanych w organizacji. Ponadto wskazano na uczestnictwo IOD w Komisjach, Zespołach i innych czynnościach, gdzie mamy do czynienia z przetwarzaniem danych osobowych, jak np. brakowanie dokumentacji, czy utylizacja sprzętu.

Reasumując, IOD jest wysokiej klasy specjalistą, który ma za zadanie wspierać swoją wiedzą i doświadczeniem administratora danych w realizacji jego obowiązków wynikających z przepisów o ochronie danych osobowych. Jednakże jego rola jest w dużym stopniu rolą doradczą, więc bez ścisłej współpracy z administratorem oraz zaangażowania personelu jego wysiłki będą nieskuteczne[267]. Jednak nie należy zapominać o kluczowej roli IOD w procesie dotyczącym realizacji żądań osób w zakresie realizacji ich uprawnień określonych w RODO. Dobrą praktyką będzie tu wdrożenie z inicjatywy IOD instrukcji postępowania w zakresie realizacji praw osób, których dane dotyczą i kanały ułatwiające komunikację w tym zakresie z klientami zewnętrznymi, o czym mowa powyżej. Kluczową rolę IOD w tym zakresie wzmacnia nadzór nad jego prowadzeniem rejestru wniosków oraz przechowywanie dokumentacji dotyczącej wpływających wniosków i udzielanych odpowiedzi dotyczących realizacji praw osób, których dane dotyczą. Kluczowym elementem jest również wdrożenie

266 M. Czaplińska, *IOD dla grupy przedsiębiorstw, komentarz praktyczny*, op. cit.

267 S. Czub-Kiełczewska, *Okiem IOD-a: status i zadania IOD-a - dobre praktyki*, op. cit.

we współpracy z IOD instrukcji postępowania w sytuacji naruszenia ochrony danych ze wskazaniem konkretnych zadań w zakresie zawiadamiania osób, których dotyczyło naruszenie oraz współpracy z organem nadzorczym. Nieodzownym elementem takiej procedury powinien być wzór takiego zawiadomienia wraz z danymi kontaktowymi do IOD.

Rozdział III Audyt bezpieczeństwa informacji i ochrony danych osobowych, jako podstawowe zadanie IOD oceniające aktualny stan bezpieczeństwa informacji i ochrony danych osobowych w jednostce.

III.1. Pojęcie i istota oraz metody realizacji audytu w obszarze bezpieczeństwa informacji i ochrony danych osobowych

Na wstępie należy zaznaczyć, że obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji w jednostkach sektora finansów publicznych wynika z przepisów prawa, co nie zwalnia podmiotów prywatnych z konieczności jego prowadzenia w celu weryfikacji prawidłowości funkcjonowania jednostki w tym zakresie. Odpowiedzialność za zapewnienie skutecznego działania tego systemu i uprawnienia z tym związane zostały przypisane kierownikowi jednostki. Dopuszczenie do wystąpienia dysfunkcji w obszarze bezpieczeństwa informacji może spowodować w konsekwencji zniekształcenia w zachowaniu ciągłości działania i realizacji założonych celów i zadań. Mogą także pojawić się problemy w utrzymaniu reżimu dotyczącego zarządzania finansami jednostki, co negatywnie może wpłynąć na wynik finansowy, a w dalszej kolejności – na jego ocenę przez biegłego rewidenta lub przedstawicieli komisji rewizyjnej. Brak skutecznej kontroli nad bezpieczeństwem informacji oznacza także możliwość wystąpienia poważnego ryzyka związanego z utratą danych liczbowych czerpanych z elektronicznych systemów przetwarzających dane w rachunkowości. Może to być uzasadnionym problemem w procesie tworzenia stosownych analiz ekonomiczno-finansowych pomocnych w zarządzaniu jednostką. Należy pokreślić, że w każdej organizacji – niezależnie od formy prawnej – informacja stanowi podstawę do podejmowania decyzji zarządczych, przez co powinna być kompletna, dokładna, wiarygodna, elastyczna, szybko przetwarzana i ekspediowana na potrzeby kadry zarządzającej. A co najważniejsze – powinna być skutecznie chroniona zgodnie z wymaganiami stawianymi przez prawo [268].

268 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, Finanse Komunalne, 2016, nr 1-2.

Należy podkreślić kluczową kwestię, iż realizacja zadania audytowego powinna dotyczyć nie tylko ochrony danych osobowych, ale przede wszystkim wszelkich informacji prawnie chronionych. Niezwykle istotnym elementem funkcjonowania wielu podmiotów, często nawet nieuświadomionym, jest bezpieczeństwo informacji – i to nie tylko tych, które stanowią dane osobowe. Należy podkreślić, że w większości przypadków, podczas opracowywania i wdrażania systemu ochrony danych osobowych zostają uregulowane takie elementy funkcjonowania organizacji, które dotąd nie zostały wdrożone, a bezpośrednio rzutują na bezpieczeństwo wszystkich posiadanych przez podmiot informacji. Ochrona danych osobowych praktycznie zawsze bezpośrednio przekłada się na poprawę bezpieczeństwa wszystkich innych aktywów informacyjnych. Reasumując, procedury wprowadzane w ramach ochrony danych osobowych bezpośrednio wpływają na bezpieczeństwo innych informacji, których organizacja ujawniać nie chce bądź nawet nie może (np. w sytuacji, gdy stanowią one jednocześnie informacje niejawne), zatem ich wdrożenie jest ze wszech miar niezbędne i korzystne [269]. Należy tu odwołać się do § 20 ust. 1 rozporządzenia z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności (dalej KRI) [270], który precyzuje, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Analogicznie zastosowanie ma metodyka ISO/IEC 27001 [271]. W świetle wymienionego aktu prawnego kierownik jednostki jest zobowiązany zapewnić warunki umożliwiające realizację i egzekwowanie działań wymienionych w § 20 ust. 2 pkt 1–14 KRI. Katalog ten nie jest

str. 126-133, https://sip.lex.pl/#/publication/151278164, dostęp z dnia 23.08.2020 r.

269 M. Korga, *Z praktyki zespołu audytorów – jak przygotować jednostkę do zmian, które niesie za sobą Rozporządzenie unijne?* IAP nr 3/2017 r., C.H.Beck, str. 16, Legalis.pl, dostęp z dnia 28.05.2020 r.

270 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. z 2017 r. poz. 2247, t.j.

271 ISO/IEC 27001 to międzynarodowa norma opracowana dla zarządzania bezpieczeństwem informacji. Norma Norma ta określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji. Norma obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji. Wymogi określone w niniejszej Normie Międzynarodowej są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru.

zamknięty z uwagi na użycie w treści przywołanego przepisu sformułowania w „szczególności", co oznacza możliwości dopuszczenia do podejmowania także innych działań służących zapewnieniu skutecznego zarządzania bezpieczeństwem informacji. Do przykładowych działań w tym zakresie należy zaliczyć wdrożenie i aktualizację regulacji wewnętrznych w zakresie zarządzania bezpieczeństwem informacji, czy aktualizację sprzętu i oprogramowania służącego do realizacji warunków bezpiecznego przetwarzania i archiwizowania informacji, a także dbanie o respektowanie podstawowych zasad gwarantujących bezpieczną i higieniczną pracę przy przetwarzaniu informacji w środowisku informatycznym. Bardzo istotne jest przeprowadzanie co najmniej raz w roku udokumentowanej analizy ryzyka w zakresie utraty integralności, dostępności lub poufności informacji oraz zapewnienie, aby osoby zaangażowane w proces zarządzania bezpieczeństwem informacji zostały wyposażone w stosowne certyfikaty, uprawnienia po uprzednim odbyciu specjalistycznych szkoleń. Nie należy zapomnieć o zapewnieniu odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polegającego w szczególności na dbałości o aktualizację oprogramowania, zapewnieniu bezpieczeństwa plików systemowych oraz kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa. Ponadto podczas realizacji audytu w tym obszarze zadaniem audytora jest także wyrażanie niezależnej opinii o skuteczności działania systemów bezpieczeństwa informacji na podstawie rozwiązań wynikających z ustawy z dnia 6.09.2001 r. o dostępie do informacji publicznej [272], a także wymogów ustanowionych w ustawie z dnia 17.02.2005 r. [273] o informatyzacji działalności podmiotów realizujących zadania publiczne [274].

Z kolei, aby przetwarzanie odbywało się zgodnie z zasadami RODO12, administrator lub podmiot przetwarzający obowiązany jest wdrożyć „odpowiednie", a więc spełniające wymagane warunki środki techniczne i organizacyjne, polityki ochrony danych, czy też zakresy działalności. Dla uznania czy zastosowane instrumenty ochrony danych są odpowiednie, administrator i podmiot przetwarzający powinien samodzielnie to ustalić, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych, a w zakresie bezpieczeństwa przetwarzania również stan wiedzy technicznej, koszt wdrażania oraz ryzyko naruszenia praw

272 Ustawa z dnia 6.09.2001 r. o dostępie do informacji publicznej Dz. U. z 2019 r., poz. 1429 z późn. zm.

273 Ustawa z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz. U. z 2020 r., poz. 346 z późn. zm.

274 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133,

lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Na powyższe wskazuje również Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19, stwierdził, że art. 32 RODO (…) nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych. Sąd podkreślił również, że przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka [275].

Rozporządzenie właściwie wprost od administratora nie wymaga prowadzenia audytów, a w konsekwencji także nie określa ich ram, przedmiotu czy charakteru. W to miejsce RODO wymaga wykazywania zgodności z przepisami tego rozporządzenia, w tym zastosowania się administratora do wymogów zasad rozliczalności przetwarzania określonych w art. 5 RODO. Należy tu wskazać uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO, wykazywania, że środki te są poddawane przeglądom i uaktualniane. Jeżeli jednak przyjmiemy, że RODO, z jednej strony, nakładając różne obowiązki, nie określa, w jaki sposób mają być one spełnione, pozostawiając inwencję administratorowi, ale z drugiej strony wymaga od administratora – niekiedy wprost, a niekiedy pośrednio, aby wykazał, że obowiązki te zostały przez niego spełnione, to dojdziemy do konkluzji, że narzędziem wykazywania owej zgodności z RODO może być audyt wewnętrzny [276].

Należy wskazać, że jednym z (oprócz wyżej wymienionych) obowiązków w przedmiocie zarządzania bezpieczeństwem informacji jest również zapewnienie okresowego przeprowadzania audytu wewnętrznego. Co więcej, zadanie audytowe o tej tematyce ma zostać przeprowadzone nie rzadziej niż raz na rok – przedmiotowy obowiązek wynika z treści § 20

275 S. Hady – Głowiak, D. Kozłowski, *Dekalog ochrony danych osobowych- stosowanie zasad przestrzegania danych osobowych jako podstawa bezpieczeństwa przetwarzanych danych,* op. cit., str. 12-13

276 M. Czaplińska, *IOD dla grupy przedsiębiorstw, komentarz praktyczny, op. cit.*

ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności. Sformułowanie wynikające z tego przepisu prawa wzbudziło uzasadnione wątpliwości interpretacyjne środowiska zawodowego audytorów wewnętrznych zatrudnionych w jednostkach sektora finansów publicznych. Z przepisów prawa nie wynika bowiem, czy do audytu wewnętrznego o tej problematyce należy stosować przepisy rozdziału drugiego – zatytułowanego „Sposób sporządzania, elementy oraz realizacja planu audytu" – rozporządzenia Ministra Finansów z 1.02.2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego. Chodzi tu o rozwiązania metodyczne audytu wewnętrznego związane m.in. z dokonywaniem identyfikacji ryzyka oraz jego analizy. Jeżeli przyjąć, że audyt w zakresie bezpieczeństwa informacji ma być przeprowadzany nie rzadziej niż raz na rok, to nie jest jasne, czy w planie rocznym audytu wewnętrznego należy ująć to zadanie bez względu na otrzymany wynik analizy ryzyka. Dla audytora wewnętrznego przecież ten obszar niekoniecznie musi zostać uznany za obarczony bardzo poważnym ryzykiem, więc ocena potrzeb realizacji audytu bezpieczeństwa informacji może się okazać zbyt niska. Wówczas nie zachodziłaby konieczność ujęcia tego audytu w rocznym planie audytu wewnętrznego [277].

Zidentyfikowanie rodzajów przetwarzanych danych i stosowanych w związku z tym procesów pozwoli podjąć następne działania zmierzające do zaplanowania wewnętrznych zasad postępowania, opracowania dokumentacji i dobrania adekwatnych sposobów zabezpieczania danych.

W związku z tym warto dokonać przeglądu, choć RODO wprost nie nakłada takiego obowiązku, celem ustalenia jakie rodzaje danych osobowych są przetwarzane w danej placówce oraz czy dane gromadzone w zbiorach są uporządkowane, czy są rozproszone oraz czy można je skatalogować według jakiegoś wspólnego kryterium [278].

Audyt pozwala na odpowiednie zaprojektowanie systemu ochrony danych osobowych, adekwatne reagowanie na zmiany, zagrożenia, potrzeby bieżące i długofalowe, wzrost świadomości osób odpowiedzialnych za przetwarzanie danych osobowych i stosowane zabezpieczenia, uzyskiwanie informacji co do efektywności wprowadzonych rozwiązań oraz kierunków ich przeobrażeń. Audyt, w toku którego ustalone zostaną: charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych, następnie

277 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

278 J. Lesińska Joanna, *Harmonogram wdrożenia RODO – krok po kroku*, Lex/el. 2018, dostęp z dnia 28.05.2020 r.

dokonana będzie ocena zastosowanych środków technicznych i organizacyjnych dla przetwarzania zgodnie z RODO i efektywności tych środków [279].

Jednym z najważniejszych elementów zapewniania zgodności z przepisami RODO, jest stosowanie środków ochrony adekwatnych do ryzyk związanych z przetwarzaniem (art. 24 i 32 RODO) [280].

Przepisy rozporządzenia w sprawie Krajowych Ram Interoperacyjności milczą odnośnie do wskazania, jaki rodzaj audytu wewnętrznego należy zastosować do oceny systemu zarządzania bezpieczeństwem informacji. W literaturze przedmiotu dokonano podziału audytu na wiele jego rodzajów. Przy czym do podstawowych realizowanych w jednostkach sektora finansów publicznych należy zaliczyć: audyt finansowy, audyt operacyjny i audyt informatyczny [281]. Dotychczas w obrębie ochrony danych osobowych szczególną popularnością cieszył się „audyt informatyczny" rozumiany jako niezależna ocena rozwiązań informatycznych i organizacyjnych składających się na systemy informatyczne działające w organizacjach [282]. Jak podkreśla Kazimiera Winiarska, audyt informatyczny ma na celu kontrolę systemów informatycznych działających w jednostce, przez co istnieje możliwość identyfikacji ryzyka oraz ewentualnych luk w tym systemie. Natomiast według Krzysztofa Czerwińskiego obecne uzależnienie od IT jest bardzo duże i powiększa się z każdym rokiem, dlatego organizacje muszą kontrolować swoje systemy informatyczne, ponieważ koszty błędów i nieprawidłowości wynikające z braku kontroli są zwykle bardzo wysokie i pociągają negatywne skutki dla organizacji. Realizując audyt wewnętrzny w obszarze zarządzania bezpieczeństwem informacji, badaniem należy objąć w szczególności takie zagadnienia, jak misja IT oraz uzgodnione cele i zadania działań związanych z IT, czy strategia IT, plany jej wdrożenia oraz monitorowanie postępu. Nie bez znaczenia pozostają również uzgodnienia polityk użytkowania i ochrony IT oraz monitorowanie ich stosowania, samoocena systemu kontroli, raporty z kontroli dotyczące IT, czy procedury dotyczące przetwarzania danych w środowisku informatycznym.

---

279 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, [w:] M. Jagielski (red.) *Dokumentacja ochrony danych osobowych ze wzorami*], Wolters Kluwer, Warszawa 2019, str. 187

280 S. Czub-Kiełczewska, *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* Lex/el. 2019, dostęp z dnia 28.05.2020 r.

281 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

282 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, [w:] M. Jagielski (red.) *Dokumentacja ochrony danych osobowych ze wzorami*] op. cit., str. 186

Wyniki prac audytu informatycznego powinny stanowić dla kierownictwa odpowiedź na pytanie, czy jest zapewniona poprawna eksploatacja systemów w środowisku informatycznym, a także czy skutecznie odbywa się zarządzanie bezpieczeństwem informacji, zapewniając jej poufność, integralność i dostępność osobom upoważnionym. Audyt, o którym tu mowa obejmować będzie także audyt bezpieczeństwa danych osobowych definiowany na podstawie normy ISO 27000 jako systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu, choć tak określony zakres audytu nie wyczerpuje kwestii weryfikacji przetwarzania danych osobowych z punktu widzenia zgodności z RODO. Wykazywanie zgodności z RODO dotyczyć musi bowiem różnych obszarów systemu ochrony danych osobowych i różnych przepisów tego rozporządzenia [283].

Wybrane wymagania wynikające z normy PN-ISO/IEC 27001 to :

– zrozumienie organizacji i jej kontekstu – co oznacza, że organizacja powinna określić czynniki zewnętrzne i wewnętrzne istotne dla celu jej działania i takie, które wpływają na zdolność do działania w systemie zarządzania bezpieczeństwem;

– określenie zakresu systemu zarządzania bezpieczeństwem informacji – co oznacza konieczność określenia granic i możliwości zastosowania systemu bezpieczeństwa informacji, przy czym zakres powinien być dostępny w formie udokumentowanej informacji;

– planowanie działań odnoszących się do ryzyk i szans – oznacza obowiązek określenia czynników ryzyka i szans w celu zapewnienia m.in., że system zarządzania bezpieczeństwem informacji osiągnie zamierzony wynik, a także organizacja powinna opracować i wdrożyć proces szacowania ryzyka w tym obszarze;

– postępowanie z ryzykiem bezpieczeństwa informacji – zobowiązuje organizację do opracowania i wdrożenia procesu postępowania z ryzykiem bezpieczeństwa, a w szczególności sformułowania planu postępowania z tym ryzykiem;

– komunikacja – co oznacza konieczność określenia potrzeb w zakresie komunikacji wewnętrznej i zewnętrznej dotyczącej systemu zarządzania bezpieczeństwem informacji;

– działania operacyjne, planowanie i nadzór nad działaniami operacyjnymi – co zobowiązuje organizację do zaplanowania, wdrożenia i nadzorowania procesu niezbędnego do spełnienia wymagań w zakresie bezpieczeństwa informacji; w tym celu konieczne staje się wdrożenie stosownych planów bezpieczeństwa;

283 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 186

– monitorowanie, pomiar, analiza i ocena – co oznacza konieczność dokonywania oceny wyników i działań na rzecz bezpieczeństwa informacji;
– audyt wewnętrzny – który należy przeprowadzać w zaplanowanych odstępach czasu, w celu dostarczenia informacji o tym, czy system zarządzania bezpieczeństwem spełnia wymagania z własnymi założeniami, politykami oraz regulacjami prawa oraz jest skutecznie wdrożony i utrzymywany [284].

W zależności od przyjętej metodologii audytów planowych można określić zakres audytów w oparciu o poszczególne procesy przetwarzania danych osobowych lub w oparciu o poszczególne wymogi prawa [285].

Uogólniając, czynności kontrolne i audytowe w zakresie zgodności przetwarzania i jako takiej ochrony danych osobowych z przepisami prawa wykonywane są przez podmioty, które przetwarzają dane i stanowi on jeden z mechanizmów zarządzania. To kontrola, którą można określić mianem „kontroli funkcjonalnej", ponieważ sprawowana jest w ramach funkcji kontrolnych, będących istotnym elementem bieżącego zarządzania procesami przetwarzania danych osobowych [286].

W RODO nie sprecyzowano terminów przeprowadzania ewentualnych audytów. Wydaje się jednak, że nie powinny być one być rzadsze niż raz w roku. Okres ten pozwala inspektorowi na ocenę zmian, jakie zachodzą w systemie przetwarzania danych funkcjonującym w organizacji, jak i pozwala na wprowadzenie rekomendacji wydanych przy poprzednim audycie [287]. Normy ISO zalecają przeprowadzanie audytów wewnętrznych w cyklu rocznym, oczywiście decyzję w tym zakresie podejmuje najwyższe kierownictwo [288].

Wykazywanie zgodności z RODO może następować również wobec administratora, gdy odpowiednio podmiot przetwarzający, subprocesor, czy przedstawiciel wykazać mają administratorowi, że zapewnili wystarczające gwarancje wdrożenia odpowiednich środków

284 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

285 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 96

286 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 188 - 189

287 M. Zadorożny, *Inspektor ochrony danych (IOD) jako następca ABI* [w:] A. Dmochowska (red.), M. Zadorożny (red.) *Unijna reforma ochrony danych osobowych*, C. H. Beck, Warszawa 2018, str. 146

288 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 89

technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą [289].

Warto, aby przyszły inspektor ochrony danych zapoznał się z normą PN-EN ISO 19011 (wytyczne dotyczące audytowania systemów zarządzania jakością i/lub zarządzania środowiskowego), która opisuje m.in. zasady przeprowadzania audytu. Zadaniem inspektora jest przedstawienie wiarygodnych informacji najwyższemu kierownictwu organizacji dotyczących przetwarzania i ochrony danych osobowych. Aby IOD posiadał takie informacje, zobowiązany jest do przeprowadzania systematycznych audytów. Aby audyt był wiarygodnym i efektywnym narzędziem do dostarczania niezbędnych informacji dla kierownictwa organizacji, powinien opierać się na kilku zasadach przedstawionych w przedmiotowej normie ISO [290].

Mając powyższe na uwadze oraz doświadczenie audytowe i wiedzę specjalistyczną każdy IOD powinien wraz z zespołem ekspertów realizować zadania audytowe w oparciu o wyżej wskazane normy i przepisy, ponieważ są one ze sobą bezpośrednio powiązanie, a nie jedynie opierać się na przepisach RODO w tym zakresie.

III. 2. Rola IOD w zakresie audytu bezpieczeństwa informacji i ochrony danych osobowych

Jak wspomniano w pierwszym rozdziale niniejszej pracy jednym z kluczowych zadań IOD zgodnie z art. 39 ust. 1 RODO jest „monitorowanie przestrzegania niniejszego rozporządzenia, 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". Wspomniano również o jego kwalifikacjach jako audytora wynikających z RODO oraz z rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania. Z powyższego wynika, że zawód ten został sklasyfikowany pod pozycją audytor/kontroler w ramach specjalistów do spraw administracji i rozwoju. Podkreślono również, że kluczowa w tym zakresie wydaje się być znajomość specyfiki branży, RODO i przepisów szczegółowych, a także posiadanie stosownego doświadczenia zawodowego,

289 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 188

290 M. Zadorożny, *Inspektor ochrony danych (IOD) jako następca ABI*, op. cit., str. 147

w tym w zakresie realizacji audytów bezpieczeństwa informacji i ochrony danych osobowych, jak również weryfikacji sposobów zabezpieczenia informacji przetwarzanych zarówno metodą tradycyjną, ale również przy użyciu urządzeń i nośników informacji. Zatem wiedza IOD w obszarze bezpieczeństwa teleinformatycznego, a także oceny ryzyka i działań zapewniających i doradczych okazuje się fundamentalna w celu właściwej realizacji jego zadań ustawowych.

Rozpoczynając rozważania oraz w celu określenia roli IOD, jako audytora realizującego swoje zadania w zakresie bezpieczeństwa informacji i ochrony danych osobowych należy w pierwszej kolejności omówić i odróżnić często pojawiający się problem kumulowania się kompetencji i roli audytu wewnętrznego w tym zakresie. Należy tutaj mocno podkreślić i rozróżnić zakres kompetencji i zadania IOD oraz audytora wewnętrznego w przedmiotowym zakresie. Zarówno rola, jak również i zadania tych osób są całkowicie odmienne. Z kolei sposób wykonywania zadań oraz zasady pracy audytora, jego usytuowanie i zasady niezależności powinny być realizowane w oparciu o kodeks etyki, zgodnie z normą PN-EN ISO 19011, a także zgodnie z międzynarodowymi standardami praktyki zawodowej audytu wewnętrznego (zwane dalej standardami). Kodeks etyki jest konieczny i wręcz nieodzowny dla audytu wewnętrznego, ponieważ sprawą podstawową jest zaufanie pokładane w udzielanym przez audyt obiektywnym zapewnieniu dla ładu organizacyjnego, zarządzania ryzykiem i kontroli [291], co jest niezwykle istotne również podczas audytu bezpieczeństwa informacji. W rozumieniu normy PN-EN ISO 19011 wśród zasad dotyczące audytorów należy wskazać postępowanie etyczne będące podstawą profesjonalizmu. Zaufanie, rzetelność, poufność są istotne dla audytowania. Kolejną zasadą jest rzetelna prezentacja – obowiązek przedstawienia spraw dokładnie i zgodnie z prawdą. Ustalenia i wnioski oraz raporty z audytu odzwierciedlają działania audytowe dokładnie i zgodnie z prawdą. Znaczące przeszkody napotkane podczas audytu oraz nierozstrzygnięte lub rozbieżne opinie pomiędzy zespołem audytowym a audytowanym są odnotywane w raporcie. Nie należy zapomnieć o należytej staranności zawodowej przejawiającej się w postaci pracowitości i rozsądku w audytowaniu. Audytorzy wskazują staranność odpowiednią do ważności zadań, jakie wykonują oraz do zaufania, jakie mają do nich klienci audytu i inne strony zainteresowane. Ważne, aby audytorzy mieli odpowiednie kompetencje. Z kolei wśród zasad audytowania dotyczących audytu możemy

291 Kodeks etyki oraz Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego, Tłumaczenie na język polski, THE INSTITUTE OF INTERNAL AUDITORS, wrzesień 2016, https://www.iia.org.pl/o-nas/standardy, dostęp z dnia 21.05.2020 r., str. 4

wyróżnić niezależność będącą podstawą bezstronności audytu i obiektywność wniosków z audytu. Audytorzy są niezależni od działalności poddanej audytowi oraz wolni od uprzedzeń i konfliktów interesów. Audytorzy zachowują obiektywizm podczas całego procesu audytu, aby zapewnić, że wnioski oraz ustalenia z audytu będą oparte wyłączenie na dowodach z audytu. Kolejną zasadą jest podejście oparte na dowodach jako racjonalna metoda uzyskania wiarygodnych i odtwarzalnych wniosków z audytu w systematycznym procesie audytu. Dowód z audytu jest weryfikowalny. Ponieważ audyt prowadzony jest w ograniczonym czasie z użyciem ograniczonych zasobów, jest ograniczony do próbek dostępnych informacji. Odpowiedni dobór próbki związany jest ściśle z zaufaniem, jakie można mieć do wniosków z audytu [292]. Z kolei celem Standardów jest dostarczenie wskazówek, jak przestrzegać obowiązkowych elementów Międzynarodowych ramowych zasad praktyki zawodowej. Istotne jest również wyznaczenie ramowych zasad wykonywania i upowszechniania szerokiego zakresu usług audytu wewnętrznego, przysparzających organizacji wartości dodanej. Celami Standardów są również stworzenie podstaw oceny działalności audytu wewnętrznego i przyczynienie się do usprawniania procesów i działalności operacyjnej organizacji [293].

W celu lepszego zrozumienia roli i zadań IOD oraz audytora wewnętrznego należy zwrócić uwagę na ustawowe regulacje tych stanowisk. Zwykle przez „audyt" rozumie się niezależną ocenę zgodności ze specyfikacją, standardami, umową lub innymi kryteriami [294]. Pojęcie audyt wewnętrzny zostało sprecyzowane w art. 272 u.o.f.p. jako działalność niezależna i obiektywna, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej [295] oraz czynności doradcze. Ocena, o której mowa powyżej, dotyczy w szczególności adekwatności, skuteczności i efektywności kontroli zarządczej w dziale administracji rządowej lub jednostce. Z wytycznych zaprezentowanych przez Ministerstwo Finansów wynika, że realizacja audytu o tematyce bezpieczeństwa informacji powinna następować zgodnie z wymogami określonymi w przepisach u.o.f.p., a także rozporządzenia w sprawie przeprowadzania i dokumentowania

292 M. Zadorożny, *Inspektor ochrony danych (IOD) jako następca ABI*, op. cit., str. 147

293 Kodeks etyki oraz Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego, Tłumaczenie na język polski, THE INSTITUTE OF INTERNAL AUDITORS, wrzesień 2016, https://www.iia.org.pl/o-nas/standardy, dostęp z dnia 21.05.2020 r., str. 9

294 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 186

295 Zgodnie z art. 68 ust. 1 u.o.f.p. kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.

audytu z uwzględnieniem standardów zawodowych audytu wewnętrznego. Resort finansów wskazuje, że wymogi dotyczą w szczególności takich zagadnień, jak roczne planowanie audytu wewnętrznego, przygotowanie programu zadania audytowego, czy prezentowanie wyników zadania w formie sprawozdania. Powyższe oznaczałoby konieczność umieszczania tego zadania w planie audytu. W przypadku, gdy zadanie to nie wynikałoby wprost z przeprowadzonej analizy ryzyka, podstawą do uwzględniania zadania w obszarze bezpieczeństwa informacji w planie audytu może być § 7 ust. 1 pkt 3 rozporządzenia w sprawie przeprowadzania i dokumentowania audytu wewnętrznego [296]. Należy również podkreślić, że ochrona zasobów jest tylko jednym z 7 celów kontroli zarządczej [297], co jednoznacznie wskazuje na konieczność wsparcia działań przez IOD, jako wykwalifikowanego fachowca i jego kluczowej roli w tym zakresie. Potwierdza to opinia prawna Grzegorza Sibigi, z której wynika, że „(...) czynności audytowe mogą naruszać niezależność ABI w rozumieniu przedstawionym w pkt 2.8, gdy dotyczą audytowania wykonywanych przez niego zadań. Już same zalecenia stanowią ingerencję w realizację zadań przez ABI. Zalecenia zawarte w sprawozdaniu z audytu wewnętrznego są monitorowane przez audytora wewnętrznego, który po upływie terminu do realizacji zaleceń przeprowadza czynności sprawdzające. To kolejna ingerencja, której nie można pogodzić z niezależnością ABI. Ponadto, jeżeli ABI odmówi wykonania zaleceń, to na podstawie § 19 ust. 3 rozporządzenia Ministra Finansów z 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu będzie zobowiązany przedstawić pisemne stanowisko kierownikowi jednostki oraz audytorowi wewnętrznemu, podczas gdy formalnie ABI nie może w żaden sposób podlegać audytorowi wewnętrznemu. Wobec powyższego ustawowa gwarancja niezależności ABI stanowi

296 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, Finanse Komunalne, 2016, nr 1-2. str. 126-133, https://sip.lex.pl/#/publication/151278164, dostęp z dnia 23.08.2020 r.

297 Celem kontroli zarządczej jest zapewnienie w szczególności:

1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;

2) skuteczności i efektywności działania;

3) wiarygodności sprawozdań;

4) ochrony zasobów;

5) przestrzegania i promowania zasad etycznego postępowania;

6) efektywności i skuteczności przepływu informacji;

7) zarządzania ryzykiem.

ograniczenie przeprowadzania wobec niego audytu wewnętrznego (...)" [298]. Dotychczas zakres planu sprawdzeń (audytu) był ściśle uregulowany przepisami prawa, warto jednak podkreślić, że stan rzeczy uległ zmianie po przekształceniu funkcji ABI w IOD. Zgodnie z definicją wynikającą z norm ISO: „plan audytu to opis działań oraz ustaleń organizacyjnych związanych z audytem" [299].

Wykonywanie zadań IOD podobnie, jak audytora wewnętrznego jest związane z analizą ryzyka oraz szeroko rozumiane czynności doradcze. IOD pełni również funkcję punktu kontaktowego zarówno dla osób z zewnątrz, jak również dla organu nadzorczego. Audytor wewnętrzny wykonuje swoje zadania w oparciu o roczny plan audytu wewnętrznego przygotowany na podstawie analizy ryzyka. Podobnie powinien to wykonywać IOD, co jednoznacznie wynika z analizy jego zadań ustawowych. Ponadto zarówno IOD, jak i audytor wewnętrzny podlegają bezpośrednio Kierownikowi jednostki. Audytor wewnętrzny ma prawo wstępu do pomieszczeń jednostki oraz wglądu do wszelkich dokumentów, informacji i danych oraz do innych materiałów związanych z funkcjonowaniem jednostki, w tym utrwalonych na elektronicznych nośnikach danych, jak również do sporządzania ich kopii, odpisów, wyciągów, zestawień lub wydruków, z zachowaniem przepisów o tajemnicy ustawowo chronionej.

RODO nie precyzuje kompetencji IOD wewnątrz organizacji administratora lub procesora. Podmiot powołujący IOD powinien określić (np. w polityce ochrony danych), jakie uprawnienia będą przysługiwać IOD. Oczywiście muszą one służyć realizacji zadań IOD. Szczegółowe kompetencje IOD mogą obejmować stały dostęp do wszystkich pomieszczeń, sprzętu, nośników i instalacji służących do przetwarzania danych osobowych oraz możliwość żądania od pracowników i współpracowników organizacji dostępu do informacji, dokumentów, pomieszczeń, nośników danych itp. Należy również pokreślić możliwość prowadzenia wewnętrznych postępowań w sprawach związanych z ochroną danych osobowych oraz wnioskowania o uzyskanie zewnętrznej opinii prawnej.

W piśmiennictwie wyrażono pogląd, iż wewnątrzorganizacyjne kompetencje IOD można porównać do uprawnień podmiotów kierujących komórką audytu wewnętrznego lub

298 K. Hudzik, *Inspektor ochrony danych osobowych a audytor wewnętrzny zatrudniony w jednostce sektora finansów publicznych. Łączenie funkcji, zasady współpracy,* IAP nr 4/2019, str. 27, Legalis.pl, dostęp z dnia 28.05.2020 r.

299 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit., s*tr. 89

osób kierujących komórką do spraw zapewnienia zgodności mając na uwadze zasady ładu korporacyjnego dla podmiotów nadzorowanych przyjętymi przez Komisję Nadzoru Finansowego [300].

Jednakże na nadrzędną rolę IOD w zakresie ochrony danych osobowych określają regulacje art. 38 RODO, gdzie wskazano, że IOD ma być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, a Administrator oraz podmiot przetwarzający zapewniają, by IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań ustawowych. Ponadto Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

W przypadku komórki audytu wewnętrznego, w której jest zatrudniony tylko jeden audytor lub gdy realizacja obowiązku prowadzenia audytu następuję poprzez usługodawcę niezatrudnionego w jednostce, przyjęcie jednego obszaru do oceny pod nazwą zarządzanie bezpieczeństwem informacji do przeprowadzania nie rzadziej niż raz na rok może destabilizować pracę audytora przy realizacji ewaluacji w innych obszarach działalności jednostki. Dodatkowo sprawę mogą komplikować słabe kwalifikacje audytora lub ich brak albo brak doświadczania w problematyce realizacji audytu IT. Kwestia dobrej znajomości metodyki tego rodzaju audytu odgrywa ważną rolę w formułowaniu rekomendacji odnośnie do działania systemu zarządzania bezpieczeństwem informacji [301].

Podsumowując należy stwierdzić, że zarówno IOD, jak i audytor wewnętrzny wspierają kierownika jednostki sektora finansów publicznych w realizacji celów i zadań tej jednostki. Jednostki sektora finansów publicznych będące administratorami danych ponoszą bowiem odpowiedzialność za pełną i całościową zgodność przetwarzania danych osobowych z przepisami prawa. Do zadań IOD należy monitorowanie zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa. Natomiast do zadań audytora wewnętrznego należy m.in. ocena zgodności działalności jednostki z przepisami prawa (a zatem również przepisami prawa o ochronie danych osobowych) oraz procedurami wewnętrznymi, a także skuteczności i efektywności działania, ochrony zasobów oraz zarządzania ryzykiem.

300 M. Gumularz, *Ochrona danych osobowych w sektorze publicznym, op. cit.*

301 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

W związku z tym działania audytorów wewnętrznych i inspektorów ochrony danych powinny być komplementarne. W celu wsparcia prawidłowego funkcjonowania jednostki powinni oni wymieniać informacje i dokumenty niezbędne dla prawidłowej realizacji swoich zadań. Zarówno inspektorzy ochrony danych, jak i audytorzy podlegają bezpośrednio kierownikowi jednostki, a ich praca może podlegać jego kontroli, w tym kontroli zleconej przez kierownika podmiotom wewnętrznym lub zewnętrznym. Zarówno w przypadku audytora wewnętrznego jak i inspektora ochrony danych kluczową rolę odgrywa niezależność w realizowaniu zadań. Stąd audytorzy i inspektorzy muszą w swojej pracy uwzględniać wzajemną niezależność i nie wpływać na jej ograniczanie. W przypadku, gdy audyt obejmuje zadania realizowane przez IOD audytor wewnętrzny powinien odnosić się do badanego obszaru, nie formułując wniosków dotyczących bezpośrednich działań IOD. W tym zakresie ostateczne decyzje podejmuje kierownik jednostki. Jeżeli IOD nie zgadza się ze stanowiskiem kierownika jednostki sektora finansów publicznych, powinien mieć możliwość przedstawienia swojego stanowiska, które powinno zostać uzasadnione i udokumentowane. Materiał ten może być przydatny w celach dowodowych w przypadkach oceny prawidłowości wykonywania funkcji IOD w kontekście jego odpowiedzialności na gruncie przepisów prawa pracy lub kodeksu cywilnego (odpowiedzialności kontraktowej) przez właściwe organy, co omówiono szczegółowo w rozdziale drugim niniejszej pracy [302].

Nie sposób nie wspomnieć również o kwestii możliwości łączenia funkcji audytora wewnętrznego i IOD. Audytor wewnętrzny, co do zasady, nie powinien brać udziału w określaniu celów i sposobów przetwarzania danych w jednostce. Dodatkowo audytor, podobnie jak IOD, podlega bezpośrednio kierownikowi jednostki (w przypadku jednoosobowej komórki audytu wewnętrznego, w wieloosobowej komórce, to kierownik komórki audytu wewnętrznego podlega bezpośrednio kierownikowi jednostki). Dlatego też wydaje się, że nie powinno dojść do konfliktu interesów, o którym mowa w RODO przy łączeniu funkcji audytora wewnętrznego oraz inspektora ochrony danych. Jednak, jak wskazuje Grupa Robocza Art. 29, z uwagi na indywidualny charakter każdej organizacji aspekt naruszenia niezależności inspektora ochrony danych powinien być analizowany dla każdego podmiotu oddzielnie [303].

302 *Zasady współpracy audytora wewnętrznego i inspektora ochrony danych przy realizacji zadań w jednostce sektora finansów publicznych*, https://uodo.gov.pl/pl/138/445, dostęp z dnia 21.05.2020 r.

303 K. Hudzik, *Inspektor ochrony danych osobowych a audytor wewnętrzny zatrudniony w jednostce sektora finansów publicznych. Łączenie funkcji, zasady współpracy,* op. cit., str. 26

III.3. Plan, cele oraz metody realizacji audytu (w zakresie bezpieczeństwa informacji i ochrony danych osobowych) w oparciu o metodykę ISO/IEC 27001, KRI, RODO

Nie ma jednego modelu prowadzenia dokumentacji audytowej. Ważne jest jednak, by rzeczywiście służyła udoskonalaniu systemu ochrony danych osobowych i pozwalała na wykazywanie zgodności z RODO, KRI i innymi przepisami czy normami, o których wspomniano w 1 części niniejszego rozdziału. Audyt, stanowiąc instrument weryfikacji przetwarzania danych osobowych z punktu widzenia zgodności z RODO, każdorazowo dokonywany powinien być w zależności od kontekstu, charakteru, zakresu, celu czy podstawy przetwarzania danych [304].

Inspektor powinien dokonywać okresowych przeglądów polityk ochrony danych. Przyjmuje się, że przegląd powinien być wykonywany nie rzadziej niż raz do roku, ale w zasadzie, poszczególne procedury będą oceniane wraz z każdym audytem przeprowadzanym w tym obszarze przez inspektora. Monitorowanie dokumentacji etapami, wraz z poszczególnymi audytami zgodności prowadzonymi przez IOD jest bardzo dobrym rozwiązaniem, gdyż pozwala na bieżąco dokonywać niezbędnych zmian w procedurach, a także analizować ich zgodność z wciąż zmieniającymi się przepisami prawa. Inspektor dokonując analizy dokumentacji powinien zwrócić uwagę na to, czy treści poszczególnych polityk są dostępne i są znane odpowiednim pracownikom, a następnie czy są stosowane. Jeżeli nie są stosowane, to jakie są przyczyny, czy w szczególności nie jest to kwestia tego, że procedura jest nieadekwatna do procesu przetwarzania lub zbyt skomplikowana [305].

Częstotliwość audytów określamy w treści dokumentacji ochrony danych osobowych, a zależy ona od rozproszenia organizacji administratora danych oraz od złożoności procesów przetwarzania danych osobowych. Warto pamiętać, że audyty nie muszą obejmować każdego przypadku faktycznego przetwarzania danych osobowych, a jedynie procesy ich przetwarzania pod kątem zgodności z przepisami prawa ochrony danych osobowych [306].

Dokumentacja audytu wewnętrznego (kontroli, sprawdzeń) powinna być prowadzona w taki sposób, by spełniała dwojakiego rodzaju zadania. Po pierwsze, aby była pomocna podmiotowi, który audyt przeprowadza, w weryfikacji zastosowanych rozwiązań,

304 M. Czaplińska, *IOD dla grupy przedsiębiorstw, komentarz praktyczny, op. cit.*

305 S. Czub-Kiełczewska, *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* op. cit.

306 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 95

systematyzowaniu przedsięwziętych działań, udoskonalaniu systemu ochrony danych osobowych. Po drugie, aby mogła posłużyć wykazywaniu zgodności z RODO głównie w relacji z organem nadzorczym, w trakcie prowadzonych przez niego kontroli czy postępowań, jak również w wykazywaniu zgodności z rozporządzeniem wdrożonych rozwiązań technicznych i organizacyjnych wobec administratora, na którego rzecz działa lub ma działać podmiot przetwarzający, subprocesor, przedstawiciel [307].

Jedną z kluczowych zasad przeprowadzania audytu wewnętrznego jest, aby inspektor przeprowadzający audyt przygotował programu audytu. IOD musi podjąć decyzję czy audyt będzie dotyczył całej organizacji, czy tylko wybranych obszarów. Zasadniczo każdy audyt wewnętrzny powinien składać się z kilku etapów. Należy pamiętać, że audytor nie działa z zaskoczenia, dlatego datę audytu ustala się przynajmniej na kilka lub kilkanaście dni przed planowanym terminem audytu. Pozwoli to również osobom biorącym udział w audycie na przygotowanie się i zebranie odpowiednich materiałów. Kolejną ważną zasadą jest, że rozpoczęcie audytu powinno zostać poprzedzone spotkaniem otwierającym, mającym na celu przedstawienie zakresu audytu, jego porządku itd. Samo przeprowadzenie audytu obejmuje analizę dokumentacji dotyczącej kontrolowanego obszaru działalności organizacji oraz badania bezpośrednio stanowisk pracy, a, co do zasady, polega na przeprowadzeniu odpowiednich wywiadu i obserwacji. Audyt powinien być zakończony spotkaniem zamykającym, podczas którego przekazywane są pierwsze oceny. Z każdorazowego audytu wewnętrznego powinien zostać opracowany dla najwyższego kierownictwa raport z audytu. Raport powinien zawierać: datę, zakres i cele audytu; wskazanie danych inspektora przeprowadzającego audyt i osób biorących w nim udział; charakterystykę organizacji; przedstawienie dokumentów związanych z badaniem; zaobserwowane niezgodności, uwagi pozytywne i potencjały doskonalenia. Opinie inspektora w kwestii stopnia zgodności przedmiotu badania z przepisami RODO i właściwą dokumentację obowiązującą w danej jednostce. Raport powinien zostać przekazany przez najwyższemu kierownictwu. Jeżeli audyt wykaże niezgodności, konieczne jest podjęcie odpowiednich działań korygujących. Wdrożenie i nadzorowanie tych działań jest domeną najwyższego kierownictwa. Inspektor ochrony danych powinien również nadzorować, czy i jak wdrażane są działania korygujące zaproponowane w raporcie [308].

307 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 189

308 M. Zadorożny, *Inspektor ochrony danych (IOD) jako następca ABI,* op. cit., str. 148

Ważne jest jednak, by dokumentacja audytowa rzeczywiście służyła udoskonalaniu systemu ochrony danych osobowych i pozwalała na wykazywanie zgodności z RODO. Warto także skorzystać z rozwiązań wypracowanych jeszcze w poprzednim stanie prawnym na podstawie ustawy o ochronie danych osobowych z 1997 r. oraz rozporządzeń wydanych z jej delegacji, a mianowicie: rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych [309] oraz rozporządzenia Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (zwanego dalej r.t.s.r.z.) [310]. Zwłaszcza ten ostatni akt może stanowić dobry punkt wyjścia do opracowania własnego systemu prowadzenia działań audytowych i ich odpowiedniego dokumentowania [311].

Przed przystąpieniem do opracowania planu zadania audytowego dotyczącego oceny aktualnego stanu bezpieczeństwa informacji i ochrony danych osobowych w jednostce Zespół audytujący powinien w mojej ocenie posiadać niezbędne informacje w formie stosownej ankiety/formularza. Ankieta ta zawiera odpowiedzi na kluczowe pytania dla Zespołu audytującego, m.in. co do wielkości organizacji/instytucji, liczby urządzeń końcowych oraz serwerów i używanych aplikacji i systemów IT, posiadanej dokumentacji z zakresu bezpieczeństwa informacji i ochrony danych osobowych i przeprowadzonych audytów w tym zakresie, czy liczby partnerów biznesowych, z którymi następuje automatyczna wymiana danych komercyjnych.

309 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. 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. z 2004 r., nr 100, poz. 1024

310 Rozporządzenie Ministra Administracji i Cyfryzacji z 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. z 2015 r., poz. 745

311 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, [red. M. Jagielski *Dokumentacja ochrony danych osobowych ze wzorami*], Wolters Kluwer, Warszawa 2019, str. 190 - 191

L.p.	Pytania ankietowe/informacje niezbędne	Wymagane dane	Informacje dodatkowe
1.	Liczba pracowników (ogółem)		np. pracownicy nieetatowi korzystający ze sprzętu i oprogramowania ADO Czy wszystkie osoby mające dostęp do danych osobowych posiadają aktualne upoważnienie do przetwarzania danych osobowych i podpisały aktualne oświadczenia o poufności
2.	Liczba oraz dokładne lokalizacje audytowanej jednostki		Należy wskazać również dokładne adresy kolejnych lokalizacji/oddziałów
3.	Liczba pracowników korzystających z dostępu do systemów IT z uwzględnieniem wykonywania zadań w formie zdalnej		Informacje o świadczeniu pracy w formie telepracy
4.	Urządzenia końcowe (stacja robocza, laptop, terminal, smartphone)		Należy wyszczególnić urządzenia używane do wykonywania

			telepracy oraz pracy zdalnej
5.	Lokalizacja data center/serwerowni		Należy uwzględnić odległości pomiędzy poszczególnymi lokalizacjami
6.	Serwery (fizyczne/wirtualne)		Należy uwzględnić liczbę serwerów i obsługiwanych systemów
7.	Aplikacje służących do przetwarzania danych osobowych		Proszę wskazać maksymalny tolerowany czas niedostępności
8.	Informacje w zakresie wykorzystywania przez jednostkę scentralizowanego zarządzania procesami i urządzeniami IT (np. Actve Directory)		Tak/nie i w jakim stopniu
9.	Struktura i funkcjonowanie dedykowanej komórki organizacyjnej odpowiedzialnej za IT		Tak/nie i liczba pracowników
10.	Struktura i funkcjonowanie komórki organizacyjnej odpowiedzialnej za bezpieczeństwo informacji		Tak/nie i liczba pracowników oraz zakres ich zadań i odpowiedzialności
11.	Informacje nt. wdrożenia przez jednostkę systemu zarządzania bezpieczeństwem informacji		Tak/nie

12.	Informacje nt. posiadanej przez jednostkę dokumentacji w zakresie bezpieczeństwa informacji i ochrony danych osobowych, tj. polityki bezpieczeństwa, polityk, instrukcji zarządzania systemami informatycznymi służącym do przetwarzania danych osobowych i innych dokumentów wewnętrznych dotyczących bezpieczeństwa i funkcjonowania IT		Tak/nie i wskazanie posiadanej dokumentacji
13.	Informacje nt. prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania		Liczba procesów przetwarzania danych osobowych i ich wyszczególnienie
14.	Informacje nt. realizacji obowiązków informacyjnych wobec osób, których dane dotyczą		Kanały dystrybucji klauzul informacyjnych
15.	Informacje nt. prowadzenia rejestru naruszeń i incydentów		Należy uwzględnić zgłoszenie lub nie naruszenia do Prezesa UODO
16.	Informacje nt. outsourcingu kluczowych funkcji IT		Tak/nie i liczba podmiotów realizujących
17.	Informacje nt. powołania IOD, w tym pisemnego uzasadnienia braku jego powołania		Tak/nie

18.	Informacje nt. realizacji audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych z wyszczególnieniem daty ostatniego audytu		Tak/nie i data ostatniego audytu i jego zakres
19.	Liczba partnerów biznesowych z którymi następuje automatyczna wymiana danych komercyjnych		Informacja, czy zawarto z tymi podmiotami stosowne postanowienia o poufności oraz wymagane przepisami umowy powierzenia przetwarzania danych osobowych
20.	Liczba podmiotów, z którymi zawarto umowę/porozumienie w zakresie współadministrowania danymi osobowymi		Zawarto/nie zawarto i liczba podmiotów

Źródło: opracowanie własne autora na podstawie doświadczenia nabytego podczas współpracy z firmą Locos P. Błaszczeć

Zgodnie z § 3 ust. 2 pkt 2 r.t.s.r.z. wprowadzono instytucję sprawdzenia doraźnego realizowanego w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez administratora bezpieczeństwa informacji wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.

Analogicznie przeprowadzenie audytu pozaplanowego – doraźnego można brać pod uwagę w sytuacji, gdy stwierdzono naruszenie ochrony danych osobowych, zachodzi przypuszczenie, że doszło do naruszenia, w tym w podobnych okolicznościach przetwarzania u innego administratora lub u podmiotu przetwarzającego. Dotyczy to również sytuacji, gdzie konkretny obszar przetwarzania danych osobowych objęty jest zagrożeniem wystąpienia naruszeń. Przeprowadzenie audytu pozaplanowego należy brać również pod uwagę w sytuacji,

gdy dochodzi do nieplanowanych wcześniej zmian w procesie przetwarzania danych osobowych, planowane jest powierzenie przetwarzania danych osobowych lub zawarcie umowy o współadministrowanie, czy dokonuje się zmiany podmiotu przetwarzającego. Z audytem pozaplanowym będziemy mieć również do czynienia, gdy osoba, której dane dotyczą, wniosła skargę na niezgodne z prawem przetwarzanie danych osobowych, a także, gdy organ nadzorczy wydał wytyczne dotyczące danego obszaru przetwarzania danych osobowych. Audyt pozaplanowy może okazać się skuteczny, gdy pojawią się orzeczenia sądów administracyjnych lub powszechnych w odniesieniu do zbliżonych okoliczności przetwarzania danych osobowych oraz gdy konieczne jest zweryfikowanie standardów przetwarzania danych osobowych u procesora. Administrator może również w ramach audytu pozaplanowego polecić przeprowadzenie audytu wewnątrz własnej organizacji, u podmiotu przetwarzającego lub u subprocesora. Należy tu również mieć na uwadze realizację audytu pozaplanowego w ramach bieżących czynności nadzorczych administratora lub inspektora ochrony danych (np. kontrola zabezpieczenia pomieszczeń, kontrola realizacji zasady „czystego biurka", kontrola przestrzegania tzw. polityki kluczy, kontrola częstotliwości zmiany haseł itp.) [312].

Plan audytów wewnętrznych pozwala na odpowiednie przygotowanie się kontrolującego i samej organizacji do przeprowadzenia czynności audytowych. Analiza, które z obszarów systemu ochrony danych osobowych wymagają weryfikacji i w jakiej kolejności, umożliwia zaprojektowanie w czasie działań zaradczych. Plan audytu pozwala na zastosowanie audytu, jako instrumentu cyklicznego nadzoru, jeśli konkretne procesy przetwarzania, zbiory danych, czy operacje przetwarzania audytowanie są systematycznie, bądź wtórnie. Przy planowaniu audytów należy określić czas, w jakim plan ma być wykonany oraz to, aby plan audytów był zakreślony w taki sposób, by działania audytowe przyniosły pożądany skutek w postaci oceny stanu zgodności przetwarzania danych osobowych z prawem oraz weryfikację zastosowanych środków technicznych i organizacyjnych. Przed jego konstruowaniem warto również zorientować się co do projektowanych w czasie objętym planem przedsięwzięć zadań, inwestycji, zmian organizacyjnych czy technologicznych, które mogą wpłynąć na przetwarzanie danych osobowych. Choć z przepisów RODO nie wynika zatwierdzanie planów audytów przez administratora, nie wydaje się, aby takie audyty mogły odbywać się poza jego wiedzą [313].

312 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 194

313 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op.cit., str. 191

Plan działań IOD winien zakładać dokonywanie okresowych sprawdzeń w zakresie przestrzegania każdej z zasad rozliczalności przetwarzania danych osobowych wynikających z art. 5 RODO oraz dopuszczalności przetwarzania danych zwykłych na podstawie art. 6 RODO, dopuszczalności przetwarzania danych wrażliwych. Plan okresowych audytów IOD powinien również obejmować weryfikację prawidłowości pozyskiwania zgód na przetwarzanie danych osobowych oraz przetwarzania danych na tej podstawie, w tym wyrażania zgody przez dzieci w przypadku usług społeczeństwa informacyjnego. Weryfikacja powinna dotyczyć także realizacji każdego z praw osób, których dane dotyczą, zabezpieczeń fizycznych i technicznych danych osobowych, organizacji ich przetwarzania, czy procesów przetwarzania danych osobowych. Należy również sprawdzić zasady udostępniania danych osobowych, przetwarzania danych osobowych w poszczególnych zbiorach danych i organizacji tego przetwarzania oraz czy uwzględniano ochronę danych osobowych w fazie projektowania i zastosowanie zasady domyślnej ochrony danych osobowych. Istotne jest sprawdzenie funkcjonowania obszaru rejestrowania czynności przetwarzania i poszczególnych czynności przetwarzania, obsługi naruszeń, raportowania o naruszeniach, dokumentowania naruszeń, czy przeprowadzania oceny skutków dla ochrony danych. IOD powinien dokonać również okresowej weryfikacji przestrzegania zasad wynikających z wiążących reguł korporacyjnych, procedur obowiązujących w przypadku kontroli organu nadzorczego, czy w przypadku wystąpienia z roszczeniem cywilnoprawnym na podstawie art. 79 lub 82 RODO. Na koniec należy również wziąć pod uwagę okresową analizę przetwarzania danych osobowych dla celów archiwalnych oraz prowadzenia przewidzianej w wewnętrznych regulacjach administratora lub podmiotu przetwarzającego dokumentacji z zakresu ochrony danych osobowych, osobowej, organizacyjnej [314].

Cele oraz poszczególne etapy zadania audytowego powinny być jasno określone i obejmować m.in. ocenę prawidłowości działań jednostki w zakresie ochrony danych osobowych i bezpieczeństwa informacji, w tym weryfikację wymaganej dokumentacji w przedmiotowym zakresie. Analiza powinna obejmować również, czy przetwarzanie danych następowało wyłączenie na polecenie administratora przez osoby upoważnione zgodnie z art. 29 RODO, oraz weryfikację posiadanych przez pracowników uprawnień w systemach teleinformatycznych. Istotna jest również realizacja oceny zgodności funkcjonowania bezpieczeństwa informacji w jednostce względem najlepszych praktyk stosowanych w zakresie bezpieczeństwa informacji i ochrony danych osobowych, a także zapewnienia zgodności

314 M. Czaplińska, *IOD dla grupy przedsiębiorstw,* komentarz praktyczny, op. cit.

z prawem. Należy przy tym uwzględnić również identyfikację zasobów, zagrożeń, podatności, incydentów oraz istniejących mechanizmów kontrolnych oraz ocenę prawdopodobieństwa wystąpienia ryzyka z obszaru teleinformatycznego i jego konsekwencji. Cele i poszczególne etapy zadania audytowego powinny obejmować rekomendacje w stosunku do wybrania i implementacji działań korygujących i zapobiegawczych oraz zapewnienie zgodności działań z obowiązującymi przepisami prawa, a także sporządzenie raportu-sprawozdania i przedstawienie wniosków oraz rekomendacji po przeprowadzonym audycie.

Ostatnim elementem planu audytu, jaki powinniśmy określić, jest metoda prowadzenia audytów. Przy analizie systemów informatycznych wybrana metodologia często decyduje o skuteczności audytu. Na przykład opieranie się jedynie na wywiadzie osobowym z administratorem systemów informatycznych stwarza bardzo wysokie ryzyko braku rzetelności w procesie audytu. Przy audycie systemów informatycznych powinno się położyć większy nacisk na metody, których wynikiem jest dowód audytowy (np. w postaci wyciągu z systemu informatycznego lub zrzutu ekranu) [315].

Audyt w głównej mierze powinien opierać się (w zależności od wielkości organizacji) na wywiadzie osobowym z pracownikami uczestniczącymi w procesie przetwarzania danych przez organizację oraz na szeroko rozumianej wizji lokalnej, tj. weryfikacji, czy fakty przedstawiane przez pracowników uczestniczących w audycie mają odzwierciedlenie w rzeczywistości [316].

Każdy IOD musi wypracować własne narzędzia pełnienia nadzoru dostosowane do jego charakteru i posiadanego doświadczenia. Należy zgodzić się ze stanowiskiem K. Galaj Emiliańczyka, że doświadczony IOD jest w stanie przeprowadzić skutecznie wywiad osobowy lub wizję lokalną bez wcześniejszego przygotowania niemal w każdej organizacji. Natomiast początkujący IOD musi opierać się na wcześniej przygotowanej liście kontrolnej, tak by nie pominąć żadnego obszaru, który musi zostać zweryfikowany, lub nie zapomnieć zadać odpowiednich pytań. Przed przystąpieniem do audytu IOD powinien przygotować harmonogram poszczególnych czynności składających się na audyt. W praktyce chodzi

315 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów,* op. cit., str. 98

316 M. Zadorożny, *Inspektor ochrony danych (IOD) jako następca ABI*, [w:] A. Dmochowska (red.), M. Zadorożny (red.) *Unijna reforma ochrony danych osobowych*, C. H. Beck, Warszawa 2018, str. 147

o wyznaczenie osób do wywiadów osobowych, określenie przedziału czasowego potrzebnego na przeprowadzenie wizji lokalnej, jak również na określenie czasu na analizę dokumentów [317]. Zgodnie z przepisami nieobowiązującego już co do zasady rozporządzenia w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji plan sprawdzeń miał obejmować wskazanie sposobu i zakresu dokumentowania sprawdzeń (§ 3 ust. 3 r.t.s.r.z.). Niemniej, analogicznie jak to było na gruncie przywołanego rozporządzenia, należy dążyć do tego, aby czynności przeprowadzone w toku audytu (sprawdzenia) były dokumentowane w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami RODO oraz do opracowania raportu (sprawozdania) z audytu. Dokumentowanie czynności w toku audytu może polegać w szczególności na:

1) utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych,

2) dokonaniu wydruku tych danych,

3) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,

4) odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem,

5) sporządzeniu kopii otrzymanego dokumentu,

6) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych,

7) sporządzeniu kopii danych pochodzących z rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub danych dotyczących konfiguracji technicznych środków zabezpieczeń tego systemu [318].

Mając powyższe na uwadze oraz doświadczenie własne autora oparte na realizacji czynności audytorskich opracowano plan audytu obecnego stanu bezpieczeństwa informacji i ochrony danych osobowych w jednostce zgodnie z wymogami normy ISO/IEC 27001, KRI oraz RODO, który przedstawia się następująco:

317 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 101

318 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 196

Temat audytu: **Audyt obecnego stanu bezpieczeństwa informacji i ochrony danych osobowych w jednostce**		**Zgodność z przepisami, normami: ISO/IEC 27001, KRI, RODO**
Audytor wiodący i członkowie zespołu audytującego: ……. Termin rozpoczęcia audytu: ……		
Tematyka	**Zespół**	**Zaangażowane osoby**
Data:	**Audytor:**	**Strona audytowana:**
Spotkanie otwierające. Przedstawienie celu i zakresu audytu oraz sposobu realizacji czynności audytowych.		Kierownictwo organizacji, Kierownicy komórek organizacyjnych
Krótkie omówienie przez Zamawiającego procesów przetwarzania informacji w organizacji. Organizacja bezpieczeństwa informacji i systemu ochrony danych osobowych. Weryfikacja podstawowych stref przetwarzania informacji, pomieszczeń i zabezpieczeń fizycznych.		Osoba odpowiedzialna za bezpieczeństwo informacji i ochronę danych osobowych.
Bezpieczeństwo zasobów ludzkich. Weryfikacja procesu rekrutacyjnego oraz procesów związanych z zatrudnieniem. Weryfikacja obowiązujących procedur w zakresie wykonywania pracy zdalnej i telepracy		Osoba odpowiedzialna za HR, Osoba odpowiedzialna za kadry.
Działania nadzorczo-kontrolne w obszarze bezpieczeństwa informacji. Bezpieczeństwo fizyczne i środowiskowe. Bezpieczeństwo sprzętu. Kontrola dostępu. Pozyskiwanie i rozwój systemów informatycznych. Relacje z dostawcami Aspekty zarządzania ciągłością działania.		Osoba odpowiedzialna za administrację budynkami i zabezpieczenia fizyczne. Osoba odpowiedzialna za bezpieczeństwo informacji i ochronę danych osobowych. Osoba odpowiedzialna za IT.
Zgodność z regulacjami prawnymi (RODO, KRI), w tym dotyczącymi ochrony danych osobowych.		Osoba odpowiedzialna za zgodność. Dział promocji i marketingu.

Weryfikacja podstawowych rejestrów, ewidencji, wykazów, upoważnień (rejestr incydentów, rejestr udostępnionych danych osobowych, ewidencja osób upoważnionych do przetwarzania danych osobowych, wykaz zawartych umów powierzenia przetwarzania danych osobowych). Weryfikacja obowiązków spoczywających na ADO w zakresie: – dostosowanie systemów przetwarzania danych do zasad konstytuowanych przez RODO – art. 5 i 25 RODO; – spełnianie obowiązku informacyjnego – art. 13 i 14 RODO; – zawarcie lub aktualizacja umów powierzenia danych – art. 28 RODO (ewentualnie zawarcie uzgodnienia na podstawie art. 26 RODO); – przeprowadzenie analizy ryzyka w celu wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku – art. 24 i 32 RODO; w uzasadnionych przypadkach sporządzenie oceny skutków dla ochrony danych – art. 35 RODO; – aktualizacja/opracowanie wewnętrznej dokumentacji (polityk ochrony danych) – art. 24 ust. 2 RODO; – zapewnienie, by przetwarzanie danych następowało wyłączenie na polecenie administratora przez osoby upoważnione – art. 29 RODO, w tym weryfikacja posiadanych przez pracowników uprawnień w systemach teleinformatycznych;		Dział prawny, radca prawny, Osoba odpowiedzialna za ochronę danych osobowych/IOD Wybrani kierownicy komórek organizacyjnych.

– sporządzenie rejestru czynności przetwarzania/ rejestru kategorii czynności przetwarzania – art. 30 RODO; – opracowanie procedur na wypadek incydentów i naruszeń ochrony danych osobowych oraz zaprowadzenie rejestru naruszeń – art. 33 i 34 RODO; – wyznaczenie inspektora ochrony danych – art. 37–39 RODO oraz zgodnie z ustawą o ochronie danych osobowych, – w zakresie przesłanek legalności przetwarzania danych osobowych, merytorycznej poprawności danych i ich adekwatności do celu przetwarzania oraz innych wymogów wynikających z RODO i przepisów ustawowych. Weryfikacja procedur i zasad realizacji praw osób, których dane dotyczą Weryfikacja zasad funkcjonowania Inspektora Ochrony Danych i wykonywanych przez niego zadań w jednostce. Weryfikacja zasad i funkcjonowania oceny skutków przetwarzania danych osobowych Działania marketingowe. Profilowanie.		
Bezpieczeństwo systemów i sieci. Przetwarzanie mobilne Kryptografia- wybrane aspekty. Bezpieczeństwo komunikacji Krytyczność systemów i aplikacji- wybrane aspekty Eksploatacja i utrzymanie systemów informatycznych. Zarządzanie incydentami.		Osoba odpowiedzialna za systemy teleinformatyczne i przetwarzanie danych w systemach IT.

Zasady zgłaszania i postępowania w przypadku naruszenia ochrony danych osobowych.		
Spotkanie zespołu audytorów		-
Spotkanie zamykające		Osoby wskazane przez koordynatora.

Źródło: opracowanie własne autora na podstawie doświadczenia nabytego podczas współpracy z firmą Locos P. Błaszczeć

Przeprowadzenie zadania audytowego możemy podzielić w praktyce na następujące etapy:

1) wstępną analizę dokumentów przekazanych przez pracowników (formularzy, druków, umów, wszelkich procedur związanych z ochroną informacji), dokonywaną jeszcze przed przeprowadzeniem rozmów z pracownikami;
2) wywiady audytowe dotyczące procesów związanych z przetwarzaniem danych osobowych – w formie osobistych spotkań z pracownikami poszczególnych działów;
3) wizję lokalną w siedzibie audytowanej organizacji oraz poszczególnych jej lokalizacjach, w których są przetwarzane dane osobowe;
4) weryfikację spełniania przez systemy informatyczne służące do przetwarzania danych osobowych wymagań prawa ochrony danych osobowych;
5) weryfikację wszystkich przekazanych do analizy dokumentów służących do przetwarzania danych osobowych (formularzy, umów, druków itp.) pod kątem adekwatności gromadzonych danych w stosunku do celu przetwarzania, czasowości, celowości, merytorycznej poprawności, legalności;
6) opracowanie raportu podsumowującego wyniki audytu wraz z wykazem niezgodności oraz wskazaniem rozwiązań służących wyeliminowaniu ewentualnych naruszeń i przekazanie go kadrze zarządzającej w celu zapoznania się i wspólnego omówienia [319].

Fakt, że ADO odpowiada za przestrzeganie przepisów RODO, nie powinno budzić kontrowersji, iż powinien mieć on wiedzę i wpływ na to, w jakim zakresie owo przestrzeganie przepisów RODO będzie testowane. Dlatego też sporządzony plan sprawdzeń powinien co najmniej być przedłożony do jego wiadomości, a uzasadnione byłoby także nadanie temu planowi odpowiedniej rangi poprzez jego zatwierdzenie przez administratora. Nie należy zgodzić się z poglądem wyrażonym przez M. Sakowską -Baryłę, że w zależności od praktyki

319 M. Korga, *Z praktyki zespołu audytorów – jak przygotować jednostkę do zmian, które niesie za sobą Rozporządzenie unijne?* IAP nr 3/2017 r., C.H.Beck, str. 18, Legalis.pl, dostęp z dnia 28.05.2020 r.

konkretnego podmiotu plan sprawdzeń podawany jest do wiadomości jego personelu albo pozostaje dokumentem, którego treść znana jest wyłącznie administratorowi (najwyższemu kierownictwu administratora) oraz osobom, które audyt wewnętrzny prowadzą, ponieważ może to naruszać zasadę transparentności [320].

Osoby występujące w imieniu administratora danych (właściciele procesów) muszą zostać poinformowane o terminie audytu odpowiednio wcześnie przed jego przeprowadzeniem tak, by zdążyły się do niego przygotować. Określając terminy poszczególnych audytów, należy brać pod uwagę takie czynniki, jak liczba osób, z którymi trzeba będzie przeprowadzić wywiady osobowe, liczba lokalizacji, w których trzeba będzie przeprowadzić wizje lokalne, liczba dokumentów, które trzeba będzie przeanalizować w poszczególnych procesach, czy liczba witryn internetowych i usług świadczonych drogą elektroniczną. Warto również pamiętać, że gromadzenie informacji jest jedynie elementem audytu planowego, kolejno należy przeanalizować zgromadzone informacje pod kątem ich zgodności z przepisami prawa i wytycznymi organu nadzorczego, co również wymaga czasu [321].

Rozpoczęcie czynności audytowych powinno być poprzedzone spotkaniem otwierającym, podczas którego dokonuje się przedstawienia celu i zakresu audytu oraz sposobu realizacji czynności audytowych. Istotnym elementem wspomagającym przeprowadzenie zadania audytowego, w tym ułatwiającym prowadzenie wywiadów i badanie dokumentacji może być lista kontrolna porządkująca poszczególne elementy i obszary podlegające sprawdzeniu.

Każdy audyt czy kontrola u administratora w zakresie sposobów przetwarzania przez niego danych, rozpoczyna się od zapoznania z obowiązującą u niego dokumentacją. W następnej kolejności jest oceniana zgodność dokumentacji z przepisami oraz stanem faktycznym, w tym rydzykami dla ochrony danych. Istotną rolą IOD jest uświadomienie administratorowi, jak ważne jest opracowanie i stosowanie dokumentacji ochrony danych, a także ciągłe szkolenie pracowników z wynikających z niej zasad [322].

320 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 192

321 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 96

322 S. Czub-Kiełczewska, *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* ……..

Wizja lokalna jest często zaniedbywaną metodą prowadzenia sprawdzeń przez IOD, jednak jest to jedyna metoda, by w praktyce dokonać weryfikacji zastosowanych zabezpieczeń [323].

Niezwykle istotnym elementem, a zarazem trudnością pojawiającą się podczas przeprowadzania audytu w poszczególnych działach organizacji, jest duża liczba przepisów prawnych, które odnoszą się do różnorakich form jej działalności. Należy tu w szczególności wskazać przepisy prawa pracy wraz z przepisami wykonawczymi w tym zakresie, w tym dotyczące bezpieczeństwa i higieny pracy, zakładowego funduszu świadczeń socjalnych, czy pracowniczych kas zapomogowo-pożyczkowych. Nie należy zapomnieć również o przepisach prawa cywilnego, prawa autorskiego, zamówień publicznych, czy o świadczeniu usług drogą elektroniczną. Wskazane powyżej przepisy są zazwyczaj punktem wyjścia do analizy zachodzących w audytowanej jednostce procesów i dokumentacji. Dochodzą do nich bowiem przepisy branżowe i sektorowe, czy przepisy szczególne, ściśle związane z obszarem prowadzonej przez podmiot działalności, które obligatoryjnie należy przed audytem przeanalizować [324]. Mając powyższe na uwadze w przypadku jednostek administracji publicznej nie sposób nie wspomnieć o konieczności weryfikacji takich przepisów, jak ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych, czy przepisy oraz instrukcje w sprawie organizacji i zakresu działania archiwów zakładowych. KRI, czy szeregu regulaminów, polityk, instrukcji, wytycznych i innych regulacji wewnętrznych obowiązujących w danej jednostce, które często oparte są na przepisach szczegółowych, czy branżowych.

Najtrudniejszym elementem analizy dokumentacji zgodności z RODO są środki techniczne i organizacyjne. W przeciwieństwie do pozostałych elementów tego dokumentu trzeba bowiem zweryfikować w jego treści nie tylko to, czy zostały uwzględnione, ale również to, jakie jest ich zastosowanie w praktyce. Inaczej mówiąc, musimy brać pod lupę konkretne zabezpieczenia z dokumentacji i następnie identyfikować ich zastosowanie w organizacji. Procedury opisujące zabezpieczenia techniczne w systemach informatycznych są praktycznie niemożliwe do zweryfikowania bez podstawowej wiedzy informatycznej posiadanej przez IOD i/lub bez wsparcia ASI (administratora systemów informatycznych). Najtrudniejszym

323 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 107

324 M. Korga, *Z praktyki zespołu audytorów – jak przygotować jednostkę do zmian, które niesie za sobą Rozporządzenie unijne?* Op. cit., str. 18-19

elementem weryfikacji jest określenie ich funkcjonalności, gdyż są one często zaszyte w samym kodzie oprogramowania [325].

Inspektor prowadząc audyty zgodności z RODO powinien być dociekliwy i zakładać, że nic nie jest oczywiste i niczego nie wie. Jest to jedna z podstawowych zasad prowadzenia audytów zgodności systemów zarządzania bezpieczeństwem informacji według normy ISO 27001. Ważne jest, aby nawet podstawowe pytania były zadawane w sposób otwarty, dając możliwość udzielenia konkretnych wyjaśnień osobie, do której są kierowane. Bardzo dobrą praktyką jest prowadzenie audytów zgodności z RODO na podobnej zasadzie [326].

Każde z pytań może prowokować kolejne pytania. Z tego względu powinniśmy jak najczęściej zadawać pytania otwarte, czyli niesugerujące odpowiedzi. W ten sposób zgromadzimy najwięcej informacji. Tworząc listę pytań, powinniśmy sugerować się nie tylko wymogami prawa, ale również wytycznymi GR art. 29 ds. ochrony danych, które są opublikowane i posegregowane tematycznie na stronie Prezesa UODO. Dodatkowo warto korzystać ze stron internetowych publikujących informacje o wyciekach danych osobowych oraz na temat luk w systemach informatycznych. Prowadząc wywiady osobowe, IOD również uczy się od osób z poszczególnych działów, jak w praktyce działy te funkcjonują. Wywiady osobowe są również bardzo dobrą okazją dla IOD, by zweryfikować poziom świadomości osób przetwarzających dane osobowe w zakresie bezpieczeństwa informacji [327].

Doskonałym punktem wyjścia do każdego audytu jest przeprowadzenie wywiadów z pracownikami w zakresie znajomości wewnętrznych polityk administratora, zaczynając od pytania, czy są jakieś sformalizowane zasady, jeśli tak, gdzie są dostępne oraz do czego zobowiązują. Uwzględnianie w prowadzonych audytach wewnętrznych zbadania sposobu stosowania wewnętrznych regulacji dotyczących przetwarzania danych osobowych, pozwoli wykryć ryzyka związane z tymi procesami[328].

Przeprowadzenie wizji lokalnej powinno uwzględniać najczęściej występujące zagrożenia w badanym obszarze. Jeżeli w trakcie wizji lokalnej znajdziemy zagrożenie, na

---

325 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 108

326 S. Czub-Kiełczewska, *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* op. cit.

327 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 104

328 S. Czub-Kiełczewska, *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* op. cit.

które organizacja nie jest przygotowana, czyli nie ma zabezpieczenia, to pojawia się konieczność przeprowadzenia analizy ryzyka. IOD powinien określić, jak duże jest prawdopodobieństwo wystąpienia zagrożenia oraz jaka byłaby waga jego następstw, uwzględniając istniejące zabezpieczenia. Jeżeli w trakcie analizy ryzyka okaże się, że jest to ryzyko nieakceptowalne, IOD powinien przygotować stosowną rekomendację obniżającą poziom ryzyka [329].

W celu lepszego zobrazowania niniejszej tematyki oraz w oparciu o doświadczenie własne autora w zakresie oceny stanu bezpieczeństwa (środowiska wewnętrznego oraz otoczenia obiektu) i ryzyka z tym związanego dokonując pełnego przeglądu w obszarze bezpieczeństwa fizycznego i środowiskowego wskazano poniżej przykładowe zagrożenia dla organizacji i ich rodzaje. Przegląd, o którym mowa powinien dotyczyć sprawdzenia (w tym organoleptycznie) wszystkich rodzajów zabezpieczeń mechanicznych, elektronicznych zainstalowanych w budynku, w pomieszczeniach administracyjnych i innych. Znajomość tych zagrożeń i ryzyka z nimi związanego znacznie ułatwi przeprowadzenie zadania zapewniającego przez IOD. Wśród zagrożeń związanych z bezpieczeństwem fizycznym i środowiskowym należy wyróżnić zagrożenia zewnętrzne i wewnętrzne, czy będące wynikiem działania człowieka lub od niego niezależne. I tak wśród zagrożeń nie będących wynikiem działania człowieka należy wyróżnić m.in., klęski żywiołowe (ulewy, wichury, powodzie, itp.), pożary obiektów, katastrofa budowlana spowodowana działaniem „natury", czy awarie techniczne. Zagrożeń będących wynikiem działania człowieka będzie znacznie więcej i tu możemy wyróżnić m.in. uszkodzenie, kradzieże i dewastację mienia, działania na rzecz konkurencji, sabotaż, czy naruszenia bezpieczeństwa informacji i przepisów prawnie chronionych, w tym dotyczących ochrony danych osobowych. Powodem tych działań jest niewystarczające lub niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń, pomieszczeń, w których są przechowywane oraz przetwarzane informacje i dane osobowe, ułatwiając w ten sposób dostęp do informacji osobom nieuprawnionym. Należy tu również wskazać nieprzestrzeganie podstawowych zasad „czystego biurka i ekranu", czy ochrony haseł np. poprzez opuszczenie przez pracownika stanowiska pracy bez zabezpieczenia sprzętu oraz dokumentów. Istotnym ryzykiem będzie również niewłaściwe zabezpieczenie sprzętu IT oraz oprogramowania przed utratą lub wyciekiem m.in. poprzez używanie prywatnych urządzeń, sprzętu, itp., do realizacji zadań służbowych, w tym nośników informacji (laptopy, pendrive, aparaty/kamery

329 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 105-106

fotograficzne, telefony komórkowe), które mogą służyć kradzieży danych/informacji, a jednocześnie mogą wprowadzać do komputerów służbowych i sieci wewnętrznej wirusy lub złośliwe oprogramowanie. Najczęstszą przyczyną występowania ryzyka są błędy użytkowników oraz nieprzestrzeganie lub brak obowiązujących zasad i procedur.

Obecnie nie ma regulacji dotyczących dokumentowania poszczególnych czynności audytowych. Istotne jest, aby dążyć do tego, żeby czynności przeprowadzone w toku audytu (sprawdzenia) były dokumentowane w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami RODO oraz do opracowania raportu (sprawozdania) z audytu. Bezspornie należy rekomendować sporządzanie tego rodzaju dokumentów, które będą stanowić istotne narzędzie w udoskonalaniu systemu ochrony danych osobowych w konkretnej organizacji [330].

Po zrealizowaniu audytu bezpieczeństwa informacji audytor powinien przedstawić kierownikowi jednostki rozwiązania, które pozwolą podjąć decyzję dotyczącą prac w przedmiocie projektowania skutecznych mechanizmów kontroli gwarantujących w ten sposób pełne bezpieczeństwo zarządzanej informacji oraz jej integralność. Tylko adekwatne i skutecznie działające mechanizmy kontroli wspomagają kierownictwo w zarządzaniu jednostką, gdyż w obecnym stanie prawnym tworzą spójny system kontroli zarządczej, zapewniającej realizację założonych celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Generalnie istota i cel funkcjonowania mechanizmów kontroli polega na ciągłym zapobieganiu i ograniczaniu znaczącego ryzyka w działalności jednostki w konkretnych obszarach. Mają one za zadanie nie dopuścić do materializacji poważnego ryzyka, co w konsekwencji spowodowałoby zakłócenie realizacji założonych celów i zadań [331].

Wraz z kolejnymi audytami IOD identyfikuje coraz większą liczbę zgodności z przepisami prawa. Wtedy przed IOD otwiera się całkiem nowy obszar możliwości modyfikowania i upraszczania zabezpieczeń. Najczęściej wraz ze wzrostem poziomu zgodności z przepisami prawa pracownicy (właściciele procesów) organizacji zdobywają coraz większy poziom świadomości co do istniejących zagrożeń, co z kolei umożliwia zastosowanie niższego poziomu zabezpieczeń, np. fizycznych, czy technicznych. Z drugiej strony możliwość doskonalenia może polegać również na stosowaniu coraz bardziej zautomatyzowanych

330 M. Czaplińska, *IOD dla grupy przedsiębiorstw,* op. cit.

331 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

zabezpieczeń w celu uniknięcia zbyt dużej liczby procedur, o których pracownicy muszą pamiętać [332].

Z punktu widzenia IOD, każdy „niedziałający właściwie" proces przetwarzania danych, powinien zostać uzdrowiony poprzez opracowanie i wdrożenie do stosowania odpowiedniej procedury. Nie tylko zminimalizuje to bieżące ryzyko, ale pozwoli zminimalizować je także w przyszłości, gdy proces będzie realizowany przez nowych pracowników [333].

W dobie outsourcingu warto kontrolować procesorów pod kątem stosowanych przez nich zabezpieczeń. Coraz częściej bowiem do incydentów ochrony danych osobowych dochodzi po stronie tych osób, podczas gdy to administrator danych może ponieść odpowiedzialność za brak nadzoru nad powierzonymi do przetwarzania danymi. Uzbrojony w efektywne narzędzia pełnienia nadzoru IOD może ostatecznie przejść do audytu początkowego systemu ochrony danych osobowych [334].

Efektem przeprowadzonego audytu jest zazwyczaj raport podsumowujący jego wyniki oraz ustalający rzeczywisty stan ochrony danych w jednostce [335]. Uzasadnione jest, by w raporcie tym wskazano cel przeprowadzonego audytu, opis stanu faktycznego, a więc kontekstu przetwarzania danych osobowych oraz uwarunkowań, które miały wpływ na prowadzenie ustaleń kontrolnych. W raporcie powinny być też wskazane stwierdzone uchybienia oraz rekomendacje co do sposobów i trybu ich usunięcia [336]. Bez tego elementu cel, jakim jest dostosowanie organizacji do wymogów prawa, nie zostanie osiągnięty. Rekomendacje powinny być ściśle powiązane z konkretnymi niezgodnościami, a te z kolei powinny być powiązane z przepisami prawa, do których dostosowujemy stan faktyczny [337]. Nie ma przeszkód, by treść raportu wzorowana była na zakresie wspomnianego sprawozdania ze sprawdzenia, choć – w zależności od potrzeb konkretnych działań kontrolnych – należałoby rozszerzyć go o takie jednostki redakcyjne, które pozwolą na uzyskaniu pełniejszego obrazu

332 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 126

333 S. Czub-Kiełczewska, *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* op. cit.

334 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 114

335 M. Korga, *Z praktyki zespołu audytorów – jak przygotować jednostkę do zmian, które niesie za sobą Rozporządzenie unijne? o*p. cit., str. 19

336 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit., str. 201 - 202

337 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 126

w odniesieniu do audytowanego obszaru oraz zastosowanie odpowiednich rozwiązań technicznych i organizacyjnych pozwalających na uzyskanie stanu zgodności przetwarzania danych osobowych z przepisami RODO lub innych przepisów z zakresu *ochrony danych osobowych*. Pamiętać należy jednocześnie o doborze załączników do raportu. Stanowić je może całość *dokumentacji* przebiegu i efektów audytu, jak również wybrane dokumenty mające szczególnie istotne znaczenie dla ustaleń dokonanych w toku audytu i w raporcie [338].

Według wytycznych Standardu oznaczonego numerem 15 „Mechanizmy kontroli dotyczące systemów informatycznych" należy określić mechanizmy gwarantujące bezpieczeństwo danych i systemów informatycznych. Jest to ogólna wytyczna, która stanowi jedynie wskazówkę dla kierownika jednostki co do dalszych działań w budowaniu spójnego modelu kontroli zarządczej. Przykładowe mechanizmy kontroli dla obszaru bezpieczeństwa informacji zarządzanej w systemach informatycznych mogą być następujące:

– mechanizmy kontroli przetwarzania (np. kontrola edycji sumy kontrolnej inne działania zaprogramowane w oprogramowaniu aplikacyjny, ścieżki rewizyjne);

– mechanizmy kontroli wyników (np. przegląd danych wyjściowych, raporty na temat niestandardowych zdarzeń, raporty na temat zmian plików głównych);

– zgodność zarządzania informacją w IT z licencjami na oprogramowanie;

– pisemne procedury w przedmiocie kontroli sprzętu komputerowego;

– plany dotyczące rozwoju i modernizacji sprzętu IT;

– polityka eksploatacji sprzętu IT i zarządzania zmianami w systemie bezpieczeństwa informacji;

– polityka w zakresie nadzoru, szacowania ryzyka, raportowania i postępowania z ryzykiem bezpieczeństwa informacji;

– plany awaryjne dotyczące awarii urządzeń w środowisku IT;

– zapewnienie okresowych przeglądów – audytów systemów informatycznych [339].

Raport przekazywany jest administratorowi danych (w praktyce kadrze zarządzającej audytowaną jednostką) w celu wspólnego omówienia kluczowych wniosków, możliwych rozwiązań, wyjaśnienia wątpliwości oraz podjęcia ustaleń, które będą stanowić podstawę do wdrożenia poszczególnych elementów systemu ochrony danych osobowych, a także stworzenia

338 M. Sakowska – Baryła, *Dokumentacja audytów wewnętrznych*, op. cit, str. 201 - 202

339 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

lub uaktualnienia dokumentacji dotyczącej ochrony danych osobowych [340].

Rekomendacje kierowane przez IOD do ADO powinny zawierać przede wszystkim: co ma być zrobione, dlaczego, przez kogo oraz kiedy. Taki kształt rekomendacji nie pozostawia wątpliwości po stronie osoby odpowiedzialnej za konkretny proces przetwarzania danych osobowych lub za konkretny obszar organizacji administratora danych osobowych. Oczywiście rekomendacje mogą być podważane, a zadaniem IOD jest takie ich przedstawienie, by były one uzasadnione [341].

Warto mieć na uwadze, że koszty opracowania i wdrożenia mechanizmów kontroli nie powinny przewyższać oczekiwanych rezultatów. Jest to związane z faktem poszanowania kardynalnej zasady głoszącej o racjonalizacji wydatków publicznych. Utrata kontroli nad bezpieczeństwem informacji, w szczególności zaś nad poufnością, dostępnością oraz integralnością informacji, jest klasyfikowana jako bardzo wysokie ryzyko – z uwagi na dotkliwe skutki w przypadku jego materializacji [342].

Podsumowując nie sposób nie wspomnieć również o wynikach kontroli NIK w jednostkach samorządu terytorialnego w województwie podlaskim. Wszelkie informacje o obywatelach, w tym dane wrażliwe, przechowywane w formie elektronicznej przez jednostki samorządowe, nie były odpowiednio zabezpieczone przed nieuprawnionym dostępem. Dane mogły w każdej chwili zostać przejrzane, przejęte lub zniszczone. Samorządy nie wiedziały nawet, kto ma do nich dostęp, gdyż nie monitorowały tych kwestii. Większość skontrolowanych jednostek nawet nie podejmowała działań minimalizujących ryzyko utraty informacji [343].

Kontrolą objęte zostały 3 starostwa powiatowe, 11 urzędów gmin (w tym 1 urząd miasta na prawach powiatu) oraz 11 ośrodków pomocy społecznej (w tym 1 w mieście na prawach powiatu). Przy wyborze podmiotów do kontroli uwzględniono zakres oraz aktualność informacji zawartych w rejestrze zbiorów danych osobowych oraz w rejestrze ABI prowadzonym przez GIODO. Kontrolą objęte zostały jednostki, które zgłosiły GIODO do zarejestrowania relatywnie małą liczbę zbiorów danych osobowych w porównaniu

340 M. Korga, *Z praktyki zespołu audytorów – jak przygotować jednostkę do zmian, które niesie za sobą Rozporządzenie unijne, op. cit., str. 19*

341 K. Gałaj-Emiliańczyk, *Inspektor ochrony danych. Kompetencje, obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów, op. cit.,* str. 128

342 P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, op. cit., str. 126-133

343 https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/bezpieczenstwo-informacji-woj-podlaskie.html

z pozostałymi podmiotami tego rodzaju. Kolejnym czynnikiem był fakt powołania lub niepowołania w danej jednostce tzw. administratora bezpieczeństwa informacji (obecnie podobne funkcje pełni IOD). Przy wyborze podmiotów brano również pod uwagę teren, na którym działa dana jednostka (wiejski, wiejsko-miejski, miejski), aby wybrana do kontroli grupa była reprezentatywna i jak najbardziej oddawała rzeczywisty stan badanej działalności w województwie podlaskim. Kontrolę we wszystkich jednostkach prowadzono na podstawie art. 2 ust. 2 ustawy o NIK. Kryteriami kontroli były legalność i rzetelność [344].

O tym jak ważne jest właściwe zabezpieczenie informacji gromadzonych w jednostkach samorządu terytorialnego świadczą przypadki ich utraty nagłośnione przez media w ostatnich latach. Należy tu wskazać przykład, jak w ciągu dwóch lat (2013-2014) hakerzy okradli pięć polskich gmin, w tym gminę Jaworzno na prawie milion złotych. W 2014 r. wyciekły dane dzieci z przemyskiego Urzędu Miejskiego. Z kolei w 2017 r. z Urzędu Miasta Łodzi wyciekły dane z tzw. deklaracji śmieciowych, przez co bez problemu można było poznać dane właścicieli łódzkich nieruchomości. Następnie w 2018 r. wyciekły dane części posiadaczy Karty Krakowskiej. W ocenie NIK, blisko 70 proc. skontrolowanych urzędów (16 z 23 urzędów) nie radziło sobie z zapewnieniem bezpieczeństwa przetwarzania informacji, co Izba oceniła negatywnie. Kontrolerzy NIK stwierdzili, że w ponad 60 proc. badanych urzędów brakowało systemowego podejścia do zapewnienia bezpieczeństwa informacji, gdyż opracowane w tych jednostkach regulacje dotyczyły głównie danych osobowych i nie obejmowały bezpieczeństwa innych informacji. Ponadto stwierdzono, że w prawie 3/4 kontrolowanych urzędów brak było pełnej i aktualnej informacji o posiadanych zasobach informatycznych służących do przetwarzania danych. Oznacza to, że w przypadku wystąpienia poważnej awarii lub innego zdarzenia losowego (takiego jak zalanie, pożar czy kradzież), utrudnione będzie szybkie odtworzenie infrastruktury i zapewnienie ciągłości świadczenia usług dla obywateli. Kontrola NIK wykazała, że w części urzędów nie przestrzegano obowiązujących zasad mających na celu zwiększenie bezpieczeństwa przetwarzania danych. W ponad 80 proc. skontrolowanych urzędów wystąpiły nieprawidłowości w zarządzaniu uprawnieniami użytkowników w systemach informatycznych [345].

Kolejna kontrola NIK zakończona we wrześniu 2020 r. dotycząca wprowadzenia RODO w urzędach dużych miast potwierdziła, że choć czasu na wprowadzenie w życie

344 J. Noga-Bogomilska, *Kto może kontrolować podmioty w zakresie ochrony danych osobowych?*, Lex/el. 2019, dostęp z dnia 18.12.2020 r.

345 https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie-znaczylo-bezpiecznie.html, dostęp z dnia 23.02.2020

unijnego rozporządzenia było dużo, to administracja publiczna nie przygotowała się w wystarczający sposób do wdrożenia potrzebnych procedur. NIK wybrała do kontroli te urzędy, które w najszerszym zakresie przetwarzają dane osobowe - urzędy wojewódzkie oraz urzędy dużych miast, a także MSWiA. Jak ocenia NIK, administracja publiczna radziła sobie z wyzwaniami związanymi z wprowadzeniem RODO w sposób zadowalający. Zanim nowe unijne przepisy dotyczące ochrony danych osobowych weszły w życie, wszystkie kontrolowane urzędy przygotowywały się do ich wprowadzenia analizując m.in. słabości dotychczas stosowanych rozwiązań. Zwykle zadanie to powierzano powołanym w urzędach Inspektorom Ochrony Danych czy specjalnym zespołom, ale także firmom zewnętrznym, które kompleksowo przygotowywały urząd do wdrożenia RODO. Przeprowadzały audyt dotyczący bezpieczeństwa informacji i ochrony danych osobowych, a następnie wskazywały co trzeba zmienić, np. w obowiązujących dokumentach czy procedurach, co należy ocenić pozytywnie. Jednak by te działania były efektywne i skuteczny nieodzowne jest prowadzenie okresowych audytów bezpieczeństwa informacji bowiem ich brak może powodować brak możliwości zachowania ciągłości działania jednostki i realizacji założonych celów i zadań. W każdym z kontrolowanych urzędów powołano IOD, który powinien podlegać tylko administratorowi tych danych, czyli ministrowi, wojewodzie lub prezydentowi miasta. W jednym przypadku (Urząd Miejski w zachodniopomorskim Stargardzie), niezgodnie z RODO IOD podlegał, także pod względem merytorycznym, sekretarzowi miasta. Zdaniem NIK taka podległość stwarza możliwość tzw. władczego oddziaływania na istotne sprawy pozostające w gestii IOD, czyli jednostronnego rozstrzygania - w tym przypadku sekretarza miasta - o prawach i obowiązkach Inspektora Ochrony Danych, co jednoznacznie potwierdza nieprawidłowości i przedstawione statystyki, o których mowa w poprzednich rozdziałach niniejszej pracy. W większości skontrolowanych urzędów zastosowane środki bezpieczeństwa (techniczne, fizyczne i informatyczne), służące utrzymaniu poufności, integralności oraz dostępności systemów i usług przetwarzania danych, były zgodne z wewnętrznymi uregulowaniami obowiązującymi w tych urzędach. Dostęp do zasobów informatycznych wymagał odpowiedniego uwierzytelnienia. Pracownicy oraz osoby zatrudniane na podstawie umów cywilno-prawnych mieli upoważnienia do przetwarzania danych osobowych, które powinny być niezwłocznie odbierane po rozwiązaniu umowy o pracę. Jednak w sześciu urzędach na 17 kontrolowanych, byłym pracownikom nie zablokowano dostępu do zasobów informatycznych. Dla przykładu w Urzędzie Miasta Stołecznego Warszawy nieuprawniony dostęp do konta - od jednego dnia do niemal roku - miało 16 z 21 byłych pracowników Urzędu Dzielnicy Ochota. Nieprawidłowości dotyczące fizycznego zabezpieczenia danych polegały głównie na

utrzymywaniu w niewłaściwym stanie technicznym serwerowni, w której gromadzone są informacje dotyczące najważniejszych sfer działalności urzędu, a ich utrata lub brak dostępności do nich może doprowadzić do sytuacji kryzysowej. Najbardziej jaskrawy przykład to serwerownia jednego z kontrolowanych urzędów miast, do której wejście mieściło się holu dostępnym dla petentów. Wejście to nie było zabezpieczone ani alarmami przeciwwłamaniowymi, ani monitoringiem wizyjnym, ani elektroniczną weryfikacją dostępu. Drzwi do serwerowni nie miały atestu antywłamaniowego, a wyposażenie pomieszczenia - atestu przeciwpożarowego (drzwi drewniane, wykładzina podłogowa), do tego zamontowany wewnątrz system gaszenia pożaru nie był odpowiedni dla sprzętu informatycznego. Stwarzało to zarówno możliwość nieautoryzowanego dostępu do serwerowni osobom postronnym, jak i niedostatecznie minimalizowało ryzyko zagrożenia pożarowego. We wszystkich kontrolowanych urzędach przed wejściem w życie przepisów RODO opracowano regulacje dotyczące niezbędnych działań, które powinny zostać podjęte w przypadku ewentualnego naruszenia ochrony danych osobowych. Ustalono w jaki sposób oceniany będzie poziom takiego naruszenia, oraz kto będzie odpowiadał za konkretne działania i jakie one będą. Kontrola wykazała jednak dwa przypadki nieprawidłowego postępowania już po stwierdzeniu naruszenia ochrony danych osobowych, gdzie nie przekazano informacji o naruszeniu danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, co było niezgodne z RODO. Unijne rozporządzenie przewiduje także możliwość żądania sprostowania bądź uzupełnienia niekompletnych danych. Skala takich żądań w kontrolowanym okresie była niewielka - od 1 do 7 przypadków, jedynie w Urzędzie Miasta Stołecznego Warszawy zgłoszono ich znacznie więcej - 344 osoby zażądały usunięcia swoich danych. NIK oceniła, że w większości skontrolowanych przypadków działania w reakcji na stwierdzone naruszenia ochrony danych osobowych oraz żądania ich usunięcia lub sprostowania były prowadzone prawidłowo.

Wnioski pokontrolne najczęściej dotyczyły upoważniania pracowników do przetwarzania danych osobowych z chwilą powstania stosownego obowiązku oraz niezwłocznego odbierania uprawnień dostępu do systemów informatycznych byłym pracownikom. Podkreślono również kwestię zabezpieczania pomieszczeń serwerowni przed utratą danych poprzez zminimalizowanie ryzyka nieautoryzowanego dostępu oraz zagrożenia pożarowego. Ponadto wskazano na stosowanie bezpiecznych rozwiązań informatycznych związanych m.in. z systemem autoryzacji dostępu do elektronicznych zasobów danych

osobowych gromadzonych w jednostce oraz z tworzeniem i przechowywaniem kopii bezpieczeństwa zgromadzonych danych [346].

Powyższe jednoznacznie potwierdza konieczność prowadzenia systematycznych audytów i działań monitorujących przestrzeganie przepisów o ochronie danych osobowych przez IOD. Należy w tym miejscu wspomnieć o karze administracyjnej w wysokości 50 tys. zł nałożonej przez Prezesa UODO będącej wynikiem stwierdzonego naruszenia ochrony danych osobowych przez Szkołę Główną Gospodarstwa Wiejskiego w Warszawie. Prezes UODO otrzymał w listopadzie 2019 roku zgłoszenie naruszenia ochrony danych osobowych kandydatów na studia w SGGW. Zgłoszenie było związane z kradzieżą przenośnego prywatnego komputera pracownika tej uczelni, który używał tego urządzenia także do celów służbowych, w tym do przetwarzania danych osobowych kandydatów na studia w SGGW na potrzeby czynności rekrutacyjnych. Po kontroli przeprowadzonej na uczelni w związku z naruszeniem ochrony danych, Prezes UODO wszczął z urzędu postępowanie administracyjne. Decydując o wysokości kary, organ nadzorczy wziął pod uwagę, że naruszenie ochrony danych osobowych dotyczyło kandydatów na studia w SGGW za okres ostatnich pięciu lat, obejmowało szeroki zakres danych, a liczba osób dotkniętych naruszeniem może wynosić do 100 tys. (górna granica). Wskazany okres 5 lat był niezgodny z wyznaczonym okresem przechowywania danych osobowych kandydatów na studia, co stanowiło naruszenie zasady ograniczenia przechowywania określonej w RODO. Znaczenie dla wysokości kary miało również to, że administrator nie miał wiedzy o przetwarzaniu danych osobowych na prywatnym komputerze pracownika, a także nie kontrolował procesu przetwarzania danych poprzez brak weryfikacji na jakich nośnikach są przetwarzane dane osobowe kandydatów na studia pobierane z systemu informatycznego oraz brak rejestrowania tej operacji w systemie informatycznym. Powyższe okoliczności świadczą o naruszeniu zasady poufności i rozliczalności określonej w RODO. Ponadto w wyniku przeprowadzonego postępowania ustalono, że uczelnia nie wdrożyła odpowiednich środków organizacyjnych i technicznych, które pozwalają na zapewnienie bezpieczeństwa przetwarzania danych osobowych kandydatów na studia. Ponadto powinny być one na bieżąco poddawane przeglądom i uaktualniane do obowiązujących przepisów i zmieniającej się technologii. W ocenie organu nadzorczego zastosowane przez uczelnię środki obejmujące proces przetwarzania danych kandydatów na studia były niewystarczające. Jednocześnie Prezes UODO stwierdził, że w przedmiotowej sprawie IOD wypełniał swoje zadania bez należytego uwzględnienia ryzyka związanego

346 https://www.nik.gov.pl/aktualnosci/rodo-w-urzedach-miast.html, dostęp z dnia 23.02.2020

z operacjami przetwarzania. Powołany inspektor ochrony danych nie był angażowany przez uczelnię w proces rekrutacji na studia obejmujący funkcjonowanie systemu informatycznego przeznaczonego do tego działania [347]. Włączenie inspektora mogłoby obniżyć ryzyko niewłaściwego przetwarzania danych, nie wspominając o konieczności przeprowadzania regularnych działań monitorujących, o których mowa powyżej.

Powyższe potwierdza również kolejna kontrola Prezesa UODO będąca efektem naruszenia ochrony danych, w wyniku którego nieuprawniona osoba uzyskała dane klientów z jednej z baz operatora telekomunikacyjnego, co skończyło się nałożeniem kary w wysokości 1,9 mln złotych. UODO w toku postępowania nie zgodził się z administratorem, który utrzymywał, że testował i monitorował zastosowane środki techniczne, jak i organizacyjne mające zapewnić bezpieczeństwo danych osobowych. Organ nadzoru uznał, że te działania nie były ani regularne, ani kompleksowe, gdyż były podejmowane incydentalnie i nie obejmowały wszystkich systemów, w których przetwarzane są dane. W toku postepowania okazało się, że wymiana danych między aplikacjami w systemie informatycznym miała następować po zweryfikowaniu pewnych parametrów z wniosków rejestracyjnych klientów usług prepaid. Chodziło o to, by program sprawdził, czy żądanie, w wyniku którego miały być przekazane dane, wpłynęło od uprawnionego podmiotu. W praktyce ta weryfikacja nie działała, a przed jej wdrożeniem mechanizm ten nie został przetestowany. Tymczasem podatność w tym procesie (polegająca na braku weryfikacji odpowiednich parametrów) wykorzystała osoba nieuprawniona, by pozyskać dane. Dopiero po tym incydencie podjęto odpowiednie działania związane z naprawą wspomnianej funkcjonalności w systemie informatycznym spółki. Organ nadzoru uznał, że wdrożenie systemu służącego do przetwarzania danych do użytku bez poprawnie działającej walidacji zakładanych parametrów jest rażącym naruszeniem administratora. UODO nakładając karę wziął pod uwagę, że naruszenie do którego doszło u operatora ma poważny charakter, gdyż stwarza wysokie ryzyko negatywnych skutków ochrony prawnej dla dużej liczby osób (np. ryzyko kradzieży tożsamości). Pomimo, iż osoby nieuprawnione miały krótkotrwały dostęp do systemów, ale wystarczający aby pobrać dużą liczbę danych. Ponadto sam stan naruszenia był długotrwały – podatność zagrożenia wyciekiem danych istniała od dawna. Urząd wziął pod uwagę również okoliczności łagodzące, jak np. dobrą współpracę administratora, szybkie usunięcie naruszenia po jego wykryciu, ale i wdrożenie dodatkowych rozwiązań, które mają dodatkowo podnieść bezpieczeństwo przetwarzanych danych. Biorąc jednak pod uwagę skalę naruszeń i ich wagę UODO uznał, że

347 https://uodo.gov.pl/pl/138/1711 dostęp z dnia 23.02.2020 r.

zastosowanie innych środków naprawczych niż administracyjnej kary pieniężnej byłoby nieproporcjonalne [348].

Na koniec należy również podkreślić, iż w wyniku kontroli NIK w zakresie ochrony danych osobowych w szpitalach zmiana w podejściu do ochrony danych osobowych i prywatności pacjentów jest nie tylko konieczna, ale i pilna. Jak wykazała bowiem kontrola rutyna i utarte schematy działania gubią personel szpitali, zobowiązany do dbałości o bezpieczeństwo danych osobowych i medycznych pacjentów. Tylko pojedyncze ze skontrolowanych szpitali wprowadziły rozwiązania, które stwarzały warunki do odpowiedniego przechowywania papierowej dokumentacji medycznej oraz gwarantowały prawo pacjentów do prywatności w trakcie rejestracji lub na salach szpitalnych. W pozostałych placówkach nie zapewniono skutecznej ochrony danych osobowych i medycznych przed ujawnieniem osobom nieupoważnionym. W ponad połowie skontrolowanych szpitali doszło do naruszeń ochrony danych osobowych, z czego w sześciu sytuacja była na tyle poważna, że konieczne było powiadomienie Prezesa Urzędu Ochrony Danych Osobowych [349].

Mając powyższe na uwadze należy wysunąć jednoznaczny wniosek, iż rola fachowego IOD dla podmiotów przetwarzających dane osobowe stała się kluczowa, celem bezpiecznego i zgodnego z przepisami przetwarzania danych osobowych, a realizacja systematycznych audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych wręcz nieodzowna.

Rozdział IV. Działania doradcze IOD w wybranych obszarach, a także dobre praktyki związane z identyfikacją, przeglądem zagrożeń i naruszeń danych osobowych

IOD został przyznany szczególny status osoby, która w warunkach niezależności, wolna od konfliktu interesów, posiadająca odpowiednią wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych, wykonuje zadania określone w art. 39 ust. 1 RODO [350].

Rozpoczynając rozważania na wstępie należy zaznaczyć, że czynności doradcze IOD są jednymi z fundamentalnych i kluczowych zadań z punktu widzenia organizacji wspomagających funkcjonowanie administratora i wszystkich jego pracowników. Jak wspomniano w I rozdziale niniejszej pracy zadania te zostały znacznie rozbudowane

348 https://uodo.gov.pl/pl/138/1791, dostęp z dnia 18.12.2020 r.

349 https://www.nik.gov.pl/aktualnosci/rodo-w-szpitalu.html, dostęp z dnia 23.02.2020 r.

350 M. Sakowska-Baryła, *Ochrona danych osobowych w warunkach pracy zdalnej,* WKP 2020, str. 40

w stosunku do poprzednika IOD, którego zadaniem było zapewnianie zapoznania osób upoważnionych do przetwarzania danych z prawem ochrony danych osobowych. Zadania informacyjne i doradcze zostały określone w art. 39 ust 1 RODO, jako:"

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
2) działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym działania monitorujące przestrzeganie RODO i innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, a także audyty."

Zakres zadań, o których mowa powyżej oraz rola IOD w organizacji powodują, że każdorazowo w przypadku zmian mogących wpływać na warunki, zasady, sposób, narzędzia i procesy przetwarzania danych osobowych Inspektor powinien podejmować działania, o których mowa w art. 39 RODO. Jednocześnie – co w świetle art. 5 ust. 2 oraz art. 39 ust. 2 RODO zasługuje na rekomendację – powinien starannie dokumentować podejmowane czynności, aby móc wykazać zgodność działań administratora z RODO oraz wykonywanie swoich zadań z należytą starannością i uwzględnieniem ryzyka [351].

Nie sposób nie wspomnieć również o art. 38 RODO, który stanowi, iż administrator oraz podmiot przetwarzający zapewniają, "by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych", co wiąże się bezpośrednio ze sprawną i zgodną z prawem realizacją zadań przez IOD, o czym była mowa szczegółowo w rozdziale 2 niniejszej pracy. Zatem do wszystkich spraw związanych z zatrudnieniem, w tym organizacją pracy zdalnej oraz wprowadzenia przez pracodawcę zasad funkcjonowania wszelkich form monitoringu, jak również udział w procesach udostępniania i powierzenia danych do przetwarzania, m.in. poprzez udział w czynnościach związanych z udzielaniem zamówień publicznych ADO powinien bezzwłoczne angażować IOD.

351 M. Sakowska-Baryła, *Ochrona danych osobowych w warunkach pracy zdalnej, op. cit.*, str.40

IV.1.1. Wybrane działania doradcze w obszarze zatrudnienia dotyczące pracy zdalnej

Pandemia spowodowana rozprzestrzenianiem się koronawirusa Covid-19 stała się przyczyną rozwoju i wdrożenia pracy zdalnej zarówno w przedsiębiorstwach prywatnych, jak również w administracji publicznej. Pandemia COVID-19 sprowokowała zarówno Urząd Ochrony Danych Osobowych, jak i Europejską Agencję Bezpieczeństwa Sieci i Informacji do wydania wytycznych w związku z pracą zdalną. Okoliczności te zostały zidentyfikowane jako podwyższające ryzyko naruszenia przepisów RODO [352].

Praktyka pokazuje, że wielu administratorów wcześniej – jeszcze przed pandemią koronawirusa – przewidywało wykonywanie pracy poza siedzibą pracodawcy w związku z telepracą bądź też w związku z regulowaniem zagadnień dotyczących z pracy z wykorzystaniem urządzeń mobilnych [353]. Taka praktyka funkcjonowała w szczególności w sektorze prywatnym.

Ten szczególny czas jest okazją do zrewidowania dotychczasowych procedur zapewniania ciągłości działania, ich poprawienia, a także aktualizacji. I tutaj kluczowa jest rola doradcza IOD w tym zakresie. Nowe wyzwania powinny także skłaniać inspektorów ochrony danych do wspierania administratorów poprzez proponowanie odpowiednich procedur postępowania, mających na celu rozwiązywanie bieżących problemów [354]. Przetwarzanie danych osobowych w warunkach pracy zdalnej powinno stać się także przedmiotem działań i analiz IOD – mając na uwadze zmiany organizacji pracy mogące wpływać na warunki, zasady, sposób, narzędzia i procesy przetwarzania danych osobowych oraz związane z tym ryzyka.

IOD powinien dokonać analizy obowiązujących w tym zakresie polityk i procedur wewnętrznych oraz udzielić niezbędnych wskazówek i wytycznych w celu dostosowania ich do obowiązujących przepisów dotyczących planowania, wykonywania i raportowania pracy zdalnej, a także w zakresie zapewnienia warunków wykonywania przez pracowników pracy zdalnej i zapewnienia bezpieczeństwa jej świadczenia adekwatnie do zagrożeń. Niezwykle istotne jest również monitorowanie zapoznania się pracowników z warunkami i zasadami wykonywania pracy zdalnej oraz z istniejącymi zagrożeniami w tym zakresie.

352 M. Krzyszkowska-Dąbrowska, *Praca zdalna. Praktyczny przewodnik,* WKP 2020 dostęp z dnia 11.03.2021 r.

353 M. Sakowska-Baryła, *Ochrona danych osobowych w warunkach pracy zdalnej, op. cit.*, str. 35

354 S. Czub-Kiełczewska, *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej*, Lex/el. 2020, dostęp z dnia 11.03.2021 r.

Pandemia spowodowała wprowadzenie pewnych rozwiązań na poziomie ustawowym dotyczącym pracy zdalnej. Od marca 2020 r. w celu przeciwdziałania COVID-19 pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania (praca zdalna) [355]. I tak zgodnie z art. 3 ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych [356] (zwanej dalej u.s.r.z.z) ustawodawca dopuścił możliwość polecenia pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę, poza miejscem jej stałego wykonywania w celu przeciwdziałania COVID-19. Powyższy przepis ma zastosowanie w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie 3 miesięcy po ich odwołaniu. Jednakże Pracodawca może w każdym czasie cofnąć polecenie wykonywania *pracy zdalnej*. Został więc wydłużony okres, przez który praca zdalna może być polecana. Początkowo było to 180 dni od dnia wejścia w życie u.s.r.z.z., tj. do 4 września 2020 r. Pojawiła się również propozycja nowelizacji Kodeksu pracy, która pozwoli na stałe wprowadzić instytucję pracy zdalnej do naszego systemu prawnego [357]. Ponadto w art. 3 ust. 3 ww. przepisu określono, że wykonywanie *pracy zdalnej* może zostać polecone, jeżeli pracownik ma umiejętności i możliwości techniczne oraz lokalowe do wykonywania takiej pracy i pozwala na to rodzaj pracy. Narzędzia i materiały potrzebne do wykonywania *pracy zdalnej* oraz obsługę logistyczną *pracy zdalnej* zapewnia pracodawca.

Z przepisu art. 94 pkt 1 i 2 k.p. wynika niewątpliwie obowiązek zarządzania pracą leżący po stronie pracodawcy. Do organizacji pracy w powyższym kontekście w szczególności odnosi się również art. 104^1 § 1 pkt 1 k.p. Przy czym – jak wynika z orzeczeń Sądu Najwyższego – powinność zaznajomienia pracowników podejmujących pracę z zakresem ich obowiązków oraz sposobem wykonywania pracy na wyznaczonych stanowiskach, może być zrealizowana także ustnie z uwzględnieniem charakteru pracy i skali jej złożoności, wykształcenia i doświadczenia zawodowego pracownika i nie może zostać wykonana poprzez odwołanie regulaminu pracy do regulaminów, instrukcji i przepisów obowiązujących na stanowisku pracownika. Oznacza to, że pracodawca powinien zapewnić pracownikom zdalnym

355 J. Marciniak, *Praca zdalna,* Lex/el. 2020, dostęp z dnia 11.03.2021 r.

356 Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych - Dz. U. z 2020 r., poz. 1842 t. j., z późn.zm.

357 J. Marciniak, *Praca zdalna,* Lex/el. 2020, dostęp z dnia 11.03.2021 r.

należyty instruktaż dotyczący pracy na danym stanowisku adekwatny do stopnia trudności wykonywanych zadań, podobnie jak pracownikom „stacjonarnym". Do podmiotu zatrudniającego należy wybór środka umożliwiającego realizację tego celu [358]. Przepis nie określa sposobu, czy też kryteriów, na podstawie których pracodawca miałby zweryfikować warunki lokalowe pracownika, czy też możliwości techniczne jakimi dysponuje. Można więc przyjąć, że jeżeli pracownik złoży oświadczenie, iż nie ma warunków do pracy zdalnej, to prawo pracodawcy do wprowadzenia pracy zdalnej zostanie ograniczone [359].

W szczególności *praca zdalna* może być wykonywana przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość lub dotyczyć wykonywania części wytwórczych lub usług materialnych. Ponieważ ustawa nie precyzuje, jakie umiejętności powinien posiadać zatrudniony, aby pracować zdalnie to do pracodawcy należy ocena, czy dany pracownik posiada odpowiednie cechy, wiedzę i umiejętności, które pozwolą mu efektywnie wykonywać czynności zawodowe w formule zdalnej. Należy przyjąć, że nie chodzi o jakąś dodatkową, specjalną, ocenę dokonywaną pod kątem pracy zdalnej, ale o np. o analizę kompetencji pracownika dokonywaną na podstawie informacji zebranych już wcześniej przez pracodawcę. W szczególności praca zdalna może być wykonywana przy wykorzystaniu środków bezpośredniego porozumiewania się na odległość lub dotyczyć wykonywania części wytwórczych lub usług materialnych. Wspomniane wykonywanie „części wytwórczych", czy też świadczenie usług materialnych, może oznaczać pracę na dokumentach, przygotowywanie dokumentów, czy grafik, ale również analiz (w tym analizy i obróbkę danych dotyczącą konkretnego procesu), weryfikację informacji, kontakty z klientami i współpracownikami itp. Jest to również związane z bardzo szerokim pojęciem "usług", którą można określić jako dowolne działanie, jakie jedna strona może zaoferować innej. Dla pracy zdalnej jest charakterystyczne celowe (kontekst epidemii) wykonywanie zlecanych przez pracodawcę czynności poza siedzibą firmy i wykorzystywanie zarówno do kontaktów z pracodawcą, jak i do poszczególnych czynności w procesie pracy informatycznych, elektronicznych form łączności i komunikacji. Istnieje również wyraźny związek przedmiotu pracy z informacją jako ważnym elementem działania (to nie występuje zawsze np. może być to wykonywanie projektów, ale tak czy inaczej przetwarzanie informacji w jakiejś formie dominuje). Ustawodawca dopuścił również możliwość używania narzędzi lub materiałów niezapewnionych przez pracodawcę do wykonywania pracy zdalnej pod warunkiem,

358 M. Krzyszkowska-Dąbrowska, *Praca zdalna. Praktyczny przewodnik,* op. cit.

359 J. Marciniak, *Praca zdalna, op. cit.*

że umożliwia to poszanowanie i ochronę informacji poufnych i innych tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa lub danych osobowych, a także informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę [360].

Należy nadmienić, że do podstawowych obowiązków pracownika należy sumienne i staranne wykonywanie pracy oraz stosowanie się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa lub umową o pracę (art. 100 § 1 k.p.). Inne zobowiązania nałożone ustawowo na osobę zatrudnioną dotyczą m.in. przestrzegania czasu pracy ustalonego w zakładzie pracy, przestrzegania regulaminu pracy i ustalonego w zakładzie pracy porządku, przestrzegania przepisów oraz zasad bhp, a także przepisów przeciwpożarowych, dbania o dobro pracodawcy, ochrony jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie narazić mogłoby go na szkodę, przestrzegania tajemnicy określonej w odrębnych przepisach, a także przestrzegania w zakładzie pracy zasad współżycia społecznego. Wszystkie wskazane powyżej obowiązki będą aktualizować się podczas pracy zdalnej [361]. Tak więc, nie ma przeszkód aby firma porozumiała się z pracownikiem, że np. w domu pracuje on na prywatnym sprzęcie komputerowym (oczywiście jeśli jest to możliwe z uwagi np. na dostęp do wewnętrznej sieci elektronicznej pracodawcy). Samo polecenie pracy zdalnej nie zwalnia pracodawcy z obowiązku dbania o zdrowie i życie zatrudnionych oraz zapewnienia bezpiecznych i higienicznych warunków pracy. Jeśli firma zleca danej osobie pracę z domu, to powinna poinformować ją o konieczności przestrzegania zasad bhp, zgłaszania nieprzewidzianych zdarzeń, pozostawania w kontakcie z pracodawcą i do jego dyspozycji. Jeśli w trakcie pracy zdalnej dojdzie do wypadku, to będzie on kwalifikowany jako wypadek przy pracy [362].

Istotą jest, by dokumentacja pracy zdalnej tworzona przez pracodawcę odpowiadała przepisom prawa, ale i zabezpieczała interesy tegoż pracodawcy, jego pracowników oraz wielu grup podmiotowych, które z mocy przepisów prawa mają wiele uprawnień i gwarancji, które pracodawca zmuszony jest respektować. Interesy pracodawcy w przypadku pracy zdalnej można rozważać w różnych aspektach, jednak w kontekście ochrony danych osobowych warto zwrócić uwagę na konieczność realizacji zasad rozliczalności przetwarzania określonych w art. 5 RODO, które z kolei znajdują odzwierciedlenie zarówno w przepisach określających przesłanki dopuszczalności przetwarzania danych osobowych, a więc w art. 6 i 9 RODO, jak

360 J. Marciniak, *Praca zdalna,* op. cit.

361 M. Krzyszkowska-Dąbrowska, *Praca zdalna. Praktyczny przewodnik, op. cit.*

362 J. Marciniak, *Praca zdalna, op. cit.*

i w wymogach dotyczących bezpieczeństwa danych osobowych, uwzględniania ryzyka naruszeń praw lub wolności osób fizycznych, konieczności dokumentowania przetwarzania danych osobowych w odpowiednich politykach, rejestrach, umowach, dokumentacji związanej z naruszeniami. Kolejnym aspektem jest zabezpieczenie przed odpowiedzialnością administracyjną (uprawnienia naprawcze, w tym administracyjne kary pieniężne orzekane przez organ nadzorczy – Prezesa UODO), przed odpowiedzialnością względem osób, których dane dotyczą oraz przed sporami prawno-pracowniczymi lub roszczeniami pracowników. Istotna jest również realizacja obowiązków pracodawcy w zakresie BHP oraz dotyczących niedyskryminacyjnego traktowania (np. ze względu na kompetencje lub ich brak, możliwości techniczne – sprzętowe, lokalowe, sieciowe), a także w zakresie poszanowania godności i dóbr osobistych pracowników (zgodnie z art. 11^1 k.p.). Należy również zwrócić uwagę na bezpieczeństwo finansowe pracodawcy. Dokumentowanie pracy zdalnej i posługiwanie się przez pracodawcę stosownymi procedurami przekłada się również na respektowanie interesów pracowników i innych osób w następującym zakresie: poszanowanie dóbr osobistych pracownika, zapewnienie narzędzi, procedur i wsparcia pracowników wykonujących pracę zdalną, udzielanie wsparcia logistycznego, przeciwdziałanie nieprawidłowym działaniom w sieci, przeciwdziałanie odpowiedzialności pracowników. Dotyczy to również zapewnienia adekwatnego standardu przetwarzania danych osobowych bez względu na to, w jaki sposób, gdzie i za pomocą jakich narzędzi są przetwarzane, a także realizacji praw osób, których dane dotyczą, oraz innych praw i wolności osób fizycznych [363].

W stosunku do pracowników zdalnych – w przeciwieństwie do telepracowników – nie zostały wprost określone obowiązki, tak jak w art. 67^{12} k.p., zgodnie z którymi pracodawca określa zasady ochrony danych przekazywanych telepracownikowi oraz przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie, a z kolei telepracownik potwierdza na piśmie zapoznanie się z zasadami ochrony danych, o których mowa w § 1, oraz jest obowiązany do ich przestrzegania. Nie ma jednak wątpliwości, że tożsame zasady powinny znaleźć zastosowanie w tym przypadku. Zgodnie z wydawanym szeregiem zaleceń Urzędu Ochrony Danych Osobowych pracodawcy jako administratorzy danych przetwarzanych przez pracowników podczas pracy zdalnej mają obowiązek zapewnić przestrzeganie zasad przetwarzania danych, w tym zagwarantować ich bezpieczeństwo, biorąc pod uwagę większe ryzyko związane z takimi działaniami. Odnosi się to zarówno do przetwarzania danych przy wykorzystaniu środków komunikacji elektronicznej, jak i danych zawartych w dokumentach

363 M. Sakowska-Baryła, *Ochrona danych osobowych w warunkach pracy zdalnej*, op. cit., str. 33 - 35

papierowych. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych oraz muszą zapewnić ich bezpieczeństwo, przestrzegając wewnętrznych polityk oraz stosując się do innych procedur przyjętych w tym zakresie przez pracodawcę. Na pracownikach spoczywa również ogólny obowiązek dbałości o dobro zakładu pracy w zakresie ochrony danych osobowych [364].

W zasadzie we wszystkich poradnikach dotyczących pracy zdalnej, a także regulaminach opracowywanych dla pracowników pojawia się warunek, że sprzęt służbowy nie może być wykorzystywany do celów prywatnych. Jest to jedna z zasad minimalizujących ryzyko naruszenia poufności, np. poprzez zainstalowanie złośliwego oprogramowania lub przypadkowe usunięcie danych przez domownika, który współdzieli z pracownikiem komputer. Już w pierwszych dniach przestawiania się zakładów pracy na pracę zdalną, okazało się, że wyzwaniem jest zapewnienie pracownikom odpowiednich narzędzi do ich realizowania. Wiele firm w ogóle nie było na to przygotowanych, w efekcie wymagając od pracowników, aby w domu korzystali ze swojego prywatnego komputera. Brak służbowego laptopa oznacza brak służbowego sprzętu. Tymczasem bardzo szybko pojawiły się głosy, że przecież w sytuacji, gdy pracownik musi pracować w domu, a do tej pory pracował na urządzeniu stacjonarnym i nie ma możliwości zapewnienia mu laptopa, można wydać mu do domu komputer stacjonarny. Należy zgodzić się ze stanowiskiem S. Czub-Kiełczewskiej, iż wydanie pracownikowi choćby sprzętu stacjonarnego przez pracodawcę jest o wiele lepsze, niż zmuszanie pracownika do pracy w domu na prywatnym komputerze, który po pierwsze może nie spełniać nawet minimalnych standardów bezpieczeństwa, po drugie jest duże prawdopodobieństwo, że musi być dzielony z dziećmi, które od 25 marca rozpoczęły obowiązkową naukę zdalną. Jeżeli pracodawca nie zapewnił pracownikom służbowego sprzętu, może okazać się, że nie są oni w stanie skutecznie realizować swoich działań, ponieważ muszą udostępnić komputer dzieciom. Nie należy z kolei zgodzić się z twierdzeniem S. Czub-Kiełczewskiej, iż warto zweryfikować z działami kadr, HR oraz IT to ilu pracowników pracujących na prywatnym sprzęcie ma dzieci w wieku szkolnym, bowiem powyższe informacje nie mają wpływu na konieczność zapewnienia sprzętu pracownikowi. Jednocześnie dane dotyczące dzieci pracowników są zbierane w konkretnym celu przewidzianym w przepisach prawa pracy (tj. zgłaszania członków rodziny do ubezpieczenia zdrowotnego, czy korzystanie z ZFŚS), a nie do weryfikacji i zasad przydzielania sprzętu podległym

364 M. Krzyszkowska-Dąbrowska, *Praca zdalna. Praktyczny przewodnik, op. cit.*

pracownikom. Takie przekazanie powinno odbyć się za pokwitowaniem w formie pisemnej lub elektronicznej (np. podpisanego przez pracownika skanu protokołu przekazania sprzętu) [365].

Mając powyższe na uwadze IOD powinien dokonać weryfikacji, czy umowy o odpowiedzialności materialnej za powierzone mienie zawierają wymagane postanowienia dotyczące zasad bezpiecznego użytkowania sprzętu (bez względu na rodzaj sprzętu, tj. laptop, modem, router, czy karta SIM), a także odpowiedzialności za sprzęt i dane na nim zawarte zgodnie ze wzorem wynikającym z obowiązującej w jednostce Polityki Bezpieczeństwa Informacji. Umowy powierzenia mienia powinny być zawierane na bieżąco z pracownikami jednostki bez względu na rodzaj sprzętu powierzanego pracownikowi, co zapewnia realizację rozliczalności wynikającej z RODO, bieżącą inwentaryzację mienia firmy/instytucji, a także realizację przez pracodawcę wymogu ustawowego dotyczącego dostarczenia pracownikowi narzędzi i materiałów potrzebnych do wykonywania pracy zdalnej.

W przypadku realizacji przez pracownika zadań przy użyciu sprzętu prywatnego obowiązkiem pracodawcy, jako ADO jest zapewnienie odpowiednich środków technicznych i organizacyjnych dla ochrony danych. Wynika to wprost z przepisów art. 24 i 32 RODO i nie można tego obowiązku przerzucić na osoby przetwarzające dane z upoważnienia administratora. Jeżeli pracodawca nie jest w stanie zapewnić pracownikom służbowego sprzętu, troszcząc się o ciągłość własnego biznesu, powinien zapewnić przynajmniej odpowiednie środki ochrony prywatnego sprzętu. Należy przy tym zgodzić się ze stanowiskiem S. Czub-Kiełczewskiej, która uważa, że należy dopuścić możliwość realizowania pracy zdalnej z wykorzystaniem prywatnych komputerów, jednakże przy wsparciu działów informatyki, np. poprzez możliwość połączenia się zdalnie z komputerem pracownika, by sprawdzić oprogramowanie, doinstalować niezbędne aplikacje, sprawdzić i poprawnie skonfigurować ustawienia antywirusa, zapory i aktualizacji systemu. To bardzo ważne, aby nie ignorować problemów i zapewnić odpowiednie wsparcie. Należy zgodzić się z twierdzeniem S. Czub-Kiełczewskiej, iż o ile zakup sprzętu komputerowego dla pracownika dla większości pracodawców może być teraz wyzwaniem, szczególnie że są to wydatki w tysiącach złotych, to zapewnienie dostępu do Internetu, nie jest już tak wysokim kosztem, a może istotnie zwiększyć nie tylko efektywność, ale też bezpieczeństwo pracy. Korzystanie z ogólnodostępnych sieci WiFi lub współdzielenie Internetu z domownikami w ramach sieci domowej stanowi zagrożenie dla bezpieczeństwa przetwarzanych informacji. Problem ten można rozwiązać przekazując pracownikom modemy/routery wraz z kartami SIM

365 S. Czub-Kiełczewska, *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej,* op.cit.

umożliwiającymi korzystanie z Internetu, ale także uświadamiając pracowników, że większość ich telefonów także daje możliwość udostępnienia Internetu w ramach funkcji HotSpot. Jest to jedno z najtańszych i najprostszych rozwiązań zwiększających bezpieczeństwo pracy zdalnej. Inspektor ochrony danych we współpracy z informatykiem może opracować prostą instrukcję, jak uruchomić funkcję HotSpot w telefonie i korzystać z tak udostępnionego Internetu na komputerze wykorzystywanym do pracy zdalnej. Pracodawca może, w miarę zapotrzebowania, zwiększyć pakiety przesyłu danych dla poszczególnych kart SIM. To rozwiązanie odciąży także domowe sieci internetowe, które powinny również posiadać hasło do routera, co zwiększy efektywność pracy pracownika [366]. Przenoszenie firmowych danych na prywatne komputery i urządzenia mobilne powinno być zabronione. Dyski, karty pamięci oraz pozostałe elektroniczne nośniki danych muszą zostać zaszyfrowane. Pracownicy powinni posługiwać się silnymi hasłami oraz używać wielopoziomowego uwierzytelniania, co pozwoli ograniczyć dostęp do urządzenia oraz ryzyko utraty danych w przypadku jego zgubienia lub kradzieży. Należy używać wyłącznie zaufanego dostępu do sieci lub chmury i unikać otwartych sieci publicznych [367]. Niezwykle istotnym elementem w przyjętym modelu BYOD jest zabezpieczenie narzędzia przed atakami, czy też stosowanie zabezpieczeń organizacyjnych poprzez wymuszenie łączenia się z infrastrukturą pracodawcy przez bezpieczne łącze (VPN).

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) zaleciła wprowadzenie określonych zasad oraz wydała przewodnik zawierający podstawowe wskazówki mogące zmniejszyć ryzyka („cyber hygiene tips") dla pracodawców i pracowników. Dodatkowo, w jej wytycznych szczególny nacisk został położony na ustalenie zakazu instalowania przez pracowników aplikacji i oprogramowań na urządzeniach służbowych, nakazu korzystania przez nich z określonych programów antywirusowych, ostrzeżenia pracujących zdalnie przed możliwością ataków hakerskich i tzw. phishingiem, czy przekazywaniem poufnych danych, a także określenie obowiązku zabezpieczenia silnym hasłem prywatnych sieci internetowych używanych w celach służbowych, szyfrowanie przesyłanych wiadomości poczty elektronicznej, oraz zakaz korzystania z prywatnych skrzynek dla celów służbowych lub przesyłania tam materiałów. Zalecane jest także korzystanie z VPN. Znaczenie mogą mieć również takie działania jak odpowiednia weryfikacja tożsamości uczestników telekonferencji czy wideokonferencji. Szczególnie ostrożnie powinno się, zgodnie z przedmiotowymi

366 S. Czub-Kiełczewska, *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej*, op. cit.

367 Jagiełło-Jaroszewska E., *Ochrona danych osobowych a telepraca i praca zdalna* [w:] D. Dörre-Kolasa (red.), *Ochrona danych osobowych w zatrudnieniu*, C.H. Beck, Warszawa 2020 r., str. 224

wskazówkami, zabezpieczać zewnętrzne nośniki danych. Przeprowadzanie szkoleń i utrzymywanie właściwych zasobów technicznych jest również rekomendowane [368].

Kolejnym tematem, dość często omijanym szerokim łukiem przez specjalistów, jest konieczność pracy zdalnej z wykorzystaniem dokumentów papierowych zabranych z biura pracodawcy. Są zawody i specjalizacje, których praca w dużej mierze opiera się na analizie dokumentów i bez nich, nie mają możliwości świadczenia pracy z domu. Zdaniem S. Czub Kiełczewskiej wielu administratorów danych wprowadziło bezwzględne zakazy wynoszenia jakichkolwiek dokumentów do domu, [369] co należy ocenić pozytywnie. Polecenie wykonywania pracy zdalnej może dotyczyć tylko określonych dni tygodnia (tzw. model hybrydowy), analogicznie jak dopuszczalna jest telepraca wykonywana w wybrane dni tygodnia lub też niektóre tygodnie, przeplatane pracą świadczoną fizycznie w zakładzie pracy [370].

Mając powyższe na uwadze oraz odpowiedni system zastępstw wprowadzony zakaz wynoszenia jakichkolwiek dokumentów do domu wydaje się być w pełni zasadnym rozwiązaniem, a dopuszczanie wynoszenia jakiejkolwiek dokumentacji poza siedzibę pracodawcy wiązać się może z ryzykiem jej zagubienia, zniszczenia oraz dostępu osób nieuprawnionych.

IOD powinien również zadbać o sprawną realizację procedur pracy zdalnej oraz poinstruowania pracowników i osoby nadzorujące o konieczności:

- zapewnienia właściwych warunków umożliwiających pracownikowi skuteczną pracę zdalną z zachowaniem właściwego poziomu bezpieczeństwa informacji oraz by domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera oraz innych urządzeń mobilnych
- zakazie wynoszenia jakichkolwiek dokumentów do domu, a w szczególnych wypadkach zapewnienia pracy z dokumentami w sposób uniemożliwiający wgląd osobom postronnym. Szczególnie istotne jest aby pracownik otrzymał kopie, a nie oryginały dokumentów, za zgodą bezpośredniego przełożonego, co minimalizuje ryzyka związane z ich utratą, a także zapewnienie, że wszystkie kopie zostaną zwrócone po zakończeniu pracy osobie odpowiedzialnej, co zapewnia zachowanie zasady rozliczalności. Jednakże w tej sytuacji z uwagi na ryzyko zagubienia, zniszczenia oraz dostępu osób nieuprawnionych do

368 M. Krzyszkowska-Dąbrowska, *Praca zdalna. Praktyczny przewodnik, op. cit.*

369 S. Czub-Kiełczewska, *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej*, op. cit.

370 J. Marciniak, *Praca zdalna, op. cit.*

dokumentów najbardziej zasadnym rozwiązaniem wydaje się być skanowanie dokumentacji i jej udostępnianie po zaszyfrowaniu bezpiecznym kanałem przy użyciu VPN oraz wdrożenie adekwatnie do sytuacji odpowiedniego systemu zastępstw,

- realizacji pracy zdalnej z zachowaniem zasady, iż niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy,
- wykonywania pracy zdalnej zgodnie z harmonogramem ustalonym z pracodawcą, co oznacza, że pracownik jest dostępny i realizuje swoje działania w ustalonych godzinach (zgodnie z wymogami ustawy pracownik ma obowiązek prowadzić ewidencję wykonanych czynności, uwzględniającą w szczególności opis tych czynności, a także datę oraz czas ich wykonania (zgodnie z przyjętym wzorem karty czasu pracy zdalnej),
- zapewnienia, że pracownik odchodząc od komputera lub kończąc korzystanie ze służbowego sprzętu upewnił się, że urządzenie zostało zablokowane. Należy zgodzić się z S. Czub - Kiełczewską, iż bardzo ważnym elementem jest również zapewnienie przestrzegania zasad bezpieczeństwa w przypadku przesyłania danych oraz zasad postępowania z incydentami i zachowanie zasad ostrożności w przypadku otrzymywania wiadomości z nieznanego źródła oraz zawierających podejrzane linki (malware, phishing). W dobie elektronizacji i konieczności przekazywania danych osobowych środkami komunikacji elektronicznej niezbędne jest zapewnienie użytkownikom odpowiednich narzędzi, umożliwiających im zabezpieczenie danych (np. narzędzie kompresujące pliki do zabezpieczonego hasłem archiwum), a także napisanych w przystępny sposób zasad korzystania z poczty elektronicznej [371]. Powyższe zasady powinny zostać udokumentowane w postaci oświadczeń o zapoznaniu się z zasadami wykonywania pracy zdalnej oraz zachowania poufności przez pracowników, które powinny się znaleźć w aktach osobowych przed rozpoczęciem świadczenia pracy zdalnej przez pracownika. Mając powyższe na uwadze IOD wykonując czynności audytowe powinien dokonać weryfikacji zasad wykonywania pracy zdalnej wynikających z PBI i tarczy 4.0 oraz przeprowadzić wywiady z osobami funkcyjnymi w zakresie sposobu planowania pracy zdalnej, zabezpieczenia wykonania bieżących zadań, w tym zastępowalności w miejscu wykonywania pracy, a także realizacji i raportowania wykonanej pracy. IOD powinien również sprawdzić zasady zgłaszania nieprawidłowości i wszelkich awarii (sprzętu, braku zasilania, Internetu itp.) zgodnie z zasadami przyjętymi u danego pracodawcy.

371 S. Czub-Kiełczewska, *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej*, op. cit.

Jeżeli chodzi o kwestię dokumentowania wykonywania pracy zdalnej to w art. 3 ust 6 u.s.r.z.z. wskazano, że pracownik wykonujący *pracę zdalną* na polecenie pracodawcy ma obowiązek prowadzić ewidencję wykonanych czynności w formie i z częstotliwością określoną w poleceniu, uwzględniającą w szczególności opis tych czynności, a także datę oraz czas ich wykonania.

Warto w tym miejscu zauważyć, że nie chodzi tutaj tylko o biurokratyczny obowiązek. Dzięki takiemu podejściu pracownicy będą rozliczani za swoje wyniki. Będzie miało to wpływ na ich motywację do uzyskiwania określonych rezultatów i zapewni informację zwrotną. Dla pracodawcy są to dowody, że czas zdalnych pracowników był poświęcony faktycznej pracy. Wiarygodna ewidencja ma również istotne znaczenie dla opracowywania i doskonalenia harmonogramów pracy zdalnej w firmie lub instytucji [372].

Z uwagi na powyższe ustalenia dokumentowanie pracy zdalnej pozwala pracodawcy – odpowiedniemu ADO lub podmiotowi przetwarzającemu na gruncie przepisów RODO – osiągnąć takie cele, jak w szczególności zgodność z przepisami prawa, ustalenie zasad wykonywania pracy zdalnej przez pracowników oraz zapewnienie organizacji pracy zespołu podczas pracy zdalnej i rozliczalności na gruncie RODO. Nie sposób tutaj nie wspomnieć o ustaleniu spójnych reguł bezpieczeństwa, zapewnieniu przez pracodawcę wsparcia dla personelu pracującego zdalnie, przeciwdziałaniu odpowiedzialności prawnej, ewolucji procesów organizacyjnych, czy racjonalizacji i dokumentowaniu wydatków [373]. Na koniec należy pomyśleć o zapewnieniu poufności danych przetwarzanych na prywatnych urządzeniach oraz możliwość wykorzystywania prywatnego numeru telefonu pracownika do kontaktów służbowych. Odnośnie bezpieczeństwa, należy przyjąć dokładnie te same standardy, jak w przypadku służbowego komputera. Z kolei w przypadku wykorzystania prywatnego numeru telefonu pracownika do celów służbowych to należy zaznaczyć, że kodeks pracy nie wskazuje prywatnego adresu poczty elektronicznej i numeru prywatnego telefonu jako danych, których pracodawca ma prawo żądać od pracownika. W polskim systemie prawnym nie istnieje też żaden przepis, który zobowiązywałby osobę fizyczną do posiadania takich środków komunikacji. Dysponowanie adresem poczty elektronicznej i telefonem jest i powinno pozostać dobrowolne. Żeby pracodawca mógł przetwarzać w celach zawodowych dane kontaktowe do pracownika, które pozyskał podczas rekrutacji, takie jak np. adres prywatnej poczty elektronicznej czy numer prywatnego telefonu komórkowego, musi uzyskać na to jego

372 J. Marciniak, *Praca zdalna, op. cit.*

373 M. Sakowska-Baryła, Ochrona danych osobowych w warunkach pracy zdalnej, op. cit., str. 36

zgodę (pisemną, określająca zasady kontaktu) [374]. Tu również IOD powinien zająć odpowiednie stanowisko i zaproponować ADO alternatywne rozwiązania, jak zakupienie dla pracowników kart SIM, tak jak w przypadku zapewnienia pracownikom dostępu do internetu.

IV.1.2. Wybrane działania doradcze w obszarze zatrudnienia dotyczące stosowania monitoringu wizyjnego

Stosowanie monitoringu wizyjnego jako formy nadzoru nad osobami niewątpliwie wiąże się z przetwarzaniem danych osobowych wszystkich obserwowanych osób [375].

Nie ulega wątpliwości, że wykorzystywanie nowych technologii, przejawiające się w stosowaniu technik nadzoru i kontroli, w żadnym razie nie omija środowiska pracy. Jedną z nich, zyskującą na coraz większym znaczeniu, jest monitoring pracowników. Oprócz monitoringu wizyjnego, który jest najbardziej oczywistą formą monitorowania pracy, w miejscu pracy mogą być stosowane inne sposoby kontrolowania pracowników. Do metod kontroli należą: monitorowanie aktywności pracowników w Internecie, sprawdzanie służbowych skrzynek e-mailowych i logów internetowych, przeglądanie korespondencji służbowej pracownika, sprawdzanie wykazów połączeń wykonanych za pomocą telefonu służbowego, instalacja rejestratorów GPS w samochodach czy analiza urządzeń GSM rejestrujących pozycję telefonu, ewidencja czasu pracy przy wykorzystaniu danych biometrycznych [376]. Naczelny Sąd Administracyjny w wyroku z dnia 1 grudnia 2009 r. (sygn. I OSK 249/09) wskazał na brak równowagi w relacji pracodawca pracownik, co stawia pod znakiem zapytania dobrowolność wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22 Kodeksu Pracy katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody, jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22 Kodeksu pracy, stanowiłoby obejście tego przepisu. Sąd zaznaczył również, że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności, jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest

374 https://uodo.gov.pl/pl/138/1636, dostęp z dnia 23.02.2021 r.

375 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str.274

376 E. Bielak-Jomaa, M*onitoring pracowników – wybrane zagadnienia* [w:] M. Mędrala (red.) *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami]* WKP, Warszawa 2018, str. 52

nieproporcjonalne do zamierzonego celu ich przetwarzania. Pracodawca może monitorować pocztę elektroniczną swoich pracowników, ale musi pamiętać, że uprawnienie to dotyczy tylko służbowej poczty elektronicznej. Ma takie prawo jeżeli jest to nie-zbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie [377]. Zatem wszystkie wskazane rodzaje monitorowania pracy pracowników stanowią niewątpliwie dużą dolegliwość dla ich prywatności. Wiążą się jednak z realizowaniem prawa pracodawcy do kontrolowania pracownika, które wynika wprost z art. 22 k.p. i polega na obowiązku pracownika wykonywania pracy określonego rodzaju pod kierunkiem pracodawcy. Rzecz jasna, kierowanie pracą pracownika i, co za tym idzie, jego kontrolowanie, może odbywać się wyłącznie w granicach prawa i przy uwzględnieniu charakteru prawnego oraz celów stosunku pracy i nie może przybierać charakteru władztwa sprawowanego przez pracodawcę nad osobami zatrudnionymi. Biorąc pod uwagę techniczne możliwości stosowania monitoringu, trzeba zauważyć, że pracodawca może monitorować prawie wszystkie działania i zachowania pracowników zarówno w miejscu pracy, jak i poza nim, dlatego tak istotne jest wyznaczenie dopuszczalnych granic monitorowania. W tym zakresie w stosunkach pracy zasadnicze znaczenie będzie więc miało wyważenie sprzecznych interesów i wartości stron stosunku pracy: prawa pracodawcy do kontroli pracownika oraz prawa pracownika do prywatności [378].

Podstawowymi przesłankami wskazującymi na konieczność uregulowania przedmiotowego zagadnienia były częste praktyki prowadzące do naruszenia dóbr osobistych osób obserwowanych, brak zasad określających możliwość prowadzenia monitoringu, spełnienia obowiązku informacyjnego, czy realizacji praw osób, których dane dotyczą [379].

Warto także zauważyć, że technologie monitorujące komunikację mogą mieć również negatywny wpływ na podstawowe prawa pracowników do organizowania się, organizowania spotkań pracowników. Szerokie zastosowanie technologii monitorowania może również ograniczyć gotowość pracowników do informowania pracodawców o nieprawidłowościach lub niezgodnych z prawem działaniach przełożonych lub współpracowników. Monitorowanie naruszające prawa pracowników do prywatności może również zaburzyć relacje przez

377 Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców, październik 2018 r.,* https://uodo.gov.pl/pl/138/545 dostęp z dnia 13.06.2020 r.

378 E. Bielak-Jomaa, M*onitoring pracowników – wybrane zagadnienia* op. cit., str. 52 - 53

379 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, [w:] K. Żarna (red.), Bezpieczeństwo - Prawa człowieka - Stosunki międzynarodowe, t. III, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2021, str. 72

zbudowanie być może mylnego przekonania o obniżeniu zaufania do pracowników, dotychczas niepoddawanych takiej formie kontroli, którzy nie czują się związani z „podglądającym" ich pracodawcą, nie mają potrzeby współdziałania na rzecz rozwoju zakładu pracy, nie wdrażają innowacyjnych pomysłów i rozwiązań dotyczących procesu pracy. Nadmiernie wkraczający w sferę prywatności monitoring może prowadzić do zmiany postaw pracowników, którzy poczują się inwigilowani i stracą zainteresowanie budowaniem relacji z innymi pracownikami, nie będą czuć się częścią załogi, nie będą utożsamiać się więc z miejscem pracy [380].

W doktrynie prawnej panuje dominujący pogląd o celowości poinformowania pracownika o wykorzystaniu narzędzi monitoringu w jego miejscu pracy. Musi on być poinformowany osobiście lub przez wprowadzenie stosownych postanowień wewnątrzzakładowych. Są jednak od tego wyjątki. Doskonałym przykładem jest orzeczenie ETPC z 5.10.2010 r., 420/07, Köpke przeciwko Niemcom, HUDOC. Trybunał orzekł, że pracodawca jest zwolniony z poinformowania pracownika o stosowaniu monitoringu w sytuacji, gdy ma on uzasadnione podejrzenie, że działalność pracownika jest wymierzona w dobro zakładu pracy, a zastosowane środki monitoringu mają na celu wykrycie czynu zabronionego lub zapobieżenie jego skutkom, a cel ten nie może być osiągnięty przy użyciu innych, mniej inwazyjnych metod. Na gruncie prawa polskiego o takiej konieczności wypowiadał się już NSA w wyroku z 13.02.2015 r., I OSK 2436/12, LEX nr 1449889. Naczelny Sąd Administracyjny wskazał, że wymogiem prowadzonej kontroli jest przede wszystkim zgodność określonych działań z literą prawa, uzasadniony cel, transparentność, uwzględnienie przepisów o ochronie danych osobowych. Wyrok ten jednak został wydany przed 25.05.2018 r., czyli przed wejściem w życie RODO i przepisów krajowych [381].

Tutaj należy poddać pod rozwagę często pojawiający się w instytucjach publicznych schemat próby wykorzystania monitoringu do kontroli obecności w pracy podległych pracowników lub weryfikacji przebywania ich poza stanowiskiem pracy, co jest niezgodne z celem, zakresem i sposobem stosowania monitoringu.

Jeśli pracodawca ma uprawnienia kierownicze w stosunkach pracy, to uznać musimy, że uprawnienia te może realizować różnymi dopuszczonymi przez prawo narzędziami, w tym także przy wykorzystaniu rozwiązań technologicznych [382].

380 E. Bielak-Jomaa, M*onitoring pracowników – wybrane zagadnienia*, op. cit., str. 70 - 71

381 M. Jakubik, T. Świętnicki, *Indywidualny monitoring pracownika – zagadnienie monitorowania pracowników i ich danych,* Lex/el. 2020, dostęp z dnia 19.03.2021 r.

382 E. Bielak-Jomaa, M*onitoring pracowników – wybrane zagadnienia,* op. cit., str.70

Brak zasad określających prowadzenie monitoringu, wobec społecznego przyzwolenia na jego stosowanie, przejawiał się dowolnością przyjmowanych rozwiązań w zakresie jego organizacji, rozmieszczenia kamer, czasu przechowywania nagrań, jak również niewypełnianiem obowiązków dotyczących zbioru danych osobowych z monitoringu wizyjnego, określonych w ustawie o ochronie danych osobowych [383]. Niniejsza kwestia na gruncie prawa polskiego, mimo stosownych zabiegów ze strony Rzecznika Praw Obywatelskich czy Generalnego Inspektora Ochrony Danych Osobowych, do 25.05.2018 r. nie była uregulowana. Zgodnie z opinią 4/2004 Grupy Roboczej Art. 29 z 11.02.2004 r. w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer wideo monitorowanie pracowników za pomocą kamer mające na celu sprawdzenie jakości i ilości wykonywanej przez nich pracy uznawano co do zasady za niedopuszczalne. Wyjątek stanowił monitoring pracowników dla celów bezpieczeństwa [384].

Jednak polski ustawodawca w związku z rozpoczęciem bezwzględnego stosowania przepisów RODO – wprowadził niezbędne zmiany dotyczące wykorzystania monitoringu wizyjnego do przepisów sektorowych. Najważniejsze zasady postępowania przy przetwarzaniu danych osobowych, które powinny być przestrzegane podczas przetwarzania danych osobowych w związku z monitoringiem zostały określone w art. 5 RODO to zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność oraz zasada mająca szczególne znaczenie – rozliczalność. Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych wprowadziły zmiany do szeregu regulacji ustawowych w tym zakresie zarówno w sektorze publicznym (przepisy prawa pracy oraz ustaw o samorządzie gminnym, powiatowym, wojewódzkim, itp.), prywatnym, zdrowia, zatrudnienia, szkolnictwa, jak również organów ścigania i sądów. Następnie przepisy te zostały ponownie zaktualizowane [385].

Nie poddając pogłębionej analizie przepisów odnoszących się do monitoringu pracowników, warto odnotować, jakie zagadnienia związane z monitoringiem ustawodawca krajowy postanowił prawnie uregulować. Po pierwsze, trzeba wskazać, że przepisy przewidują możliwość wprowadzenia monitoringu rozumianego jako szczególny nadzór nad terenem

383 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 72

384 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* [w:] M.Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, WKP, Warszawa 2019, str. 274

385 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 73

zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu. Kolejną formą jest monitoring poczty elektronicznej, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. W przepisach kodeksu pracy mowa jest również o innych formach monitoringu (niż monitoring poczty elektronicznej), jeśli ich zastosowanie jest konieczne do realizacji takich celów, jakie określa monitoring poczty elektronicznej [386].

Zakres dopuszczalnego monitoringu pracownika wyznaczają: zasada niezbędności, zasada ochrony godności i dóbr osobistych pracownika oraz zasada wolności i niezależności związków zawodowych. Wskazane zasady są jako takie spójne z zasadami dotyczącymi przetwarzania danych osobowych określonymi w art. 5 w zw. z art. 6 i 9 RODO. W konsekwencji pracodawca, aby wykazać, że przestrzega zasady niezbędności, zobowiązany będzie udowodnić, że wskazanych powyżej celów (tj. zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę) nie był w stanie osiągnąć w inny sposób niż poprzez zastosowanie monitoringu wizyjnego. Okolicznościami, które będą istotne z punktu widzenia tej oceny, są rodzaj pracy, jej charakter i stanowisko zajmowane przez pracownika [387].

Funkcjonowanie monitoringu zwłaszcza wizyjnego w zakładach pracy nie jest niczym nowym i wbrew krążącym opiniom, monitoring stosowany przez pracodawców przed 25 maja 2018 r. nie był nielegalny. Bez wątpienia w zdecydowanie gorszej sytuacji znajdują się pracodawcy uzwiązkowieni, gdyż aby dokonać zmian w regulaminie pracy czy układzie zbiorowym, pracodawców tych czeka proces konsultacji ze stroną związkową [388].

Zgodnie z obowiązującą na gruncie RODO regułą celowości, stosownie do której dane osobowe mogą być zbierane wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nie mogą być dalej przetwarzane w sposób niezgodny z tymi celami (*vide*art. 5 ust. 1 lit. b RODO), nagrania obrazu uzyskane w wyniku stosowania monitoringu wizyjnego pracodawca jest uprawniony wykorzystać wyłącznie do celów, dla których zostały zebrane, a które to w tym przypadku jasno określają przepisy prawa [389].

386 E. Bielak-Jomaa, M*onitoring pracowników – wybrane zagadnienia,* op. cit., str. 71- 72

387 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str. 275

388 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 80

389 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str.277

Administrator powinien być w stanie wykazać proporcjonalność zastosowania monitoringu do celu, w jakim został wprowadzony. Zgodnie z opinią GR Art. 29 (obecnie przekształconej w Europejską Radę Ochrony Danych Osobowych) nr 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video (WP 89) urządzenia monitoringu wizyjnego mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy „inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, niewymagające pozyskiwania obrazu [...], okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami". Pracodawca musi bowiem dokonać oceny stanu bezpieczeństwa w zakładzie i odpowiedzieć w jej wyniku na pytania: czy kamery faktycznie są niezbędne, aby proces pracy przebiegał bezpiecznie? W przypadku, gdy dotychczas stosowane środki bezpieczeństwa okazują się niewystarczające, istnieje podstawa wprowadzenia monitoringu wizyjnego. Jeżeli jednak ocena procesu pracy w kontekście jego bezpieczeństwa nie pozwala na stwierdzenie, że kamery są niezbędne, wówczas instalacja monitoringu wizyjnego może być uznana za nielegalną i niecelową. Monitoring zakładowy niezbędny dla zapewnienia bezpieczeństwa pracy nie powinien być wyłącznie autonomiczną decyzją pracodawcy. Przyjmując, że odnosi się on do szeroko rozumianej kwestii bezpieczeństwa, zamiar jego zainstalowania powinien być przedyskutowany z pracownikami w ramach konsultacji bhp lub komisji bhp. Przepis ten wyraźnie wskazuje na konieczność uzasadnienia stosowania takiego nadzoru [390]. Ze względu na wyjątkowo inwazyjny charakter monitoringu wizyjnego każdy administrator powinien szczególnie wnikliwie dokonać analizy w zakresie potrzeby jego zastosowania, a także dostępnych środków minimalizacji skutków jego wprowadzenia dla praw i wolności pracowników [391]. Stosowanie monitoringu musi być niezbędne, tzn. gdy pracodawca nie może wykorzystać innego, mniej ingerującego w prywatność narzędzia. Urząd Ochrony Danych Osobowych jest uprawniony do analizy podjętej przez pracodawcę decyzji. Warto zauważyć, iż ustawodawca nie precyzuje o ochronę czyjego mienia chodzi w przedmiotowej regulacji. Może to być zarówno mienie należące do pracodawcy, jak również pracowników, klientów, kontrahentów czy osób trzecich przebywających na terenie zakładu pracy. **Dotychczas kontrole PUODO dotyczące monitoringu wizyjnego ujawniły** brak dokonania oceny skutków dla ochrony

390 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 80

391 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str. 279

danych osobowych. Samorządowcom trudność sprawiało także właściwe spełniane obowiązku informacyjnego np. o zasadach prowadzenia monitoringu. Skutkuje to wzrostem skarg kierowanych na sektor samorządu terytorialnego w tym zakresie. Nie sposób nie wspomnieć również o fakcie, iż monitoring uregulowany jest w podstawowym źródle prawa pracy, zatem legalność jego stosowania podlega także kontroli PIP. Przepisy ustawy o PIP dają inspektorom pracy szereg uprawnień, które są niezbędne na potrzeby prowadzenia postępowania kontrolnego, w tym w zakresie weryfikacji stosowania monitoringu wizyjnego w celu zapewnienia bezpieczeństwa pracy [392].

Istotnym jest, aby nie stosować atrap kamer przemysłowych w miejscach, gdzie faktycznie monitoring nie jest wykonywany, może to bowiem wywołać mylne poczucie ingerencji w sferę prywatności, a z drugiej strony mylne poczucie zwiększonego bezpieczeństwa. Nie jest możliwe również instalowanie ukrytych kamer rejestrujących obraz, ponieważ w takim przypadku pracodawca m.in. nie byłby w stanie wykazać, że dopełnił obowiązku informacyjnego polegającego na wyraźnym oznaczeniu miejsca, które jest monitorowane [393].

W zakresie monitoringu wizyjnego ustawodawca wprowadził bezwzględny zakaz objęcia monitoringiem wizyjnym pomieszczeń udostępnianych zakładowej organizacji związkowej. Uzasadniając tą zmianę podano, iż „monitoring pomieszczeń związkowych rodzi duże prawdopodobieństwo naruszenia zasady wolności i niezależności związków zawodowych, która została postawiona wyżej niż chociażby zapewnienie bezpieczeństwa pracowników które w dotychczasowym brzmieniu przepisu w drodze wyjątku mogło uzasadniać objęcie monitoringiem wizyjnym pomieszczeń udostępnianych zakładowej organizacji związkowej.· Monitoring nie obejmuje również zgodnie z § 2 wskazanego przepisu **„**pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa - uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego

392 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 74

393 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str. 279

pracodawcy.” Uchylenie zakazu monitoringu w tych pomieszczeniach, nawet przy spełnieniu ww. przesłanek, może budzić jednak kontrowersje. Przynajmniej pomieszczenia sanitarne oraz szatnie, z uwagi na obowiązek poszanowania godności pracowników (art. 11^1 KP), powinny być pomieszczeniami, w których zakaz monitoringu jest bezwzględny [394].

Cele, zakres oraz sposób zastosowania monitoringu wizyjnego pracodawca zobowiązany jest ustalić w układzie zbiorowym pracy lub w regulaminie pracy. W sytuacji gdy pracodawca nie jest objęty układem zbiorowym ani nie ma obowiązku ustalenia regulaminu pracy (tj. zatrudnia mniej niż 50 pracowników, *vide*art. 104 § 1^1 k.p.), wskazane powyżej zagadnienia powinny zostać uregulowane w obwieszczeniu. Niezależnie od przyjętych rozwiązań zgodnie z komentowanym przepisem pracodawca niemniej jednak zobligowany jest poinformować pracowników o wprowadzeniu monitoringu w sposób u niego przyjęty, nie później niż dwa tygodnie przed jego uruchomieniem. W odniesieniu do nowych pracowników Kodeks pracy wyraźnie zastrzega konieczność poinformowania ich na piśmie o celach, zakresie oraz sposobach zastosowania monitoringu wizyjnego [395]. Informacja ma być przekazywana pracownikowi na piśmie. Z kolei zgodnie z § 3 pkt 2 lit. f rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej [396] potwierdzenie poinformowania pracownika o celu, zakresie oraz sposobie zastosowania monitoringu powinno znaleźć się w części B akt osobowych [397].

Obowiązek informacyjny pracodawcy rodzi również konieczność oznaczenia pomieszczeń oraz terenu monitorowanego w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem. Wskazany obowiązek może być spełniony m.in. przez zamieszczenie wszędzie tam, gdzie monitoring ma miejsce, tablic informacyjnych zawierających oprócz pierwszej warstwy informacyjnej (tj. kto, po co, gdzie i jak długo monitoruje) napis „Obiekt monitorowany” lub „Teren monitorowany” oraz dodatkowo przez wywieszenie odpowiednich piktogramów, które jednoznacznie będą wskazywać na stosowanie monitoringu. Tablice informujące o funkcjonowaniu monitoringu powinny być widoczne, umieszczone w sposób

394 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 81

395 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str. 279

396 Dz. U. z 2018 r., poz. 2369

397 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 82

trwały w niedużej odległości od nadzorowanych miejsc, a ich wymiary powinny być proporcjonalne do miejsca, w którym zostały umieszczone [398].

Okres przechowywania nagrań został określony w art. 22^2 § 3, jako nieprzekraczający 3 miesięcy od dnia nagrania. Z kolei w § 4 ustawodawca dopuścił do jego przedłużenia w przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu do czasu prawomocnego zakończenia postępowania. Tutaj należy również mieć na uwadze przepis art. 94^4 KP, który określa, iż okres przechowywania dokumentacji pracowniczej mogącej stanowić dowód w postępowaniu przedłuża się o 12 miesięcy, natomiast zgodnie z art. 94^7 pracodawca niszczy dokumentacje pracowniczą w sposób uniemożliwiający odtworzenie jej treści, w terminie do 12 miesięcy po upływie okresu przeznaczonego na odbiór dokumentacji pracowniczej. Wobec powyższego z uwagi na spójność systemową dobrze byłoby wydłużyć okres przechowywania nagrania z monitoringu do 12 miesięcy. Niewątpliwie dowód z nagrania monitoringu może mieć kluczowe znaczenie w takich sprawach, jak np. roszczenia z tytułu wypadku przy pracy [399].

Według art. 22^3 § 2 k.p. monitorowanie poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracowników. Jednakże w samej praktyce oznacza to, że podczas kontroli w przypadku natrafienia przez pracodawcę na jakąkolwiek wiadomość wysłaną lub otrzymaną przez pracownika o charakterze prywatnym, pracodawca nie będzie mógł jej w całości przeczytać. Takie stwierdzenie pojawiło się już w uzasadnieniu do przepisów sektorowych, jest ono jednak dość nieprecyzyjne i zapewne w przyszłości będzie powodować wiele dyskusji. Pracodawca powinien mieć możliwość weryfikowania jedynie poczty służbowej. Pracownik, wobec którego prowadzony jest monitoring poczty, powinien zostać o tym poinformowany w regulaminie pracy lub też w inny przyjęty u pracodawcy sposób. Informacja ta powinna być przedstawiona pracownikowi przed przystąpieniem do pracy. Do prowadzenia monitoringu poczty elektronicznej często są wykorzystywane określone systemy [400].

Przepisy dotyczące monitoringu służbowej poczty elektronicznej mają odpowiednie zastosowanie do innych form monitoringu (np. monitoring floty GPS, odwiedzanych stron

398 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str. 280

399 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 82

400 M. Jakubik, T. Świętnicki, *Indywidualny monitoring pracownika – zagadnienie monitorowania pracowników i ich danych,* Lex/el. 2020**,** dostęp z dnia 19.03.2021 r.

internetowych, wysyłanych smsów). Mogą one zatem być stosowane jedynie wówczas, gdy jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Pracodawca ma prawo monitorować ruch sieciowy i e-maile wychodzące, pod kątem różnego typu danych w celu wychwytywania anomalii zachowania, które z kolei mogą wskazywać na naruszenie bezpieczeństwa lub dyscypliny pracy. E-maile wychodzące można monitorować co do ilości danych przesyłanych i domen, np. popularnych darmowych kont pocztowych, aby wychwytywać przesyłanie danych firmowych na prywatne adresy e-mail. Można również monitorować: kopiowanie plików lub danych na urządzenia pamięci masowej; popularne siedzenie na Facebooku czy innych portalach, nadto można geolokalizować położenie floty firmowej lub szczególnych urządzeń firmowych, np. terminali kurierskich. Kontrola zawartości poczty elektronicznej może zostać przeprowadzona w szczególności, gdy pracodawca ma podejrzenie popełnienia przestępstwa, ujawnienia tajemnicy przedsiębiorstwa lub szczególnej tajemnicy typu bankowej, naruszenia ochrony danych osobowych, działania na szkodę pracodawcy, naruszenia ciągłości działania procesów w organizacji lub działań mających negatywny wpływ na wizerunek i reputację organizacji [401].

Monitoring jest stosowany także w systemach GPS, czyli systemie monitorowania i rejestracji tras pojazdów. Niezwykle istotnym elementem jest polityka informacyjna. Przepisy w tej sprawie mówią, że o wprowadzeniu systemu GPS przedsiębiorca jest zobowiązany poinformować wszystkich pracowników nie później niż do dwóch tygodni przed jego uruchomieniem. Dodatkowo przedsiębiorca jest zobowiązany oznaczyć monitorowane pojazdy oraz wpisać zasady monitorowania pojazdów do regulaminu lub układu zbiorowego pracy zgodnie z wymogami art. 13 RODO. Niejednokrotnie w samochodach, które posiadają monitoring GPS, pojawia się naklejka w takim miejscu, by kierowca był świadomy monitoringu prowadzonego wobec niego. Nadto widoczne jest to w art. 35 ust. 1 RODO, gdy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przeprowadzenie i udokumentowanie powyższej oceny ryzyka (nazywanej DPIA – Data Protection Impact Analysis) może mieć charakter obowiązkowy u pracodawcy prowadzącego monitoring lokalizacyjny pojazdów flotowych, na co wskazuje Prezes Urzędu Ochrony Danych Osobowych w komunikacie z 17.06.2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania, dla

401 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 83

ich ochrony, gdzie przetwarzanie danych lokalizacyjnych pracowników zostało wyraźnie wskazane przez Prezesa UODO jako forma operacji wymagająca potencjalnej oceny skutków dla ochrony danych [402].

Administrator powinien być w stanie określić zasady postępowania w przypadku otrzymania od osoby, której wizerunek został utrwalony, żądania kopii nagrania, usunięcia, przeniesienia, dostępu, czy anonimizacji wizerunku. W prawnie uzasadnionym interesie administratora jest przechowywanie wszystkich wniosków, a także udzielonych odpowiedzi. Administrator danych powinien zapewnić rozliczalność, o której mowa w art. 5 RODO, dla danych gromadzonych w związku ze stosowaniem monitoringu. Oznacza to, że każde udostępnienie danych powinno być uzasadnione, zweryfikowane oraz odnotowane. Jeżeli administrator danych wyznaczył inspektora ochrony danych, powinien być on niezwłocznie włączony w proces udostępnienia nagrania, w szczególności zaopiniować administratorowi sposób odpowiedzi na wniosek. Samo przekazanie nagrania wymaga także należytej staranności oraz zabezpieczenia, np. przekazania na zaszyfrowanym nośniku danych. Mając powyższe na uwadze proces udostępniania danych z systemu monitoringu wizyjnego powinien być odpowiednio sformalizowany. Po pierwsze Administrator powinien odnotowywać każdy wniosek dotyczący udostępnienia danych osobowych w stosownym rejestrze, nad którym nadzór prowadzi IOD. Każdy wniosek powinien mieć formę pisemną i posiadać wyraźną podstawę prawną uprawniającą podmiot do otrzymania wnioskowanych danych z systemu. W przypadku braku takiej podstawy należy odnotować przyczynę odmowy udostępnienia danych osobowych. Przekazanie danych odbywa się przez osoby odpowiedzialne merytorycznie oraz wymaga stosownego ich zabezpieczenia [403].

W myśl przepisów rozporządzenia pracodawca będący administratorem powinien dążyć do realizacji zasady rozliczalności przez stworzenie kompleksowego systemu zarządzania ochroną danych osobowych w organizacji. Zgodnie z zasadą rozliczalności obowiązkiem pracodawcy jest przede wszystkim przestrzeganie przepisów o ochronie danych oraz wykazanie, że właściwie spełnił wymogi określone w tych przepisach. W efekcie realizacja tej zasady powoduje, że pracodawca ma być w stanie rozliczyć się z przestrzegania

402 M. Jakubik, T. Świętnicki, *Indywidualny monitoring pracownika – zagadnienie monitorowania pracowników i ich danych,* op. cit.

403 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 85

obowiązujących przepisów prawa, w szczególności przed organami ochrony danych oraz osobami, których dane dotyczą [404].

Najwyższa Izba Kontroli podczas przeprowadzanych kontroli zwróciła uwagę na to, że nagrania bardzo często są przechowywane na niezabezpieczonych urządzeniach komputerowych, które znajdują się w ogólnodostępnych pomieszczeniach. Administrator danych powinien zainwestować we właściwą infrastrukturę teleinformatyczną, obejmującą także zapewnienie bezpiecznego przechowywania nagrań i tworzenie z nich kopii zapasowych. Należy zwrócić uwagę nie tylko na zabezpieczenia teleinformatyczne, lecz także fizyczne, tzn. kontrolę dostępu do pomieszczenia, zabezpieczenia ppoż, dostęp do nagrań tylko z uprawnionych urządzeń (terminali) po dokonaniu właściwego udostępnienia itd. Każdy dostęp i wykonywana czynność powinny być identyfikowane i odnotowywane przez system monitoringu w celu zapewnienia skutecznego nadzoru i rozliczalności monitoringu. Istotne jest także ustawienie monitorów wyświetlających obraz z kamer [405].

Zgodnie z ww. ogólną zasadą integralności i poufności danych osoby upoważnione w zakresie dostępu do monitoringu wizyjnego mają obowiązek zachowania poufności uzyskanych informacji, w tym zasad bezpieczeństwa funkcjonowania monitoringu wizyjnego [406].

Jeżeli wideonadzór jest sprawowany poprzez agencję ochrony, niezbędne jest zawarcie z nią umowy powierzenia danych osobowych, ponieważ pracownicy agencji otrzymują wgląd do danych. Bardzo ważnym elementem zapewniającym odpowiedni poziom bezpieczeństwa jednostki jest zapewnienie odpowiedniego ustawienia i zasięgu kamer, aby z jednej strony zabezpieczyć się przed dostępem osób nieuprawnionych poprzez wydzielenie pomieszczeń, w których prowadzona jest obserwacja przez upoważnione do tego osoby oraz z drugiej strony ustawienie zasięgu kamer w taki sposób, aby nie powodowało to naruszenia prawa do prywatności innych osób. Decydujący głos w tej sprawie powinny mieć osoby, których dane dotyczą. Kamery powinny swoim zasięgiem obejmować jedynie siedzibę administratora oraz zarządzany przez niego teren. Jeżeli kamera sięga także na zewnątrz, zasadne jest objęcie zasięgiem tylko najbliższego przylegającego terenu, np. chodnika i części jezdni. Istotnym

404 E. Bielak-Jomaa, M*onitoring pracowników – wybrane zagadnienia,* op. cit., str. 69-70

405 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 85

406 M. Otto, *Przetwarzanie danych osobowych w kontekście zatrudnienia,* op. cit., str. 280

elementem jest również odpowiednie zabezpieczenia urządzenia rejestrującego i nagrań w pomieszczeniu niedostępnym dla osób nieupoważnionych [407].

Mając na uwadze przedstawione obowiązki ADO i wymogi prawne oraz techniczne związane ze stosowaniem systemu monitoringu IOD powinien dokonać weryfikacji, czy Administrator dokonał analizy w zakresie potrzeby jego zastosowania, mając na uwadze proporcjonalność zastosowania monitoringu do celu, w jakim został wprowadzony oraz czy nagrania wykorzystywane są wyłącznie do celów, dla których zostały zebrane, a które to w tym przypadku jasno określają przepisy prawa. Sprawdzenie realizowane przez IOD dotyczące przeglądu zasad i warunków funkcjonowania monitoringu wizyjnego powinno obejmować weryfikację podstaw prawnych jego wprowadzenia, realizacji przez ADO obowiązków informacyjnych, w tym prowadzenia rejestru czynności przetwarzania, zasad dostępu do nagrań monitoringu oraz okresu przechowywania danych, a także spełnienia warunków technicznych – rozmieszczenia kamer i urządzeń rejestrujących. Elementem obowiązkowym weryfikacji powinno być uzasadnienie jego wprowadzenia oraz przeprowadzona ocena skutków dla ochrony danych osobowych. Nie sposób nie wspomnieć tu o konieczności weryfikacji sposobu zabezpieczenia danych, w tym urządzeń i pomieszczeń, w których są one przechowywane na co zwróciła uwagę NIK. Należy również wziąć pod uwagę, fakt, czy ADO wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku wiążącym się z przetwarzaniem, w szczególności wynikającym z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Z drugiej strony weryfikacja IOD powinna sprawdzić, czy ADO zapewnił, aby realizacja celu, jakim jest monitoring nie powodowała naruszenia prawa do prywatności innych osób, np. poprzez weryfikację, czy monitoring nie obejmuje swym zasięgiem np. pomieszczeń sanitarnych, szatni, stołówek oraz palarni. Nie jest możliwe również instalowanie ukrytych kamer rejestrujących obraz, ponieważ w takim przypadku pracodawca m.in. nie byłby w stanie wykazać, że dopełnił obowiązku informacyjnego polegającego na wyraźnym oznaczeniu miejsca, które jest monitorowane. Nie sposób nie wspomnieć również o próbie wykorzystania monitoringu do kontroli obecności w pracy podległych pracowników lub weryfikacji przebywania ich poza stanowiskiem pracy. IOD powinien zweryfikować, czy ADO przed

407 S. Hady-Głowiak, K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, op. cit., str. 85

wprowadzeniem systemu monitoringu wypełnił stosowne obowiązki ustawowe w tym zakresie. I tak dla przykładu w przepisach prawa pracy prawodawca wskazał obowiązek wobec pracodawcy ustalenia celu, zakresu oraz sposobu zastosowania monitoringu wizyjnego w układzie zbiorowym pracy lub w regulaminie pracy nie później niż dwa tygodnie przed jego uruchomieniem. Na dodatek potwierdzenie poinformowania pracownika o powyższym powinno znaleźć się w części B akt osobowych. Dotyczy to zarówno systemu monitoringu wizyjnego, służbowej poczty elektronicznej, jak również innych form monitoringu (np. monitoring floty GPS, odwiedzanych stron internetowych, wysyłanych smsów). IOD powinien również sprawdzić postanowienia ewentualnej umowy powierzenia przetwarzania danych, jeżeli wideo-nadzór jest sprawowany np. poprzez agencję ochrony oraz czy podmiot ten zapewnia przewidzianą w przepisach ochronę na zasadach określonych w art. 28 RODO. Ostatnim elementem istotnym z punktu widzenia IOD powinna być realizacja przez ADO obowiązku notyfikacji w zakresie naruszenia ochrony danych osobowych.

IV.2. Zadania i rola IOD w zakresie udostępniania i powierzania danych osobowych

Administrator przetwarza dane dla własnych potrzeb. Podmiot przetwarzający przetwarza dane dla potrzeb administratora danych – na zlecenie administratora [408].

Do powierzenia danych osobowych dochodzi, gdy administrator korzysta z usług zewnętrznego podmiotu, do których realizacji jest niezbędne przetwarzanie danych. Nie ma wątpliwości, że ADO powinien upoważniać do przetwarzania danych wszystkie osoby zatrudnione na podstawie umowy o pracę przy przetwarzaniu danych. Omówienia wymaga natomiast przypadek, gdy dane są przetwarzane przez zleceniobiorcę, szczególnie jeżeli prowadzi on jednoosobową działalność gospodarczą. Wyjaśnień w tym zakresie udzielił organ nadzorczy, zajmując stanowisko, że jeżeli zleceniobiorca przetwarza dane osobowe na zlecenie administratora danych, korzystając z udostępnionych przez niego środków i narzędzi, np. biuro, sprzęt komputerowy, nośniki danych, systemy informatyczne, powinien przetwarzać te dane na podstawie nadanego upoważnienia, tak samo jak inni pracownicy administratora, ponieważ nie będzie w wyniku wykonywanych czynności dochodziło do powierzenia. Jeżeli jednak w wyniku umowy cywilnoprawnej zewnętrzny podmiot przetwarza dane na zlecenie administratora w sposób niezależny, np. jako zewnętrzny konsultant, prowadzący jednoosobową działalność gospodarczą, wówczas przetwarzanie w imieniu administratora

408 M. Gawroński, K. Kloc, M. Wojtas, *Obowiązki i rola administratora oraz podmiotu przetwarzającego,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

powinno odbywać się na podstawie zawartej z administratorem umowy powierzenia danych osobowych. Art. 28 RODO szczegółowo wskazał obowiązki administratora oraz podmiotu przetwarzającego, a także uregulował wcześniej bardzo problematyczną kwestię dalszego powierzenia danych (tzn. podpowierzenia) [409].

Sytuacje, w których będzie konieczne zawarcie umowy powierzenia przetwarzania zgodnie z art. 28 RODO, będą zachodziły, kiedy na przykład zadania z zakresu prowadzenia rachunkowości, kadr czy płac będzie wykonywało centrum usług wspólnych. Taka sytuacja będzie miała miejsce także przy korzystaniu z usług podmiotu zewnętrznego w przypadku kompleksowej obsługi bhp, itp. Decyzja o powierzeniu pewnych zadań podmiotowi przetwarzającemu może być również elementem przeniesienia na tenże podmiot pewnego rodzaju ryzyka, które wiąże się z przetwarzaniem danych osobowych [410].

Pracodawca może powierzyć przetwarzanie danych osobowych swoich pracowników na zewnątrz. Najczęstszym przykładem jest powierzenie obsługi kadrowo-płacowej zewnętrznym firmom. Aby powierzyć obsługę kadrowo-płacową zewnętrznej firmie, pracodawca musi w tym celu zawrzeć z takim podmiotem umowę o powierzeniu przetwarzania danych osobowych pracowników [411].

Mając powyższe na uwadze przy analizie przetwarzania pracowniczych danych osobowych należy mieć na względzie nie tylko relację administrator danych osobowych – osoba, której dane są przetwarzane, lecz także kontekst łączącej strony szczególnej relacji pracowniczej, opartej na wzajemnej lojalności, bez której to relacji pracodawca nie przetwarzałby danych osobowych osoby, którą zatrudnił. Pracownik ma więc prawo wymagać dołożenia przez pracodawcę wszelkich możliwych starań do ochrony jego pracowniczych danych osobowych. Ma to szczególne znaczenie, gdy pracodawca – w różnych zresztą celach – powierza przetwarzanie tych danych podmiotowi trzeciemu wobec stron stosunku pracy. Przekazanie danych podmiotowi zewnętrznemu wiąże się z podwyższeniem ryzyka naruszenia pracowniczego prawa do prywatności. Odtąd bowiem kwestia spełniania pracodawczego obowiązku szanowania tego dobra osobistego nie zależy wyłącznie od starań pracodawcy. Dlatego pracodawca powinien szczególnie ostrożnie wybierać podmioty, którym powierza

409 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* Lex/el. 2019, dostęp z dnia 16.03.2021 r.

410 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, WKP 2020, str. 93

411 Szymczak-Kamińska Paulina, *Dostęp do danych osobowych kandydatów do pracy i pracowników,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

przetwarzanie danych, a kwestię prawnych wymogów powierzenia traktować znacznie bardziej rygorystycznie niż administrator, którego nie łączy szczególna relacja z osobą, której dane przetwarza [412].

Administrator danych osobowych jest podstawowym adresatem RODO i podstawowym obowiązanym na podstawie RODO. Odpowiada za całość przetwarzania danych, także w części powierzonej podmiotowi przetwarzającemu. Jeżeli kilka podmiotów jest zaangażowanych w proces przetwarzania, kluczowe jest ustalenie, który faktycznie decyduje o celach i środkach przetwarzania [413]. Administrator często z uwagi na obniżenie kosztów działalności decyduje się na powierzenie konkretnych czynności podmiotom zewnętrznym, ale musi dokonać weryfikacji podmiotu przetwarzającego, czy ten spełnia przewidzianą w przepisach ochronę danych osobowych. ADO powinien każdorazowo konsultować z IOD kwestie zlecania konkretnych czynności przetwarzania podmiotom zewnętrznym, a w szczególności dotyczy to świadczenia usług obsługi kadr, płac, księgowości w zakresie danych osobowych pracowników, współpracowników, podwykonawców, kontrahentów, czy realizacji usług BHP w zakresie danych osobowych pracowników. Nie sposób nie wspomnieć tu o administracji systemami informatycznymi w zakresie danych osobowych przetwarzanych w tych systemach, czy usługach dotyczących hostingu poczty, serwerów w zakresie danych osobowych przetwarzanych w tych systemach. Celem umowy powierzenia może być również usługa utylizacji sprzętu IT, brakowania dokumentacji, jej archiwizacji, czy obsługa systemu monitoringu wizyjnego.

Należy również zwrócić uwagę na konieczność rozróżnienia przez ADO sytuacji, kiedy mamy do czynienia z powierzeniem danych innemu podmiotowi, a kiedy z ich udostępnieniem. Co do zasady udostępnienie danych to każde przekazanie danych lub upublicznienie danych. Jeżeli udostępnienie odbędzie się z naruszeniem przepisów RODO, to określa się je jako udostępnienie nieuprawnionemu odbiorcy. W praktyce przyjęło się mówić o udostępnieniu przede wszystkim jako działaniu mającym na celu przekazanie danych pomiędzy dwoma administratorami danych, gdzie na skutek udostępnienia otrzymujący dane staje się ich administratorem [414].

412 K. Kopeć, P. Strumiński, *Przekazanie danych pracowniczych podmiotom zewnętrznym,* [pod red. M. Mędrala *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami]* WKP, Warszawa 2018, str. 216

413 M. Gawroński, K. Kloc, M. Wojtas, *Obowiązki i rola administratora oraz podmiotu przetwarzającego,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

414 S. Czub-Kiełczewska, *Okiem IOD-a: zasady udostępniania danych osobowych innym podmiotom,* Lex/el. 2019, dostęp z dnia 16.03.2021 r.

Istnieją pewne sytuacje, w których organizacje mogą udostępniać dane osobowe, np. firma może dzielić adresy e-mail pracowników z dostawcą szkoleń lub daty ich urodzenia z zewnętrznym dostawcą świadczeń medycznych. Niemniej dane osobowe powinny być ujawniane wyłącznie upoważnionemu personelowi wewnętrznemu i niektórym zaufanym stronom trzecim. Gdy relacja biznesowa między firmą a stroną trzecią wiąże się z przetwarzaniem danych osobowych, właściciel danego procesu powinien zadbać o to, by była ona właściwie uregulowana. Oznacza to zapewnienie odpowiedniej i należytej staranności, uzgodnienie warunków umowy, okresowe sprawdzanie i monitorowanie przetwarzania danych osobowych. Osoba, której dane są przetwarzane, musi być świadoma tego, co stanie się z jej danymi osobowymi. IOD powinien podjąć niezbędne działania uświadamiające i zadbać o wprowadzenie odpowiednich procedur, aby zapewnić bezpieczeństwo przetwarzanych danych osobowych i ich ujawnienie oraz udostępnienie jedynie tym odbiorcom, którzy są upoważnieni do ich przetwarzania. Niewłaściwe ujawnienie danych osobowych może mieć bardzo poważne konsekwencje dla organizacji [415].

W przepisach RODO nie zostały określone zasady postępowania, poza stwierdzeniem, że obowiązkiem administratora jest zapewnić ochronę danych przed udostępnieniem osobom nieupoważnionym. Pomimo że w przepisach RODO nie określono wprost zasad udostępniania danych na wniosek innego administratora, niezaprzeczalnie punktem wyjścia do tego działania powinny być zasady przetwarzania danych z art. 5 RODO. Każde działanie administratora musi być realizowane w taki sposób, aby zapewnić rozliczalność danych, czyli musi być określona podstawa prawna udostępnienia, cel, adekwatność do tego celu, należy także zapewnić minimalizację udostępnianych danych. A w celu zapewnienia pełnej rozliczalności wymaga się, aby cały proces udostępnienia był udokumentowany. Tak samo jak administrator powinien posiadać procedurę realizowania praw osoby, której dane dotyczą, do właściwego postępowania z wnioskami o udostępnienie danych niezbędna jest procedura określająca nie tylko czynności, które należy wykonać, lecz także zakres odpowiedzialności poszczególnych osób. Brak wdrożonej procedury może skutkować udostępnieniem danych bez wiedzy i zgody administratora [416].

W przypadku dotyczącym wniosków o dostęp do nagrań kierowanych do administratora przez organy publiczne i służby porządkowe, powinny być one związane z realizacją zadań tych podmiotów i zgodne z obowiązującymi je zasadami pozyskiwania danych osobowych.

415 M. Kołodziej, *Vademecum IOD*, C.H. Beck, Warszawa 2020, str. 54

416 S. Czub-Kiełczewska, *Okiem IOD-a: zasady udostępniania danych osobowych innym podmiotom,* op. cit.

Każdy przypadek udostępnienia powinien być prawidłowo udokumentowany. W myśl zasady rozliczalności, jest to konieczne, by administrator mógł wykazać, że przetwarzał dane zgodnie z obowiązującym prawem, o czym wspomniano już w poprzednim podrozdziale [417]. Należy zwrócić uwagę na fakt, iż bardzo często wnioskodawcy wskazują niepoprawnie podstawę prawną, czasami robią to nawet podmioty, które co do zasady są uprawnione do otrzymania danych do wskazanego we wniosku celu. W takim wypadku administrator może wezwać wnioskodawcę do poprawienia błędów formalnych we wniosku. Analiza otrzymanego wniosku pod kątem wskazanej podstawy prawnej powinna każdorazowo obejmować sięgnięcie przez ADO do wskazanego przepisu prawa i sprawdzenie, czy faktycznie wynika z niego uprawnienie wnioskodawcy. Jest to bardzo ważne ze względu na bardzo dynamiczne zmiany w przepisach, które prowadzą do sytuacji, gdy wnioskodawcy powołują się na uchylone już akty. Właśnie z takiego powodu operator telekomunikacyjny odmówił udostępnienia danych osobowych abonenta komendantowi straży miejskiej w badanej przez Prezesa UODO sprawie sygn. ZSOŚS.440.24.2019 z dnia 19 marca 2019 r. Operator wskazał w swoich wyjaśnieniach skierowanych do organu, że odmówił udostępnienia danych, ponieważ komendant, powołując się na uchylony przepis prawa, nie wykazał wystarczającej przesłanki prawnej uprawniającej go do otrzymania wnioskowanych danych [418].

W tym miejscu polityki bezpieczeństwa można wyszczególnić te sytuacje, regulując jednocześnie sposób i zakres przekazywania danych, bądź ograniczyć się wyłącznie do wyjaśnienia samego mechanizmu udostępnienia danych i pouczenia, że może się ono odbywać wyłącznie w przypadkach przewidzianych prawem [419].

Należy zgodzić się ze zdaniem M.Sakowskiej-Baryły, iż Administrator powinien prowadzić rejestr udostępnień (dla policji, komorników, itp., szczególnie, gdy cel przetwarzania jest celem tychże podmiotów). Taki rejestr warto prowadzić dla zapewnienia rozliczalności przetwarzania i celu zapewnienia realizacji praw osób, których dane dotyczą. Z pewnością ADO musi być w stanie ustalić jakie dane, komu, kiedy, na jakiej podstawie udostępnia [420].

---

417 *Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego*, 2018, str. 16, https://uodo.gov.pl/pl/file/1200, dostęp z dnia 21.03.2021 r.

418 S. Czub-Kiełczewska, *Okiem IOD-a: zasady udostępniania danych osobowych innym podmiotom,* op. cit.

419 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, WKP 2020, str.78

420 M. Sakowska-Baryła, *Odpowiedzi na pytania ze szkolenia "Udostępnianie danych osobowych w orzecznictwie Prezesa Urzędu Ochrony Danych Osobowych"*, Lex/el. 2020, dostęp z dnia 16.03.2021 r.

Nie sposób nie wspomnieć w tym miejscu o Wyroku WSA w Warszawie z dnia 26 lutego 2021 r. [421] w przedmiocie udostępnienia przez Ministra Cyfryzacji spółce Poczta Polska S.A. danych osobowych z Rejestru PESEL. WSA stwierdził bezskuteczność czynności z dnia 22 kwietnia 2020 r., polegającej na udostępnieniu Poczcie Polskiej danych osobowych na płycie DVD i zabezpieczone hasłem z Rejestru PESEL, dotyczących żyjących obywateli polskich, którzy uzyskali pełnoletność dnia 10 maja 2020 r. i których krajem zamieszkania jest Polska. Przekazane dane w postaci numeru PESEL, imienia (imion), nazwiska oraz w zależności od tego jakie dane osoba ma zarejestrowane w rejestrze PESEL – aktualny adres zameldowania na pobyt stały, a w przypadku jego braku ostatni adres zameldowania na pobyt stały, a także adres zameldowania na pobyt czasowy zostały wydane bez wyraźnej podstawy prawnej. 30 kwietnia 2020 r. RPO zwrócił uwagę Ministrowi Cyfryzacji, że nie miał podstawy prawnej, by przekazać te dane Poczcie Polskiej. Minister odpowiedział, że dostał z Poczty taki wniosek, a dane wydał na podstawie specustawy Covidowej (Tarczy Antykryzysowej 2.0). Na tej podstawie Prezes Rady Ministrów polecił Poczcie Polskiej zorganizowanie wyborów korespondencyjnych 10 maja 2020 r. W skardze do WSA z 15 maja 2020 r. Rzecznik wskazał, że ustawa ta nie dawała podstaw do wydania spółce Poczta Polska płyty z danymi obywateli. Ustawa, na którą powołał się Minister, pozwalała realizować zadania związane z organizacją wyborów Prezydenta RP zapowiedzianych na 10 maja. Tyle że 20 kwietnia Poczta Polska nie organizowała tych wyborów. Przepisy, które na to pozwalały, weszły w życie dopiero 9 maja (prezydent podpisał je 8 maja). Tym samym Poczta Polska nie miała kompetencji, by taką decyzję wykonać – zatem jej wniosek do Ministra Cyfryzacji nie miał prawnego znaczenia. Wynika z tego, że decyzja wydana na podstawie ustawy kowidowej była niewykonalna i jej niewykonalność ma charakter trwały. Rozporządzenie RODO pozwala na przetwarzanie danych osobowych wyłącznie kiedy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Tyle że w Polsce takiej podstawy prawnej nie było [422].

Mając powyższe na uwadze udostępnianie danych osobowych powinno się odbywać protokolarnie i tylko na podstawie wyraźnej podstawy prawnej, a IOD powinien sprawować

421 Wyrok WSA w Warszawie sygn. akt IV SA/Wa 1817/20 z dnia 26.02.2021 r., https://www.rpo.gov.pl/sites/default/files/Wyrok_uzasadnieniem_26.02.2021.pdf , dostęp z dnia 28.03.2021 r.

422 https://www.rpo.gov.pl/pl/content/rpo-minister-cyfryzacji-przekazanie-poczcie-rejestru-pesel-wybory-bezskuteczne , dostęp z dnia 28.03.2021 r.

nadzór nad prowadzeniem rejestru udostępnień danych osobowych oraz nad prawidłowością obsługi tego procesu. Rejestr taki powinien zawierać co najmniej takie rekordy, jak: data wniosku, nr lub oznaczenie pisma przychodzącego i podmiotu wnioskującego, zakres wnioskowanych danych i podstawę prawną żądania, informacje, czy udostępniono dane oraz zakres udostępnionych danych, a także datę udostępnienia, nr pisma wychodzącego i dane osoby, która zrealizowała żądanie.

Powyższe nie będzie dotyczyć danych udostępnianych na wniosek. Udostępnienie może też mieć miejsce na żądanie lub za zgodą osoby, której dane dotyczą, na przykład w wyniku przeniesienia danych osobowych na zasadach określonych w art. 20 RODO. Inną formą udostępnienia, która została określona w art. 20 RODO, jest przenoszenie danych pomiędzy administratorami na żądanie osoby, której dane dotyczą. W wyniku żądania podmiotu danych administrator jest zobligowany przekazać innemu podmiotowi kopię danych osobowych umożliwiającą temu podmiotowi kontynuowanie dotychczas świadczonych usług. W wyniku tego udostępnienia podmiot otrzymujący dane osobowe staje się ich administratorem [423]. Z kolei powierzenie danych polega na przetwarzaniu danych przez wskazany podmiot w imieniu administratora, w sposób określony przez ADO, który powierzając dane osobowe do przetwarzania wskazuje zasady ich przetwarzania w ramach zawartej umowy powierzenia. Różnica jednakże w porównaniu z poprzednim przykładem jest zasadnicza i polega na tym, że dane osobowe przekazujemy podmiotowi zewnętrznemu po to, aby realizował cele i zadania w imieniu administratora [424].

Podmiot przetwarzający nie jest uprawniony do samodzielnego decydowania o celach i środkach przetwarzania, w szczególności bez zgody administratora nie może dokonać dalszego powierzenia danych lub przetwarzać danych w innych celach, niż wskazane przez administratora [425].

Prowadzenie dokumentacji jest bezspornie obowiązkiem administratora, natomiast podmiot przetwarzający przetwarza dane osobowe dla realizacji nie swojego celu, a obowiązku administratora, który mu dane w tym celu powierza. W tym miejscu należy odnieść się do art. 28 RODO i zawrzeć opis niezbędnych wymogów związanych z zawarciem umowy powierzenia przetwarzania i samym powierzeniem danych. W związku z tym, że powierzenie

423 S. Czub-Kiełczewska, *Okiem IOD-a: zasady udostępniania danych osobowych innym podmiotom,* op. cit.

424 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, WKP 2020, str. 78

425 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* op. cit.

przetwarzania wymaga przepływu danych oraz musi być odnotowane w rejestrze czynności przetwarzania, zaleca się, aby zobowiązać osoby planujące powierzenie do informowania o tym fakcie inspektora ochrony danych. Dobrą praktyką będzie parafowanie takich umów przez inspektora ochrony danych, do czego w tym miejscu w polityce bezpieczeństwa można nawiązać [426].

Administrator może powierzyć przetwarzanie danych osobowych wyłącznie podmiotowi, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi określone w RODO i chroniło prawa osób, których dane dotyczą [427].

Brak umowy powierzenia danych z podmiotem zapewniającym stronę internetową BIP, czyli naruszenie wymagań art. 28 RODO, był jedną z przyczyn nałożenia administracyjnej kary pieniężnej na burmistrza miasta Aleksandrowa Kujawskiego. Prezes UODO podczas przeprowadzanych w podmiotach publicznych kontroli sprawdzał nie tylko, czy wymagane powierzenie zostało sformalizowane, ale także czy jego treść jest zgodna z wymaganiami wynikającymi z przepisów, w tym czy zawiera co najmniej informacje wymagane art. 28 ust. 3 RODO. Wśród zaniedbań formalnych związanych z powierzeniem danych organ zwracał także uwagę na konieczność ujawniania w klauzulach informacyjnych podmiotu przetwarzającego jako odbiorcy danych osobowych [428].

Metodyczny ADO podejdzie do umowy o powierzenie przetwarzania danych przez pryzmat wszystkich obowiązków, które spoczywają na ADO i opatrzy je odpowiednimi klauzulami nakładającymi na podmiot przetwarzający obowiązki korespondujące ze swoimi. Ułożenie relacji ADO z przetwarzającym może spotkać się brakiem zrozumiem przez podmiot przetwarzający w pełni obowiązków, które spoczywają na nim w myśl RODO, lub w ogóle nie będzie rozumiał swojej roli jako przetwarzającego, dużo dyskusji może dotyczyć np. odpowiedzialności. Kolejnym aspektem jest stosowanie przez ADO tych samych wymagań i narzędzi kontrolnych do istotnego przetwarzającego i do małych przetwarzających, np. mikroprzedsiębiorców, co może być mało produktywne. Nie należy zapomnieć o pozycji siły kontraktowej, gdzie mały administrator w relacji z dużym przetwarzającym będzie stał na

426 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, op. cit., str. 79

427 Szymczak-Kamińska Paulina, *Dostęp do danych osobowych kandydatów do pracy i pracowników,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

428 S. Czub-Kiełczewska, *Okiem IOD-a: publikowanie danych w BIP a RODO,* Lex/el. 2020, dostęp z dnia 16.03.2021 r.

słabszej pozycji. Na koniec należy zauważyć problem ucieczki do trzeciej linii – według starych przepisów tylko administrator odpowiada przed organem nadzorczym i wobec podmiotów danych, natomiast zgodnie z RODO odpowiedzialność ponosi administrator, ale też przetwarzający (w zakresie bezpieczeństwa danych, legalności i trzymania się poleceń administratora). Wprawdzie odpowiedzialność względem organu nadzorczego i podmiotu danych może ponosić także podprzetwarzający (podwykonawca), ale i tak duzi dostawcy, np. dostawcy chmurowi, mogą odczuwać pokusę uplasowania się w roli podprzetwarzających, wierząc, że uchroni ich to przed bezpośrednimi sankcjami ze strony organów nadzorczych i pozwami podmiotów danych [429].

Umowa powierzenia powinna zostać zawarta przed przekazaniem danych podmiotowi przetwarzającemu. Dużym ułatwieniem dla administratorów danych jest wskazanie elementów, które muszą znaleźć się w umowie powierzenia, bezpośrednio w przepisach o ochronie danych. Najważniejszym jest określenie zakresu, celu i kategorii przetwarzania powierzonych danych. Umowa powierzenia musi być na tyle precyzyjna, aby nie było wątpliwości co do uprawnień i obowiązków podmiotu przetwarzającego. Jednocześnie administrator musi nałożyć na niego obowiązek zobligowania do zachowania tajemnicy wszystkich osób dopuszczonych do przetwarzania powierzonych danych i zapewnienia im należytej ochrony [430]. RODO w sposób szczegółowy reguluje również obowiązki samego podmiotu przetwarzającego. Należą do nich m.in. obowiązek przetwarzania danych wyłącznie na udokumentowane polecenie administratora, zapewnienie, aby osoby dopuszczone przez procesora do przetwarzania danych miały do tego stosowne upoważnienie, obowiązek podejmowania odpowiednich środków zabezpieczających przetwarzanie powierzonych danych czy też pomoc administratorowi w wykonywaniu nałożonych na niego przez RODO obowiązków [431].

Podobnie jak w przypadku art. 29 RODO, tak i tu przetwarzanie danych osobowych może odbywać się na wyłączne polecenie administratora. W art. 28 ust. 3 lit. a RODO podkreśla się, że polecenie to musi być udokumentowane. Nic nie stoi na przeszkodzie, aby rolę takiego udokumentowanego polecenia przetwarzania stanowiła umowa powierzenia przetwarzania. Kolejny nakaz, wynikający z art. 28 ust. 3 lit. b RODO, nakłada na podmiot przetwarzający obowiązek dopuszczenia do przetwarzania danych osobowych administratora tylko osób, które

429 M. Gawroński, K. Kloc, M. Wojtas, *Obowiązki i rola administratora oraz podmiotu przetwarzającego,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

430 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce, op. cit.*

431 Szymczak-Kamińska Paulina, *Dostęp do danych osobowych kandydatów do pracy i pracowników,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

zobowiązały się do zachowania poufności, chyba że podlega on odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Następnym zobowiązaniem podmiotu przetwarzającego, a płynącym z postanowień umowy powierzenia przetwarzania i wynikających z art. 28 ust. 3 lit. c RODO jest wdrożenie odpowiednich środków technicznych i organizacyjnych ochrony danych osobowych. Podobnie jak w przypadku zabezpieczeń wdrożonych przez administratora, ich rodzaj i konkretny wybór ma być adekwatny do występujących zagrożeń. Administrator nie może narzucić rodzaju środków ochrony, ale ich zastosowanie ma wynikać z konkretnego ryzyka, zaś decyzja co do ich wyboru leży w gestii podmiotu przetwarzającego. Analizując dalej art. 28 RODO, dochodzimy do ust. 3 lit. e, gdzie prawodawca unijny nakłada obowiązek zawarcia w umowie powierzenia oświadczenia podmiotu przetwarzającego, że w miarę swoich możliwości będzie pomagał administratorowi w wypełnianiu praw osób, których dane dotyczą [432].

Wśród obowiązków podmiotu przetwarzającego, które powinny zostać wskazane w umowie powierzenia jest także sposób zawiadamiania o naruszeniu ochrony danych oraz postępowania w przypadku takiego naruszenia [433].

W tym miejscu należy unormować proces (procedurę) obsługi naruszeń, tak kształtując obowiązki podmiotu przetwarzającego, aby administrator mógł dochować terminów przy ewentualnym zgłaszaniu naruszenia Prezesowi Urzędu Ochrony Danych Osobowych oraz zawiadamianiu podmiotów danych. Dla wywiązania się z tego obowiązku niezbędne jest dla niego uzyskanie pewnego rodzaju informacji na temat charakteru, zakresu i konsekwencji naruszenia. Artykuł 28 ust. 3 lit. f wymaga także zobowiązania podmiotu przetwarzającego do pomocy, w sytuacji, kiedy administrator będzie musiał dokonać oceny skutków dla ochrony danych na mocy art. 35 RODO. Pomoc owa będzie polegała głównie na dostarczeniu przez podmiot przetwarzający informacji na temat zabezpieczeń danych, które przy dokonywaniu oceny pozwolą wykazać, że planowane przetwarzanie będzie spełniało wymagania RODO [434]. Administrator określa także w powierzeniu sposób postępowania z danymi po zakończeniu umowy oraz zasady przeprowadzania przez niego audytów, do których jest uprawniony zgodnie z przepisami RODO. Na początku wiele podmiotów przetwarzających nie chciało się

432 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, op. cit., str. 97 - 99

433 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce, op. cit.*

434 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, op. cit., str. 99 – 100

zgodzić na wprowadzenie do umów powierzenia danych postanowień dotyczących audytów prowadzonych przez administratora [435].

Treść art. 28 ust. 3 lit. h RODO, dotyczący prowadzenia audytów, budzi najwięcej kontrowersji zarówno po stronie administratorów, jak i po stronie podmiotów przetwarzających. W umowach powierzenia przetwarzania można spotkać wielorakie postanowienia w tym zakresie. Począwszy od ustalenia opłaty uiszczanej przez administratora na rzecz podmiotu przetwarzającego, organizowania dni otwartych w przypadku, gdy podmiot przetwarzający obsługuje wielu administratorów, po wręcz pozbawianie tej możliwości administratora w ogóle. Zapewne ustalanie opłaty, czy też pozbawianie administratora tej możliwości będzie działaniem niezgodnym z obowiązującymi przepisami. Jednakże trudno nie przyjąć do wiadomości argumentu, że w przypadku obsługiwania wielu administratorów audyty takie mogłyby paraliżować pracę podmiotu przetwarzającego [436]. Dlatego tak ważna jest rola IOD w zakresie weryfikacji niedozwolonych klauzul umownych.

Administrator danych jest zobligowany już na etapie wyboru podmiotu przetwarzającego do analizy systemu zabezpieczeń, jaki zamierza on zapewnić powierzanym danym. Powinien on korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów RODO i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO). Powyższe wymagania wskazują, że podmiot przetwarzający musi być podmiotem profesjonalnym. W praktyce to ADO na żądanie organu nadzorczego będzie musiał udowodnić, że podmiot przetwarzający, który został przez niego wybrany, spełnia te wymagania [437].

Administrator powinien być w stanie wykazać przesłanki, którymi się kierował, np. posiadane przez podwykonawcę certyfikaty bezpieczeństwa, przedstawione przez niego standardy ochrony danych czy referencje. Innym rozwiązaniem, coraz częściej stosowanym, są ankiety oceny podmiotu przetwarzającego, przekazywane mu przed zawarciem umowy. Administrator może także, za zgodą podmiotu przetwarzającego, przeprowadzić u niego

435 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* op. cit.

436 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, op. cit., str.101

437 M. Gawroński, K. Kloc, M. Wojtas, *Obowiązki i rola administratora oraz podmiotu przetwarzającego,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

wstępny audyt, który pozwoli mu ocenić możliwość zapewnienia przez niego należytych gwarancji ochrony danych [438].

IOD powinien być każdorazowo zapraszany na spotkania z osobami nadzorującymi proces przygotowania współpracy z przyszłym dostawcą wymagającej udostępnienia informacji prawnie chronionych lub dostępu do wewnętrznego systemu organizacji. IOD zapewnia, aby zawsze w sytuacji, gdy zajdzie konieczność takiej współpracy, została ona poprzedzona podpisaniem umowy o zachowanie poufności. IOD oraz osoby odpowiedzialne przeprowadzają w takiej sytuacji analizę ryzyka bezpieczeństwa informacji oraz procesów operacyjnych specyficznych dla usług, które organizacja zamierza pozyskać oraz sposób w jaki dostawca zapewnia bezpieczeństwo świadczonych usług mając na uwadze wiarygodność i doświadczenie dostawcy oraz jakość świadczonych przez niego usług (na podstawie informacji z otoczenia rynkowego i opinii ekspertów) oraz ryzyko związane z uzależnieniem się od dostawcy zewnętrznego. W sytuacji, gdy współpraca polega na świadczeniu usług wymagających zawarcia umowy powierzenia przetwarzania danych osobowych, to IOD wraz z osobami odpowiedzialnymi przeprowadza dodatkową weryfikację dostawcy pod kątem stosowania przez niego odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z przepisami prawa w zakresie ochrony danych osobowych oraz bada, czy dostawca posiada odpowiednią wiedzę fachową, a także zasoby do realizacji przetwarzania powierzonych danych. Narzędziem stosowanym przez IOD w tym zakresie będzie lista kontrolna wspierająca taką weryfikację, podobnie, jak miało to miejsce w przypadku ankiety przed przystąpieniem do opracowania planu zadania audytowego, o czym była mowa w rozdziale trzecim niniejszej pracy. Przykładowa lista kontrolna powinna zawierać pytania w zakresie wyznaczenia IOD lub w przypadku braku takiego obowiązku innej osoby odpowiedzialnej za inicjowanie i nadzorowanie wdrażania i stosowania zasad ochrony danych osobowych i zabezpieczeń. Kolejne pytania powinny dotyczyć obowiązku prowadzenia przez Wykonawcę rejestru kategorii przetwarzania dokonywanego w imieniu każdego z administratorów oraz obowiązku jego okresowej weryfikacji i aktualizacji. Pozostałe pytania kontrolne powinny prowadzić do weryfikacji czy Wykonawca uwzględnia zasady ochrony danych w fazie projektowania (Privacy by Design) oraz domyślnej ochrony danych (Privacy by Design) zgodnie z art.25 RODO oraz czy wdrożył procedury i mechanizmy powiadamiania administratora, jak i podmiotów danych (np. klientów) o naruszeniach danych osobowych. Zgodnie z powyższym należy zapytać, czy Wykonawca

438 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* op. cit.

dokonuje oceny ryzyka bezpieczeństwa danych osobowych oraz ryzyka naruszenia praw i wolności osób, których dane dotyczą zgodnie z określoną formalną metodyką oceny oraz przeprowadza ocenę skutków dla ochrony danych (DPIA). Kolejne kwestie dotyczą posiadania lub nie przez Wykonawcę ustanowionego Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z międzynarodową normą ISO/IEC 27001 i ewentualnego posiadania przez Wykonawcę certyfikatu zgodności z jej wymaganiami, uwzględniającego w swoim zakresie usługę, która będzie wykonywana dla Zleceniodawcy. Należy również zweryfikować sposób zabezpieczenia przez Wykonawcę aktywów (np. sprzęt komputerowy) służących do przetwarzania danych osobowych, który powinien być adekwatny do przeprowadzonej oceny ryzyka oraz art. 32 RODO (wykonywanie kopii zapasowych przetwarzanych danych, dokonywanie ich okresowej weryfikacji pod kątem możliwości ich przywrócenia funkcjonowanie procedur i mechanizmów zapewniających ciągłość działania usług związanych z przetwarzaniem danych osobowych). Należy sprawdzić, czy Wykonawca wdrożył polityki/zasady/procedury/instrukcje postępowania z danymi przez osoby upoważnione do przetwarzania danych osobowych oraz realizuje szkolenia tych osób, w tym okresowe oraz czy wdrożył mechanizmy usuwania danych po zakończeniu przetwarzania. Zleceniodawca powinien również zweryfikować czy sposób zarządzania dostępem użytkowników Wykonawcy zapobiega nieuprawnionemu dostępowi do systemów i usług IT. W związku z powyższym należy zapytać o wdrożenie przez Wykonawcę procedur zapewniających cykliczne (nie rzadziej niż raz w roku) przeglądanie i sprawdzanie uprawnień użytkowników pod kątem ich adekwatności i aktualności oraz zapewnienie rozliczalności aktywności użytkowników. Nie sposób nie zweryfikować również przyjętych przez Wykonawcę rozwiązań zapewniających ochronę przed szkodliwym oprogramowaniem na wszelkich urządzaniach wykorzystywanych do przetwarzania danych osobowych oraz wdrożył procedury zapewniające skuteczne zarządzanie poprawkami bezpieczeństwa i aktualizacjami systemów operacyjnych, aplikacji i urządzeń sieciowych. To samo dotyczy również wdrożonych lub nie przez Wykonawcę procedur i mechanizmów zapewniających rozliczalność i gwarantujących adekwatny do zagrożeń poziom bezpieczeństwa fizycznego i środowiskowego, tj. kontrola dostępu do pomieszczeń kontrolę i urządzeń służących do przetwarzania danych osobowych. Mając powyższe na uwadze nie sposób nie zapytać czy w ciągu ostatnich 3 lat u Wykonawcy były przeprowadzane audyty/kontrole wewnętrzne i zewnętrzne dotyczące ochrony danych osobowych, w tym postępowania kontrolne UODO. W przypadku korzystania przez Wykonawcę z usług innych podmiotów należałoby

koniecznie zweryfikować, czy Wykonawca monitoruje wdrożenie wymaganego poziomu ochrony danych przez swoich podwykonawców lub dostawców usług.

Analizując art. 28 RODO, podkreślić trzeba, że do obowiązków podmiotu przetwarzającego należy również zawiadomienie administratora, jeśli ten wydał mu polecenie, które w ocenie podmiotu przetwarzającego narusza przepisy RODO. Kwestia, czy faktycznie tak jest, stanowi odrębną sprawę i podlegać będzie ocenie obu stron, niemniej jednak należy o tym pamiętać w odniesieniu do ewentualnych konsekwencji, w postaci na przykład kar nakładanych przez organ nadzorczy, i rzetelnie pochylić się nad problemem, jeśli takie zawiadomienie faktycznie od podmiotu przetwarzającego wpłynie [439].

Na gruncie RODO, aby podmiot przetwarzający mógł dalej podpowierzyć przetwarzanie danych, sam administrator musi na to wyrazić uprzednią pisemną zgodę [440].
Na przykład biuro rachunkowe, któremu administrator powierzył przetwarzanie danych, może korzystać z systemu kadrowego, którego wsparcie techniczne zostało powierzone zewnętrznej firmie, a także z usług hostingu, niszczenia i archiwizacji danych. Podpisując umowę powierzenia z administratorem, musi uzyskać jego zgodę na dalsze powierzenie danych swoim podwykonawcom, zapewniającym właściwe wykonanie usługi. Obowiązek wskazywania podmiotów podprzetwarzających stanowi czasami duży problem dla podmiotu przetwarzającego, który obawia się, że ujawniając dane podwykonawcy, narazi się na ryzyko, że administrator następnym razem skorzysta z usług tego podmiotu bezpośrednio (co oczywiście bezpośrednio wpłynie na koszt usługi). W takim wypadku podmiot przetwarzający powinien zabezpieczyć swój interes poprzez zawarcie odpowiedniej umowy o zakazie konkurencji ze swoimi podwykonawcami. Należy podkreślić, że umowa zawarta z podmiotem podprzetwarzającym powinna nakładać na niego takie same obowiązki, jak na podmiot przetwarzający, a w związku z tym, że wyboru tego podmiotu dokonuje nie administrator, a podmiot przetwarzający, to za jego działania odpowiedzialność spoczywa na podmiocie przetwarzającym [441].

IOD powinien podobnie, jak w przypadku zawierania umowy powierzenia zaproponować ADO przeprowadzenie weryfikacji podmiotu przetwarzającego, co pozwoli ADO na faktyczną ocenę sposobu przetwarzania przez ten podmiot danych osobowych.

---

439 A. Pielok, P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, op. cit., str.102

440 Szymczak-Kamińska Paulina, *Dostęp do danych osobowych kandydatów do pracy i pracowników,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.

441 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* op. cit.

W przypadku korzystania z usług podmiotów umożliwiających przekazanie danych (zarówno udostępnienie, jak i powierzenie przetwarzania) do państwa trzeciego było zgodne z prawem, konieczne jest spełnienie jednego z warunków wskazanych w rozdziale V RODO. Mając powyższe na uwadze ADO we współpracy z IOD powinien sprawdzić czy w stosunku do tego państwa trzeciego Komisja Europejska wydała decyzję o zapewnieniu adekwatnego poziomu ochrony. Komisja podejmuje taką decyzję w formie aktu mającego walor powszechnie obowiązującego prawa. Należy również wziąć pod uwagę fakt, iż jeśli w stosunku do takiego państwa trzeciego Komisja Europejska nie wydała decyzji, o której mowa powyżej to należy zweryfikować, czy istnieją inne zabezpieczenia wskazane w RODO, np. wiążące reguły korporacyjne bądź standardowe klauzule umowne. Wiążące reguły korporacyjne to swoiste zasady dotyczące przekazywania danych do wszystkich podmiotów w ramach jednej grupy na całym świecie mające zapewnić odpowiednie ich zabezpieczenie. Standardowe klauzule umowne natomiast to klauzule modelowe, które określają obowiązki konieczne do ochrony danych. Stanowią one podstawę do międzynarodowego transferu danych dla podmiotów spoza jednej grupy przedsiębiorstw. Jeżeli nie wystąpiła żadna z powyższych sytuacji – czy zaistniał jakiś wyjątek przewidziany w RODO, który umożliwia transfer danych do państwa trzeciego, np. podmiot, którego dane mają być przekazane, wyraził na to zgodę. Zgoda taka musi być wyraźna, a podmiot danych musi być uprzednio poinformowany o ryzykach, które wiążą się z takim transferem danych [442].

Ze względu na coraz częstszą liczbę przekazań danych do państw trzecich, a także groźbę brexitu, Prezes UODO opublikował wytyczne dotyczące powierzania danych podmiotom z państw trzecich [443].

Podsumowując należy podkreślić niezwykle istotną rolę IOD w zakresie nadzoru dotyczącego procesu udostępniania i powierzania danych osobowych. W zakresie udostępniania danych osobowych ADO powinien włączyć IOD w każdorazową weryfikację podstaw prawnych upoważniających do udostępnienia danych osobowych oraz powierzyć nadzór nad prowadzeniem rejestru udostępnień danych osobowych oraz nad prawidłowością obsługi tego procesu. W przypadku procesu dotyczącego powierzania danych osobowych IOD powinien być każdorazowo zapraszany na spotkania z osobami nadzorującymi proces przygotowania współpracy z przyszłym dostawcą. Nie sposób tu nie wspomnieć o konieczności przeprowadzenia z udziałem IOD weryfikacji dostawcy pod kątem stosowania przez niego

442 Szymczak-Kamińska Paulina, *Dostęp do danych osobowych kandydatów do pracy i pracowników,* op. cit.

443 S. Czub-Kiełczewska, *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* op. cit.

odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z przepisami prawa w zakresie ochrony danych osobowych oraz posiadania przez niego odpowiedniej wiedzy fachowej, a także zasobów do realizacji przetwarzania powierzonych danych. Bardzo ważnym elementem w tym zakresie jest przygotowanie we współpracy listy kontrolnej wspierającej taką weryfikację i analiza odpowiedzi udzielonych przez podmiot przetwarzający. Bardzo ważna jest również rola IOD w zakresie przygotowania i analizy postanowień umowy powierzenia przetwarzania danych osobowych pod kątem wystąpienia niedozwolonych klauzul umownych (utrudniających lub uniemożliwiających przeprowadzenie przez ADO audytów u podmiotu przetwarzającego, ograniczających jego odpowiedzialność do określonej w umowie kary, czy kwoty, a także dotyczących wspierania ADO w wypełnianiu praw osób, których dane dotyczą, czy zawiadamiania ADO o naruszeniu i zapewnienia mu niezbędnej pomocy w tym zakresie) i zapewnienia jej zgodności z przepisami prawa.

IV.3. Zagrożenia związane z przetwarzaniem danych osobowych w organizacji i rola IOD w tym zakresie

Identyfikacja incydentu bezpieczeństwa informacyjnego zobowiązuje administratora danych do podjęcia wszelkich środków po to, aby ten incydent we właściwy sposób sklasyfikować oraz wdrożyć właściwe kroki w celu wyeliminowania jego negatywnych następstw. Pojęcie incydentu bezpieczeństwa informacji nie zostało uregulowane w przepisach prawnych, ale należy je kwalifikować jako pojęcie szersze niż pojęcie naruszenia ochrony danych osobowych. Norma ISO 27000 w pkt 2.36 definiuje incydent związany z bezpieczeństwem informacji jako pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Natomiast naruszenie ochrony danych osobowych w myśl art. 4 pkt 12 RODO zostało zdefiniowane jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych [444].

Oznacza to, że nie każde naruszenie przepisów o ochronie danych stanowi naruszenie ochrony danych w rozumieniu przepisów unijnych, a jedynie takie naruszenie, które spełnia wymogi wskazane w definicji, a więc: stanowi naruszenie bezpieczeństwa (wymogów

444 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?*, Lex/el. 2020, dostęp z dnia 16.03.2021 r.

dotyczących zabezpieczenia danych) i skutkiem naruszenia bezpieczeństwa jest zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych [445].

Wstępna klasyfikacja zdarzenia polega przede wszystkim na ocenie tego, czy dane zdarzenie należy uznać za naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO. W pierwszej kolejności niezbędne jest ustalenie, czy dane zdarzenie dotyczyło danych osobowych w rozumieniu art. 4 pkt 1 RODO (np. imion i nazwisk, numerów PESEL, adresów e-mail czy danych dotyczących zdrowia). Następnie administrator danych musi ocenić, czy dane zdarzenie spełnia dodatkowe przesłanki, które wynikają z definicji naruszenia ochrony danych osobowych, czyli czy doszło do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu. Wskazane przesłanki stanowią punkt wyjścia dla administratora w odniesieniu do głębszej oceny naruszenia ochrony danych w kontekście obowiązków zgłoszeniowych wynikających z art. 33 oraz 34 RODO [446]. I tutaj kluczowa jest rola IOD zarówno w zakresie wdrożenia, jak i weryfikacji obowiązujących zasad i procedur w tym zakresie.

Przykładowe naruszenia ochrony danych to: kradzież nośnika (zarówno w postaci papierowej, jak i elektronicznej) zawierającego dane osobowe czy też uzyskanie dostępu do systemu informatycznego zawierającego dane osobowe przez osobę do tego nieuprawnioną. Nie stanowi naruszenia ochrony danych osobowych w rozumieniu nadanym temu pojęciu przez prawodawcę unijnego naruszenie innych przepisów o ochronie danych niż przepisy dotyczące zabezpieczenia danych, np. niedopełnienie obowiązku informowania osób o przetwarzaniu danych czy też niespełnienie żądania podmiotu danych dotyczącego skorygowania jego danych [447].

Na podstawie art. 33 RODO administrator danych jest zobowiązany do zgłoszenia naruszenia ochrony danych osobowych organowi ochrony danych. Warunkiem zwalniającym z obowiązku zgłoszeniowego jest wystąpienie małego prawdopodobieństwa, by naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Naruszenie ochrony danych osobowych w przypadku powstania obowiązku zgłoszeniowego musi zostać zrealizowane niezwłocznie, w miarę możliwości, nie później niż w terminie 72

445 P. Fajgielski, *Dokumentacja naruszeń ochrony danych osobowych,* [w:] M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, WKP, Warszawa 2019 , str. 176

446 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?*, op. cit.

447 P. Fajgielski, *Dokumentacja naruszeń ochrony danych osobowych,* op. cit., str. 196

godzin po stwierdzeniu naruszenia. W przypadku gdy do zgłoszenia dojdzie po upływie 72 godzin, niezbędne jest dołączenie organowi ochrony danych wyjaśnienia dotyczącego przyczyn opóźnienia. Regulacja dotycząca podmiotów przetwarzających została ujęta w art. 33 ust. 2 RODO, który stanowi, że podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych jest zobowiązany do zgłoszenia naruszenia administratorowi. W przypadku podmiotów przetwarzających procedura notyfikowania zgłoszenia naruszenia ochrony danych administratorowi powinna zostać odpowiednio uregulowana w umowie dot. powierzenia przetwarzania danych osobowych [448].

Za datę stwierdzenia naruszenia należy przyjąć dzień, w którym uznano, iż zdarzenie stanowi naruszenie bezpieczeństwa, co niekoniecznie będzie tożsame z dniem, w którym zdarzenie nastąpiło. Jako przykład można wskazać sytuację, w której uległo zniszczeniu urządzenie służące jako nośnik, na którym zapisane były dane osobowe. Tego rodzaju zdarzenie może, ale nie musi być kwalifikowane jako naruszenie ochrony danych, a ocena w tym zakresie uzależniona może być od wielu różnych okoliczności, np. od tego, czy dane osobowe były zgromadzone jedynie na tym nośniku (np. dysku twardym komputera), czy też na innych nośnikach (np. na dysku sieciowym) – w sytuacji gdy urządzenie uległo uszkodzeniu lub zniszczeniu, jednak dane nie zostały utracone, gdyż były przechowywane także na innym nośniku, mimo że zdarzenie nastąpiło, jego ustalenie nie jest równoznaczne ze stwierdzeniem naruszenia ochrony danych, a osoba, która zgłasza tego rodzaju zdarzenie, może nie być w stanie samodzielnie określić, czy zdarzenie stanowi naruszenie ochrony danych osobowych [449].

W przypadku gdy w wyniku procesu klasyfikacji naruszenia ochrony danych osobowych administrator danych uzna, że dane naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, wówczas administrator musi niezwłocznie poinformować osoby, których dane dotyczą, o naruszeniu. Zakres notyfikacji wynikający z art. 34 ust. 2 RODO w związku z naruszeniem jest nieznacznie zawężony w stosunku do zakresu wynikającego z treści art. 33 ust. 3 RODO. Nie obejmuje on informacji na temat specyfiki naruszenia ochrony danych z art. 33 ust. 3 lit. a RODO. Administrator danych jest zobowiązany do poinformowania podmiotów danych w zakresie: wskazania możliwych konsekwencji naruszenia ochrony danych osobowych; wskazania odpowiedniego punktu kontaktowego oraz

448 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?*, op. cit.

449 P. Fajgielski, *Dokumentacja naruszeń ochrony danych osobowych,* op. cit., str. 178

danych inspektora ochrony danych, od którego można uzyskać więcej informacji, a także wskazania zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu [450].
Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na 4 sposoby. Elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP lub za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl. Możliwe jest również przesłanie zgłoszenia tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu [451].

Administrator danych nie musi realizować obowiązku notyfikacyjnego w przypadku, gdy zostały zastosowane odpowiednie środki techniczne i organizacyjne, jak np. szyfrowanie, które uniemożliwią odczyt danych osobowych osobom do tego nieuprawnionym (art. 34 ust. 3 lit. a RODO). Zwolnienie z obowiązku notyfikacji podmiotu danych przysługuje również w przypadku, gdy administrator danych zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (art. 34 ust. 3 lit. b RODO). Administrator danych musi zatem dokonać przeglądu stosowanych środków technicznych, jak np. szyfrowanie, pseudonimizacja czy minimalizacja oraz szczegółów dot. zakresu naruszenia po to, aby przeprowadzić ocenę możliwości zastosowania zwolnienia z art. 34 ust. 3 lit. b RODO. Ostatnim zwolnieniem z obowiązku notyfikacji podmiotu danych jest przesłanka niewspółmiernie dużego wysiłku (art. 34 ust. 3 lit. c RODO) w realizacji tego obowiązku. Administrator danych wówczas stosuje alternatywne środki notyfikacji o naruszeniu w postaci wydania publicznego komunikatu lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. Należy zwrócić uwagę na to, że argument związany z wysokimi kosztami notyfikacji jako niewspółmiernie duży wysiłek nie jest wystarczający, aby administrator mógł uznać możliwość zastosowania omawianego przepisu [452].

Dobrym podejściem jest podawanie przykładów odnoszących się do konkretnego interesu danej osoby. W przypadku procesu zatrudnienia warto uzmysłowić pracownikowi,

450 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?,* op. cit.

451 Urząd Ochrony Danych Osobowych, Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, Warszawa, czerwiec 2019 r., https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjBxJzbtNPvAhWwxIsKHbPpB4sQFjAAegQIBBAD&url=https%3A%2F%2Fuodo.gov.pl%2Fpl%2Ffile%2F2210&usg=AOvVaw1PVnALtheH0KHIb5s325OA , dostęp z dnia 16.03.2021 r.

452 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?,* op. cit.

jakie mogą być konsekwencje dla niego samego w momencie wycieku danych, co pozwoli mu lepiej zrozumieć zasadność ochrony danych. Raczej nikt nie chciałby usłyszeć przez telefon, że w wyniku incydentu bezpieczeństwa jego dane wyciekły i mogą być wykorzystane w działaniach przestępczych polegających na wyłudzaniu pieniędzy, więc dla własnego bezpieczeństwa musi zastrzec swoje dokumenty czy zabezpieczyć karty płatnicze. Władcza postawa IOD, imperatywny sposób przekazywania informacji i zaleceń nie pomogą w powstrzymywaniu niekorzystnego zjawiska, jakim jest niechęć do ochrony danych osobowych w organizacji. Dobry IOD pokazuje ryzyko, jakie wiąże się z określonymi działaniami, uświadamia, jakie mogą być konsekwencje nieprawidłowości, podejmuje próbę uświadomienia pracowników, dlaczego metody, działania i narzędzia, jakimi posługiwali się wcześniej, nie mogą być dalej akceptowane i dlaczego stoją one w sprzeczności z przepisami. Warto wskazać pracownikom, jakie zagrożenia wiążą się z przetwarzaniem danych i jakie konsekwencje może nieść dla podmiotów danych (a więc także ich samych) brak odpowiedniego zabezpieczenia [453].

IOD powinien uczulić pracowników, iż najpopularniejszym sposobem zabezpieczenia jest program antywirusowy, dość skuteczny w wykrywaniu oprogramowania malware. Kolejnym ważnym elementem jest *firewall*, który filtruje ruch, jaki jest „wpuszczany" do naszego komputera. Te zabezpieczenia jednak często nie chronią nas tak, jakbyśmy sobie tego życzyli, dlatego warto przeglądać rankingi i zestawienia przed wyborem odpowiedniego oprogramowania tego typu. Nic nie zastąpi jednak rozwagi użytkownika. Przede wszystkim trzeba zwracać uwagę na zagrożenia płynące z poczty elektronicznej czy przeglądanych witryn internetowych [454].

Konkretna lista zagrożeń w większości przypadków działa na wyobraźnię i pozwala lepiej uświadomić wagę zagrożenia. Przykładami wskazanych działań mogą być: zakładanie i prowadzenie fałszywej działalności, której celem są wyłudzenia VAT, wyłudzanie kredytów gotówkowych i hipotecznych, fałszerstwa dowodów osobistych, paszportów, podszywanie się pod osobę przy pomocy fałszywego konta e-mail lub profilu społecznościowego w celu wyłudzania pieniędzy. Wśród pozostałych zagrożeń można wymienić wynajmowanie mieszkań, pokojów hotelowych, samochodów, przyjmowanie mandatów lub punktów karnych na fałszywe dane, czy zawieranie umów z operatorami telekomunikacyjnymi na fałszywe dane.

453 M. Kołodziej, *Vademecum IOD*, C.H. Beck, Warszawa 2020, str. 39

454 M. Jakubik, P. Wojciechowski, *RODO w IT: atak hakerski a ochrona danych osobowych*, Lex/el. 2020, dostęp z dnia 16.03.2021 r.

W trakcie szkoleń można przytoczyć także przykłady wycieków danych i ich częstotliwość. Warto uświadomić uczestników szkolenia, że takie przypadki są codziennością – podejście „nas to nie dotyczy" może być zgubne dla organizacji i podmiotów danych (a także pracowników). Za przykład może służyć lista wycieków z okresu od czerwca 2018 r. do lutego 2019 r., które omówiono w mediach branżowych, jak MyHeritage.com – w czerwcu 2018 r. dotyczący 92 mln rekordów danych, czy Urzędu Skarbowego we Wrocławiu – w czerwcu 2018 r., gdzie udostępniono dla petentów komputer z dostępem do Internetu i drukarki, na którym w folderze pobrane znajdowały się wypełnione druki PIT oraz potwierdzenia zapłat, a na biurkach dla petentów – ich wydruki. Kolejne wycieki we wrześniu 2018 r. Facebook, gdzie wyciekło 50 mln rekordów danych, następnie wyciek ponad 533 milionów użytkowników Facebooka, w tym dane ponad 2,5 miliona Polaków w kwietniu 2019 r. (Prezes UODO wystąpił do władz Facebook Poland o podjęcie działań w celu ograniczenia ryzyka wykorzystania danych osobowych objętych naruszeniem poprzez zaoferowanie usługi umożliwiającej wszystkim polskim użytkownikom sprawdzenia, czy naruszenie to ich dotyczy [455]), a w październiku 2018 r. Google, gdzie w wyniku zatajonej luki systemu uzyskano dostęp do 500 tys. rekordów. Nie sposób nie wspomnieć o Wietnamwiza.pl, z której w styczniu 2019 r. wyciekło ponad 3000 skanów polskich paszportów. Powyższe pokazuje, że dane osobowe nie zawsze są bezpieczne – nawet w tak dużych podmiotach jak Google,co, do których powinna być pewność w zakresie stosowania najwyższego poziomu bezpieczeństwa. Budowanie świadomości ryzyka pracowników organizacji można dodatkowo poprzeć przykładami, takimi jak sytuacja dotycząca dostępu do danych wystawionych na sprzedaż w Internecie w formie zbiorczej bazy, określonej jako Collection #1. Jest ona sprzedawana nielegalnie w tzw. deepweb lub darknet, będących obszarem sieci Internet, do którego dostęp uzyskuje się za pomocą TOR (ang. The Onion Router) – anonimowej wirtualnej sieci komputerowej. W bazie tej znajduje się 773 mln adresów e-mail i 21 mln haseł pochodzących z ponad 2000 serwisów (także polskich). Wieczysty dostęp do rzeczonej bazy wraz z regularnymi aktualizacjami kosztuje jedynie 45 dolarów. Pracownikom warto tez zwrócić uwagę na problem używania przez nich takich samych danych dostępowych (loginy i hasła lub same hasła) w sferze zarówno zawodowej, jak i prywatnej. Jeżeli przestępca uzyska dane logowania do konta w jednym z tego typu serwisów, z dużym prawdopodobieństwem będzie mógł uzyskać dostęp do służbowych zasobów pracownika [456].

455 https://uodo.gov.pl/pl/138/2022 , dostęp z dnia 6.06.2021 r.

456 M. Kołodziej, *Vademecum IOD*, op. cit., str. 40

Zadaniem IOD powinno być uświadomienie konieczności wdrożenia w organizacji lub aktualizacji planu ciągłości działania. Plan ciągłości działania jest niezbędny nie tylko do właściwego oszacowania ryzyka, ale również zaplanowania działań na wypadek ataku hakerskiego, na skutek którego może zostać utracona dostępność danych czy też usługa może stać się niedostępna. Dokument ten największe znaczenie powinien mieć dla obszaru IT, gdyż uświadamia, bez jakich danych czy też usług biznes nie może działać i które z nich są kluczowe do tego, by móc nadal funkcjonować. Dobrze zrobiony plan ciągłości działania ukazuje, jakie systemy czy dane, w tym dane osobowe, należy uznać za krytyczne dla działania organizacji [457].

Nie sposób tu nie wspomnieć o ataku, jaki miał miejsce na Urząd Marszałkowski w Krakowie 8 lutego 2021 r., gdzie systemy instytucji zostały zaszyfrowane za pomocą złośliwego oprogramowania, a hakerzy zażądali okupu za ich odblokowanie. Na skutek działania wirusa doszło do „utraty dostępności danych osobowych", w tym m.in. klientów Urzędu [458]. Podobna sytuacja miała miejsce w Starostwie Powiatowym w Oświęcimiu, które zapłaciło ponad 600 tys. zł. za odzyskanie danych, po tym, jak 13 października 2020 roku hakerzy zaatakowali serwer z bazami danych Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej w Oświęcimiu. Starosta oświęcimski o ataku hakerskim powiadomił policję, CERT Polska, czyli zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w Internecie, i Urząd Ochrony Danych Osobowych [459].

Mając powyższe na uwadze nie sposób nie odnieść się do kontroli NIK dot. wprowadzania RODO, jaka miała miejsce w urzędach dużych miast, podobnie jak o wspomnianej w III rozdziale niniejszej pracy kontrola NIK w samorządach. We wszystkich kontrolowanych urzędach przed wejściem w życie przepisów RODO opracowano regulacje dotyczące niezbędnych działań, które powinny zostać podjęte w przypadku ewentualnego naruszenia ochrony danych osobowych. Kontrola wykazała natomiast dwa przypadki nieprawidłowego postępowania już po stwierdzeniu naruszenia ochrony danych osobowych, m.in. w Urzędzie Miasta Ciechanów. Cztery osoby zgłosiły tam takie nieprawidłowości w związku z głosowaniem w ramach budżetu obywatelskiego na 2020 r. Prezydent miasta złożył w tej sprawie doniesienie w Komendzie Policji, nie przekazał jednak informacji

457 M. Jakubik, P. Wojciechowski, *RODO w IT: atak hakerski a ochrona danych osobowych*, op. cit.

458https://www.cyberdefence24.pl/atak-na-urzad-marszalkowski-w-krakowie-nadal-nie-dziala-system-informatyczny, dostęp z dnia 28.03.2021 r.

459 https://naszkrakow.com.pl/2021/03/10/czy-mamy-do-czynienia-z-seria-atakow-hakerskich/, dostęp z dnia 16.03.2021 r.

o naruszeniu danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, co - według NIK - było niezgodne z RODO. NIK oceniła, że w większości skontrolowanych przypadków działania w reakcji na stwierdzone naruszenia ochrony danych osobowych oraz żądania ich usunięcia lub sprostowania były prowadzone prawidłowo [460].

W związku z wszelkimi cyberatakami może dojść do kradzieży czy też braku dostępności danych, w tym danych osobowych. Dlatego tak ważny jest udział IOD w analizie zdarzeń wpływających na cyberbezpieczeństwo. Udział ten nie tylko pozwala na właściwe rozpoznanie, czy doszło do naruszenia danych osobowych, ale również na podjęcie odpowiednich działań. Dodatkowo udział IOD pozwala w przypadku, gdy będzie taka potrzeba, przygotować odpowiednie zgłoszenie do UODO [461].

W przepisie art. 33 RODO, nakładającym na administratorów wymóg zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych, zawarty został ust. 5, w którym przewidziano obowiązek polegający na dokumentowaniu naruszeń oraz wskazano główny cel tego obowiązku. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu" Dla prawidłowego wypełniania obowiązku zgłaszania naruszeń organowi nadzorczemu oraz dokumentowania naruszeń przez administratora istotne jest określenie odpowiedniej procedury postępowania przez osoby przetwarzające dane (pracowników, osoby wykonujące prace zlecone), które uzyskają informację o podejrzeniu lub zaistnieniu naruszenia. Osoby takie powinny być obowiązane do zgłoszenia zaistnienia tych okoliczności IOD (bądź innej wskazanej osobie, jeżeli w danej jednostce organizacyjnej inspektor ochrony danych nie został wyznaczony). Nałożenie tego rodzaju obowiązku może znaleźć się w instrukcji postępowania w przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych, która to instrukcja nadal funkcjonuje w wielu jednostkach organizacyjnych [462].

Nie sposób nie wspomnieć tutaj o karze pieniężnej nałożonej przez Prezesa UODO w wysokości ponad 1,1 mln złotych z powodu zbyt później identyfikacji incydentów i powiadamiania o nich osób, których dane dotyczą oraz zgłaszania naruszeń organowi nadzorczemu. Brak wdrożonych odpowiednich środków organizacyjnych i technicznych pozwalających szybko identyfikować naruszenia powodował, że osoby, których dane dotyczą,

460 https://samorzad.pap.pl/kategoria/aktualnosci/nik-o-wprowadzaniu-rodo-w-urzedach-duzych-miast-pojedyncze-potkniecia, dostęp z dnia 16.03.2021 r.

461 M. Jakubik, P. Wojciechowski, *RODO w IT: atak hakerski a ochrona danych osobowych*, op. cit.

462 P. Fajgielski, *Dokumentacja naruszeń ochrony danych osobowych,* op. cit., str.176-177

przez długi czas nie wiedziały o ryzyku wykorzystania ich danych przez osoby nieuprawnione, np. do tzw. kradzieży ich tożsamości. Nie mogły też przez ten czas podjąć działań, które ograniczyłyby takie niebezpieczeństwo. Nie ma tu znaczenia fakt, że naruszenia związanie były z nieprawidłowościami po stronie firmy kurierskiej, ponieważ to właśnie ukarany administrator danych nieprawidłowo realizował nadzór nad egzekwowaniem postanowień umownych, przez co dochodziło do późnej identyfikacji naruszeń [463].

W ramach ustalania zasad postępowania w sytuacji naruszenia ochrony danych administrator danych powinien określić w nich udział IOD. Zazwyczaj IOD wchodzi w skład zespołu wyznaczanego do wyjaśniania sytuacji związanych z naruszeniami ochrony danych lub podejrzeniami zajścia takich sytuacji. Zdarzają się też rozwiązania, w których powoływany jest zespół ds. wyjaśniania incydentów związanych z bezpieczeństwem informacji, który konsultuje się z IOD jedynie w sytuacjach związanych z podejrzeniem naruszenia ochrony danych, na potrzeby potwierdzenia właściwego stwierdzenia zajścia takiego zdarzenia. Zespół, w którego skład zwykle wchodzi IOD, ma takie zadania, jak analiza zgłoszonych sytuacji podejrzenia naruszenia ochrony danych, stwierdzenie naruszenia ochrony danych, ocena poziomu ryzyka naruszenia praw osób, których dane dotyczą, określenie konieczności zgłaszania zawiadomienia o naruszeniu ochrony danych do Prezesa UODO. Należy również tu wyróżnić pozostałe zadania dotyczące określenia konieczności poinformowania osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych, podejmowanie działań zaradczych, czy dokumentowanie naruszeń ochrony danych osobowych. Podczas zgłoszenia naruszenia IOD jest zazwyczaj wskazywany jako punkt kontaktowy dla organu nadzorczego. W związku z tym przedstawiciele Prezesa UODO prowadzący daną sprawę kontaktują się z IOD w sprawach dotyczących złożonego wniosku. Zazwyczaj chodzi o doprecyzowanie informacji, np. czy zostały poinformowane osoby, których danych dotyczyło zdarzenie, w sytuacji gdy we wniosku podano przyszłą datę wykonania tej czynności (takie pytanie usłyszałem, gdy po raz pierwszy kontaktował się ze mną inspektor z nowego urzędu w czerwcu2018 r.). Zadaniem IOD jest bardzo często również dokumentowanie sytuacji naruszenia ochrony danych [464].

Kluczowa jest współpraca oraz nić porozumienia na linii IOD a obszar IT. Inspektor ochrony danych powinien być poinformowany o każdorazowym cyberataku, który miał miejsce i na skutek którego mogło dojść do wycieku czy też kradzieży danych, które były danymi osobowymi. IOD powinien być poinformowany nie tylko o konkretnej kradzieży danych, ale

463 https://uodo.gov.pl/pl/138/2048, dostęp z dnia 6.06.2021 r.

464 M. Kołodziej, *Vademecum IOD*, op. cit., str. 13

również o każdej próbie dostępu do danych. Powinien on po uzyskaniu informacji z obszaru IT sporządzić raport dla administratora danych osobowych o zaistniałej sytuacji, ze szczególnym uwzględnieniem, czy działanie miało znamiona naruszenia oraz czy miało wpływ na integralność, poufność i dostępność danych osobowych. Po uzyskaniu informacji IOD powinien w swojej rekomendacji zawrzeć nie tylko faktyczny opis zaistniałej sytuacji, ale również określić, czy działanie posiadało znamiona naruszenia ochrony danych osobowych, czy też mogło mieć wpływ na wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczyły. W kwestii informacji czysto technicznych powinny zostać one przedstawione IOD w sposób zrozumiały i zwięzły, gdyż nie jest on zobligowany do posiadania wiedzy w zakresie cyberbezpieczeństwa. Inspektor ochrony danych powinien w organizacji wypracować konkretną ścieżkę zgłaszania tego typu naruszeń/incydentów, gdyż powinien być świadomy występujących zdarzeń oraz ryzyka, które się z tym wiążą. W przypadku gdy IOD oceni, że konkretne zdarzenie posiada znamiona naruszenia danych osobowych, to powinien on w terminie 72 godzin od powzięcia informacji poinformować organ nadzorczy o zaistniałym fakcie. W przypadku gdy posiada szczątkowe informacje, to zgłoszenie do UODO powinno wpłynąć w takim zakresie, w jakim IOD posiada wiedzę, a następnie powinno być sukcesywnie uzupełniane, by ostatecznie było kompletne [465].

Zarówno zgłoszenie naruszenia ochrony danych, jak i wewnętrzna dokumentacja dotycząca naruszenia ochrony danych muszą spełnić określone wymagania formalne. Na podstawie art. 33 ust. 3 RODO dokumentacja zgłoszenia ochrony danych osobowych musi zawierać elementy dotyczące specyfiki naruszenia ochrony danych, danych kontaktowych właściwego punktu kontaktowego, ocenę konsekwencji naruszenia ochrony danych osobowych oraz charakterystykę podjętych lub proponowanych działań w celu uniknięcia podobnych naruszeń ochrony danych w przyszłości. Opis charakteru naruszenia ochrony danych w myśl art. 33 ust. 3 lit. a RODO musi zawierać szczegółowe informacje dotyczące kategorii danych osobowych (np. klienci sklepu internetowego), przybliżoną liczbę osób objętych naruszeniem oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie [466]. Dokumentacja powinna pozwolić organowi nadzorczemu na weryfikowanie przestrzegania przepisu dotyczącego zgłaszania naruszeń, można uznać, że dokumentacja powinna zawierać jeszcze co najmniej jeden element: informację, czy naruszenie zostało zgłoszone do organu nadzorczego, a jeżeli nie, to wskazanie powodów braku zgłoszenia. Wskazany powyżej zakres

465 M. Jakubik, P. Wojciechowski, *RODO w IT: atak hakerski a ochrona danych osobowych*, op. cit.

466 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?*, op. cit.

ma charakter minimalny i może być rozszerzany o inne kategorie informacji, jeżeli administrator uzna to za potrzebne [467].

Na podstawie art. 33 ust. 5 RODO administrator danych jest zobowiązany do dokumentowania naruszeń ochrony danych osobowych. Dokumentacja zawarta w rejestrze naruszeń ochrony danych osobowych powinna uwzględniać okoliczności naruszenia, jego skutki oraz wykaz podjętych działań zaradczych. Dokumentacja powinna być na tyle szczegółowa, aby było możliwe prawidłowe zweryfikowanie przestrzegania art. 33 RODO [468]. W ramach prowadzenia dokumentacji związanej z naruszeniami ochrony danych osobowych zdaniem M. Kołodzieja powinny się tam znaleźć następujące rodzaje dokumentów:

1)zgłoszenia incydentów skutkujących naruszeniem ochrony danych od pracowników poszczególnych działów, od działu IT oraz od podmiotu przetwarzającego,

2)raport z postępowania wyjaśniającego dotyczącego wystąpienia incydentu skutkującego naruszeniem ochrony danych osobowych, w tym ocena poziomu ryzyka naruszenia praw osób, których dane dotyczą, oraz wykaz zaleceń lub działań zaradczych w celu zminimalizowania wystąpienia incydentu w przyszłości,

3)kopia zgłoszenia naruszenia ochrony danych do Prezesa UODO,

4)kopie listów z zawiadomieniami osób, których dane dotyczą, o naruszeniu ich danych osobowych,

5)ewidencja naruszeń ochrony danych osobowych,

6)raport z wykonania zaleceń lub podjęcia działań zaradczych przez poszczególne komórki organizacyjne administratora danych. W ramach przeprowadzania działań zaradczych związanych z naruszeniem IOD powinien przygotowywać materiały informacyjne lub szkoleniowe dla pracowników, dotyczące zaistniałych sytuacji naruszenia, w celu zminimalizowania ryzyka ich wystąpienia w przyszłości [469].

Określenie „administrator dokumentuje wszelkie naruszenia" może być także różnie rozumiane. Pomimo że przepis wyraźnie nie wymaga prowadzenia rejestru naruszeń, to wydaje się, że dokumentowanie naruszeń może być efektywnie realizowane właśnie w tej postaci, tzn. przez odnotowywanie wszystkich naruszeń w stworzonym specjalnie w tym celu rejestrze (ewidencji). Jednak można uznać, że określenie „dokumentuje" oznacza coś więcej niż tylko odnotowanie informacji i wymaga gromadzenia dokumentów, które mają istotne znaczenie dla

467 P. Fajgielski, *Dokumentacja naruszeń ochrony danych osobowych,* op. cit., str. 177

468 P. Siemieniak, *RODO w IT: atak hakerski i co dalej?*, op. cit.

469 M. Kołodziej, *Vademecum IOD*, op. cit., str. 14

oceny zaistniałego naruszenia i dalszego postępowania administratora. Wśród tych dokumentów znaleźć się powinny materiały potwierdzające informacje wskazane w rejestrze naruszeń, w tym. m.in. zawiadomienia o podejrzeniu naruszenia składane przez pracowników – jeżeli zostały złożone na piśmie, zgłoszenia pochodzące od podmiotów przetwarzających, jak również kopie zgłoszeń kierowanych do organu nadzorczego. Sformułowanie „wszelkie naruszenia" oznacza, że obowiązek dokumentacyjny jest zakreślony szeroko i obejmuje nie tylko naruszenia, które podlegają zgłoszeniu do organu nadzorczego, ale także naruszenia, z którymi nie wiąże się obowiązek zgłoszeniowy, tzn. naruszenia, w przypadku których administrator uzna, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych [470].

Zgodnie z wytycznymi Grupy Roboczej Art. 29 dotyczącymi zgłaszania naruszeń ochrony danych osobowych IOD powinien odgrywać kluczową rolę we wspieraniu administratora danych w zapobieganiu naruszeniom, przygotowaniu się na wypadek ich wystąpienia oraz w sytuacji wystąpienia takiego naruszenia. Zalecane jest, aby niezwłocznie informować IOD o wystąpieniu naruszenia oraz włączać go do procesu zarządzania taką sytuacją, w tym do zgłaszania informacji o naruszeniu do organu nadzorczego [471].

470 P. Fajgielski, *Dokumentacja naruszeń ochrony danych osobowych,* op. cit., str.178

471 M. Kołodziej, *Vademecum IOD*, op. cit., str. 13

Podsumowanie i wnioski końcowe

W polskim porządku prawnym istnieje konieczność kompleksowego uregulowania zawodu IOD mając na uwadze wymogi kwalifikacyjne niezbędne do wykonywania zadań na tym stanowisku, zasady nabywania uprawnień i ich weryfikacji oraz opracowania jednoznacznych kryteriów wskazujących na obowiązek wyznaczenia inspektora zarówno w jednostkach sektora finansów publicznych, jak i w sektorze prywatnym. Jednocześnie wewnątrzorganizacyjne kompetencje, uprawnienia i sposób wykonywania zadań przez IOD wymagają kompleksowej zmiany podejścia do tego zawodu, analogicznie do uprawnień i zadań osób kierujących komórką audytu wewnętrznego. Niniejsza dysertacja stanowi odpowiedź na zasady podejścia do zawodu IOD w ujęciu w ujęciu systemowym. Mając powyższe na uwadze w celu udowodnienia tezy głównej pozytywnie zweryfikowane zostały tezy pomocnicze. Analiza poglądów wyrażonych w doktrynie, literaturze orzecznictwie i piśmiennictwie administracyjnym, jak również dorobku acquis i stanowisko organów kontrolnych w zakresie badanej problematyki, a następnie ukazane podeście praktyczne w oparciu o syntezę i analizę obejmującą badanie dokumentacji, wyniki przedstawionych statystyk i obserwacja uczestnicząca potwierdziły poprawność sformułowanych hipotez badawczych. W niniejszej pracy zaznaczono, że zarówno RODO, jak i UODO nie dostarczają szczegółowych wytycznych w zakresie wymaganych kompetencji oraz sposobów ich weryfikacji. Zwrócono również uwagę na pozostałe szczególnie istotne wymogi formalne, które dotyczyły ABI, takie jak wymóg niekaralności, posiadania pełnej zdolności do czynności prawnych, czy korzystania z pełni praw publicznych. Jednakże ustawodawca w ustawie OchrDanychZwPrzestU wskazał ww. wymogi wobec IOD (nieskazanie, pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych) jednocześnie je pomijając w obowiązującej UODO. Ponadto w pracy wykazano, że pragmatyka wskazuje nieliczne przykłady dotyczące takich wymagań na stanowisku IOD, jak wymóg ukończenia studiów drugiego stopnia (przepisy dotyczące stanowisk i szczegółowych zasad wynagradzania urzędników i innych pracowników sądów i prokuratury, wprowadzające stanowisko inspektora ochrony danych w sądach powszechnych i wojskowych), czy wymóg posiadania wykształcenia wyższego oraz 7 lat pracy, w tym na stanowisku kierowniczym (wykaz stanowisk urzędniczych w Biurze Krajowej Rady Radiofonii i Telewizji). Podkreślono również znaczenie wytycznych dla inspektorów ochrony danych w instytucjach EU, w których zalecane jest wymaganie od IOD co najmniej siedmiu lat odpowiedniego doświadczenia w instytucji lub organie, w których ochrona danych jest związana z podstawową ich działalnością lub które mają istotny wolumen operacji przetwarzania danych osobowych.

Jednocześnie w pracy wykazano, że osoba zatrudniona na stanowisku IOD powinna na bieżąco zapewniać i doradzać najwyższemu kierownictwu w podejmowaniu decyzji i prowadzić systematyczny monitoring przestrzegania przepisów ODO, m.in. w obszarach takich, jak zamówienia publiczne, proces zatrudnienia, właściwe stosowanie monitoringu wizyjnego, nadzorowanie procesów udostępniania i powierzania danych osobowych. Kluczowe dla IOD jest również umiejętność prowadzenia audytów w zakresie bezpieczeństwa informacji i ochrony danych osobowych, wiedza z zakresu szacowania ryzyka, czy wreszcie wiedza praktyczna dotycząca zastosowań technologii informacyjno-komunikacyjnych i bezpieczeństwa teleinformatycznego, w tym w zakresie najlepszych praktyk zabezpieczeń dotyczących przetwarzania informacji chronionych. Weryfikacja przez pracodawcę faktycznie posiadanej wiedzy przez kandydata poprzez przeprowadzenie testu wiedzy, uwzględniającego przepisy szczególne i specyfikę branży, w której działa ADO może okazać się niewystarczająca. Warto przeprowadzić również weryfikację kompetencji i umiejętności IOD, co do rzetelnego i fachowego wypełniania przez niego zadań, tj. umiejętność wydawania zaleceń oraz przeprowadzania zadań audytowych, czy analizy ryzyka.

Mając powyższe na uwadze oraz praktykę i rozwiązania przyjęte w poszczególnych krajach członkowskich oraz brak szczegółowych wymogów i regulacji dotyczących zawodu IOD w polskim porządku prawnym, jak również mechanizmów weryfikujących umiejętności kandydatów na to stanowisko zaproponowano rozwiązanie konieczności uregulowania powyższego na gruncie przepisów krajowych. W dysertacji zaproponowano uszczegółowienie w UODO niezbędnych wymogów na stanowisku IOD poprzez wprowadzenie obowiązku ukończenia studiów podyplomowych z zakresu bezpieczeństwa informacji i ochrony danych osobowych kończących się egzaminem zawodowym oraz obowiązku odbycia co najmniej dwuletniej praktyki pod nadzorem doświadczonego IOD. Odbycie dwuletniej praktyki powinno być odpowiednio udokumentowane i określone w ustawie poprzez potwierdzenie przez kierownika jednostki wykonywania czynności, o których mowa w art. 39 ust. 1 i 2 RODO pod nadzorem IOD. Nie sposób nie wspomnieć o pozostałych wymogach formalnych, które dotyczyły ABI, takich jak wymóg niekaralności, posiadania pełnej zdolności do czynności prawnych, czy korzystania z pełni praw publicznych, który to wymóg dotyczy najczęściej tylko pracowników administracji publicznej zgodnie z przepisami sektorowymi. W pracy podkreślono, że program studiów powinien być oparty nie tylko na zagadnieniach dotyczących przepisów z zakresu ochrony danych osobowych i prawnego otoczenia funkcjonowania IOD, ale również o takie elementy, jak planowanie i realizacja kontroli, sprawdzeń i audytów w zakresie związanym z zabezpieczeniem informacji oraz infrastruktury informatycznej,

projektowanie i kontrola obszaru bezpieczeństwa fizycznego i środowiskowego. Kluczowe będą również zagadnienia związane z zarządzaniem ryzykiem w obrębie ochrony danych osobowych, czy systemowe podejście do zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy ISO/IEC 27001:2013. Zamiast obowiązku ukończenia studiów podyplomowych należy również dopuścić możliwość uzyskania certyfikacji IOD, które mogłyby być przyznawane przez podmioty certyfikujące akredytowane przez Prezesa UODO. Wykonywanie funkcji IOD wymaga również rzetelnego podejścia i wysokiego poziomu etyki zawodowej.

W kwestii obowiązku wyznaczenia IOD podkreślono, że RODO nakłada na niektórych ADO taki obowiązek, co stanowi istotną zmianę w porównaniu z pełną fakultatywnością powoływania ABI. Jednakże z uwagi na bardzo ograniczony katalog organów i podmiotów publicznych zobowiązanych do wyznaczenia IOD z pominięciem regulacji k.p.a. w dysertacji wskazano na potrzebę jednoznacznego wskazania przez ustawodawcę krajowego obowiązku wyznaczenia IOD przez podmioty z sektora publicznego, w tym podmioty powiązane z sektorem publicznym, a w przypadku sektora prywatnego uzależniające obowiązek wyznaczenia IOD od liczby zatrudnionych osób. Wskazane rozwiązanie zostało oparte na wytycznych GR Art. 29 oraz na rozwiązaniach przyjętych w poszczególnych krajach członkowskich. Zaznaczono, że brak konieczności wyznaczenia IOD zarówno w sektorze publicznym, jak i w prywatnym powinien być poprzedzony przeprowadzeniem analizy i udokumentowany. Zwrócono również uwagę na konieczność usunięcia niezgodności przepisów prawa krajowego z art. 37 ust. 7 RODO dotyczący obowiązku publikacji na stronie internetowej podmiotu imienia i nazwiska inspektora. W tym miejscu dobrą praktyką jest publikowanie dodatkowych informacji przez ADO ułatwiających kontakt z IOD, jak adres e-mail, czy nr telefonu.

Przedstawione w niniejszej pracy statystyki dotyczące IOD potwierdziły, że nadinterpretacje możliwości wyznaczenia wspólnego IOD dla kilku organów lub podmiotów publicznych mogą prowadzić do stworzenia fikcyjnego stanowiska oraz braku możliwości faktycznej realizacji zadań przez IOD, co może sprzyjać naruszeniom przepisów o ochronie danych osobowych. W dysertacji wykazano, iż przed podjęciem takiej decyzji należy dokonać weryfikacji dostępności, niezależności i nawiązania łatwego kontaktu z IOD mając na uwadze strukturę organizacyjną, przepisy i procedury ochrony danych, w tym przepisy administracyjne obowiązujące w tych jednostkach oraz wielkość administratorów. Analogicznie należy postępować w przypadku wyznaczenia jednego IOD dla grupy przedsiębiorstw. Przedstawiona weryfikacja powinna obejmować również zapewnienie

standardów niezależności i efektywność działań IOD w zakresie monitorowania prawidłowości procesów przetwarzania danych osobowych i skutecznej reakcji IOD w przypadku incydentów bezpieczeństwa, czy innego rodzaju naruszenia praw podmiotów danych. Nie sposób nie wspomnieć również o zapewnieniu odpowiedniego organizacyjnego i technicznego wsparcia IOD oraz wykluczeniu możliwości wystąpienia konfliktu interesów.

W pracy zwrócono również uwagę na przeciwdziałanie nieprawidłowościom polegającym na przypisywaniu IOD obowiązków w formie dodatkowych zadań już zatrudnionym pracownikom i występowania konfliktu interesów (dotyczącego zarówno stanowisk kierowniczych, jak również takich, które biorą udział w określaniu celów i sposobów przetwarzania danych). Badanie przeprowadzone w jednostkach samorządu terytorialnego wykazało, że w 8 z 13 badanych jednostek ABI, a obecnie IOD wykonuje czynności na innych stanowiskach, takich, jak sekretarz powiatu, naczelnik wydziału organizacyjnego, informatyk, czy kierownik wydziału ds. informatyki, co jednoznacznie może powodować konflikt interesów. Zaakcentowano również konieczność podjęcia pilnych działań legislacyjnych w celu uwzględnienia stanowiska IOD w tabeli grup stanowisk urzędniczych w służbie cywilnej, co w oczywisty sposób zostało pominięte i może powodować naruszenie zasady bezpośredniej podległości IOD najwyższemu kierownictwu. Niezwykle istotny jest aktywny udziału IOD we wszystkich sprawach związanych z przetwarzaniem i ochroną danych osobowych, w tym w ramach bieżących lub projektowanych procesów realizowanych w organizacji, tj. spotkania najwyższego kierownictwa udział w Komisjach, Zespołach i innych czynnościach. Niezbędne informacje powinny zostać udostępnione IOD odpowiednio wcześniej, umożliwiając inspektorowi zajęcie stanowiska. Podkreślono przy tym nieskuteczne i bezcelowe przypadki stosowania niedozwolonych klauzul w uchwałach zarządów i zarządzeniach podmiotów publicznych polegających na próbie przenoszenia odpowiedzialności za zapewnienie poufności danych osobowych na IOD. Wskazano również na konieczność weryfikacji przez ADO, czy podmioty świadczące usługi IOD spełniają formalne wymogi prowadzenia działalności, czyli legitymują się odpowiednimi uprawnieniami w zakresie zgłoszenia PKD w ramach swojej działalności oraz wymóg posiadania polisy ubezpieczeniowej od odpowiedzialności cywilnej z tytułu wykonywanej funkcji. Biorąc pod uwagę rozmiar i strukturę jednostki oraz zadania, w tym realizowane przez IOD, a także fakt jego zastępstwa w czasie jego usprawiedliwionej nieobecności istnieje konieczność, podobnie, jak to miało miejsce w przypadku ABI, powołania zespołu wspomagającego pracę IOD, w tym zastępcy IOD.

Mając powyższe na uwadze w niniejszej dysertacji omówione zostały szczególnie istotne z punktu widzenia IOD jako audytora fundamentalne i kluczowe dla organizacji

czynności doradcze na przykładach praktycznych. I tak w zakresie udostępniania danych osobowych podkreślono konieczność udziału IOD poprzez każdorazową weryfikację podstaw prawnych upoważniających do udostępnienia danych osobowych oraz pełnienia nadzoru nad prowadzeniem rejestru udostępnień danych osobowych oraz prawidłowością obsługi tego procesu. W przypadku procesu dotyczącego powierzania danych osobowych zaznaczono, iż IOD powinien być każdorazowo zapraszany na spotkania z osobami nadzorującymi proces przygotowania współpracy z przyszłym dostawcą. Nie sposób tu nie wspomnieć o konieczności przeprowadzenia z udziałem IOD weryfikacji dostawcy pod kątem stosowania przez niego odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z przepisami prawa w zakresie ochrony danych osobowych oraz posiadania przez niego odpowiedniej wiedzy fachowej, a także zasobów do realizacji przetwarzania powierzonych danych. Bardzo ważnym elementem w tym zakresie jest przygotowanie we współpracy z IOD listy kontrolnej wspierającej taką weryfikację i analiza odpowiedzi udzielonych przez podmiot przetwarzający. Nie sposób nie wspomnieć o roli IOD w zakresie przygotowania i analizy postanowień umowy powierzenia przetwarzania danych osobowych pod kątem wystąpienia niedozwolonych klauzul umownych (utrudniających lub uniemożliwiających przeprowadzenie przez ADO audytów u podmiotu przetwarzającego, ograniczających jego odpowiedzialność do określonej w umowie kary, czy kwoty, a także dotyczących wspierania ADO w wypełnianiu praw osób, których dane dotyczą, czy zawiadamiania ADO o naruszeniu i zapewnienia mu niezbędnej pomocy w tym zakresie) i zapewnienia jej zgodności z przepisami prawa.

Należy zwrócić uwagę na szczególnie istotną rolę doradczą IOD w okresie pandemii w przedmiocie organizacji i wdrożenia zasad i procedur wykonywania pracy zdalnej w organizacji. Zaznaczono przy tym konieczność zapewnienia ich zgodności z obowiązującymi przepisami prawnymi, a także zapewnienia ciągłości działania jednostki, w tym odpowiednich narzędzi oraz bezpiecznych i higienicznych warunków wykonywania pracy i użytkowania sprzętu adekwatnie do zagrożeń i ryzyk z tym związanych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych. Podkreślono również rolę doradczą IOD w kontekście konieczności zabezpieczenia interesów pracodawcy, jego pracowników oraz wielu grup podmiotowych, które z mocy przepisów prawa mają wiele uprawnień i gwarancji, które pracodawca zmuszony jest respektować, jak poszanowanie dóbr osobistych pracownika, zapewnienie narzędzi, procedur i wsparcia pracowników wykonujących pracę zdalną, czy realizacji praw osób, których dane dotyczą. Wspomniano również o konieczności weryfikacji w ramach prowadzonego audytu przestrzegania przez pracowników wdrożonych procedur, w tym zasad bezpiecznego wykonywania pracy zdalnej

(zakup kart SIM pracownikom, zabezpieczenie sprzętu przed dostępem osób nieuprawnionych, łączenie poprzez VPN, szyfrowanie sprzętu i dokumentów, zakaz wynoszenia dokumentów do domu), zgłaszania incydentów i nieprawidłowości, zapewnienia pracownikom odpowiedniego wsparcia ze strony działu IT oraz właściwej inwentaryzacji sprzętu, planowania i raportowania wykonanej pracy zdalnej.

Biorąc pod uwagę wyżej wymienione elementy, należy stwierdzić, że w podejściu modelowym mocno podkreślona została rola IOD, jako audytora. Odniesiono się przy tym do wykonywania zadań przez ABI w tym zakresie. W pracy podkreślono, że w ramach audytu inspektor przygotowuje raport dla administratora lub podmiotu przetwarzającego, który porównać można do sprawozdania wykonywanego przez ABI (zgodnie z wymogami ustawowymi). Należy jednak zaznaczyć, że działania IOD są znacznie bardziej komplementarne. Wśród dobrych praktyk realizacji zadania zapewniającego przez IOD wyszczególniono odpowiednie zaplanowanie zadania audytowego, przeprowadzenie spotkania otwierającego (omawiającego zakres audytu, jego porządek, zasady współpracy), przeprowadzenie czynności sprawdzających (oględziny, analiza dokumentacji, wywiad, obserwacja) oraz zakończenie audytu naradą zamykającą (podsumowanie zadania, przekazanie najważniejszych rekomendacji) i przekazanie raportu/sprawozdania z zadania zapewniającego. Raport powinien zawierać opis rzeczywistego stanu ochrony danych osobowych i bezpieczeństwa informacji w jednostce, wskazywać stwierdzone uchybienia i ryzyka z tym związane oraz ich istotność, a także niezbędne zalecenia do usunięcia nieprawidłowości. W niniejszej pracy przyjęto, że dobrym rozwiązaniem dla IOD przed przystąpieniem do opracowania planu zadania audytowego dotyczącego oceny stanu bezpieczeństwa informacji i ochrony danych osobowych w jednostce będzie zebranie przez IOD/audytora niezbędnych informacji w formie stosownej ankiety/formularza, zawierającego odpowiedzi na kluczowe pytania dla Zespołu audytującego. W pracy przedstawiono również wzorcowy plan audytu i jego zakres w oparciu o wymogi RODO, KRI oraz ISO/IEC 27001 zawierający m.in. ocenę prawidłowości działań jednostki w zakresie ochrony danych osobowych i bezpieczeństwa informacji, w tym weryfikację wymaganej dokumentacji w przedmiotowym zakresie, a także zapewnienia zgodności z prawem.

Audyt pozwala na ocenę systemu ochrony danych osobowych w organizacji, adekwatnie do zagrożeń, zmian organizacyjnych i ustawowych oraz wpływa na poprawę funkcjonowania procesów i ich odpowiednią koordynację przez osoby odpowiedzialne, w tym na stosowanie odpowiednich zabezpieczeń, czy uzyskiwanie informacji co do efektywności wprowadzonych rozwiązań. Audyt, aby był rzetelny i wiarygodny powinien był realizowany

systematycznie oraz w sposób zgodny z normą PN-EN ISO 19011, wymogami RODO, KRI i odnośnymi wymogami ISO 27001.

W niniejszej dysertacji podkreślono również analogię wewnątrzorganizacyjnych kompetencji i sposobu wykonywania zadań IOD do uprawnień i zadań osób kierujących komórką audytu wewnętrznego. Z uwagi na fakt, iż RODO nie precyzuje kompetencji IOD wewnątrz organizacji administratora lub procesora dobrym rozwiązaniem jest określenie w aktach wewnętrznych jakie uprawnienia będą przysługiwać IOD, tj. dostęp do pomieszczeń, sprzętu, nośników, dokumentów oraz możliwość żądania informacji i wyjaśnień od poszczególnych pracowników, podobnie jak w przypadku audytora wewnętrznego.

W praktyce omówiono sposób realizacji przez IOD sprawdzenia dotyczącego zasad i warunków funkcjonowania monitoringu wizyjnego obejmującego weryfikację podstaw prawnych i wymogów ustawowych jego wprowadzenia, okresu przechowywania danych, zasad dostępu do nagrań, sposobu rozmieszczenia kamer, realizacji przez ADO obowiązków informacyjnych, czy analizę zapisów rejestru czynności przetwarzania. Elementem obowiązkowym weryfikacji powinno być uzasadnienie jego wprowadzenia oraz przeprowadzona ocena skutków dla ochrony danych osobowych. Nie sposób nie wspomnieć tu o konieczności weryfikacji sposobu zabezpieczenia danych, w tym urządzeń i pomieszczeń, w których są one przechowywane, na co zwróciła uwagę NIK. Należy również wziąć pod uwagę, fakt, czy ADO wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku wiążącym się z przetwarzaniem. Weryfikacja IOD powinna sprawdzić, czy ADO zapewnił, aby realizacja celu, jakim jest monitoring nie powodowała naruszenia prawa do prywatności innych osób, czy sprawdzić nieprawidłowości związane z instalacją ukrytych kamer. Nie sposób nie wspomnieć również o próbie wykorzystania monitoringu do kontroli obecności w pracy podległych pracowników lub weryfikacji przebywania ich poza stanowiskiem pracy. IOD powinien również przeanalizować postanowienia ewentualnej umowy powierzenia przetwarzania danych, jeżeli wideo-nadzór jest sprawowany np. poprzez agencję ochrony oraz czy podmiot ten zapewnia przewidzianą w przepisach ochronę na zasadach określonych w art. 28 RODO. Ostatnim elementem istotnym z punktu widzenia IOD powinna być realizacja przez ADO obowiązku notyfikacji w zakresie naruszenia ochrony danych osobowych

Mając na uwadze rolę i udział IOD w zakresie zagrożeń związanych z przetwarzaniem danych osobowych podkreślono potrzebę wdrożenia i weryfikacji procedur postępowania z incydentami w organizacji (istotność oceny i klasyfikacji zdarzenia pod kątem naruszenia danych osobowych), a następnie oceny naruszenia ochrony danych w kontekście obowiązków

zgłoszeniowych wynikających z art. 33 oraz 34 RODO. Wyróżniono tu znaczenie IOD jako punktu kontaktowego zarówno dla organu nadzoru, jak również osób, których dane dotyczą, a także w zakresie podejmowania adekwatnych działań zaradczych, czy dokumentowania naruszeń ochrony danych osobowych. Podkreślono również działania uświadamiające IOD dotyczące wskazania pracownikom zagrożeń, jakie wiążą się z przetwarzaniem danych i ich konsekwencji w tym zakresie w stosunku do osób, których te dane dotyczą, mając na uwadze konieczność stosowania odpowiednich zabezpieczeń i przestrzegania procedur bezpiecznego przetwarzania danych (korzystanie z poczty elektronicznej, VPN, szyfrowanie sprzętu i danych, bieżąca weryfikacja uprawnień przez dział IT, aktualizacja oprogramowania, antywirus i inne). Przy tym nie należy zapominać o kluczowej roli IOD w procesie dotyczącym realizacji żądań osób w zakresie realizacji ich uprawnień określonych w RODO. Dobrym rozwiązaniem jakie wskazano w pracy to wdrożenie z inicjatywy IOD instrukcji postępowania w zakresie realizacji praw osób, których dane dotyczą i kanały ułatwiające komunikację w tym zakresie z klientami zewnętrznymi, o czym mowa powyżej. Kluczową rolę IOD w tym zakresie wzmacnia nadzór nad jego prowadzeniem rejestru wniosków oraz przechowywanie dokumentacji dotyczącej wpływających wniosków i udzielanych odpowiedzi dotyczących realizacji praw osób, których dane dotyczą. Kluczowym elementem jest również wdrożenie we współpracy z IOD instrukcji postępowania w sytuacji naruszenia ochrony danych ze wskazaniem konkretnych zadań w zakresie zawiadamiania osób, których dotyczyło naruszenie oraz współpracy z organem nadzorczym. Nieodzownym elementem takiej procedury powinien być wzór takiego zawiadomienia wraz z danymi kontaktowymi do IOD. Problemem są też stare przyzwyczajenia i przeświadczenie, że dawny ABI, a obecny IOD jest raczej wykonawcą, mającym rozwiązywać każdy problem dotyczący ochrony danych i odpowiadającym za ochronę danych osobowych w organizacji. Należy podkreślić, że znaczenie funkcji IOD wzrosło w stosunku do wcześniejszej funkcji ABI. Przede wszystkim dotyczy to pełnienia funkcji punktu kontaktowego dla osób, których dane dotyczą, uczestnictwa w zgłaszaniu sytuacji naruszenia ochrony danych do Prezesa UODO, jak również uczestnictwa w procesie oceny skutków dla ochrony danych – co nie było określone we wcześniejszych przepisach o ochronie danych obowiązujących w Polsce.

Niniejsza praca powstała dzięki współpracy z instytucjami sektora publicznego i prywatnego tj. Urząd Statystyczny w Rzeszowie, Urząd Miasta Sanoka, Uniwersytet Śląski, Polski Instytut Kontroli Wewnętrznej w Warszawie Sp. z o.o. oraz firmą LOCOS Piotr Błaszczeć.

Akty prawne

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz. U. z 1997 r., nr 78, poz. 483

Karta praw podstawowych Unii Europejskiej z dnia 7.12.2000 r. Dz. Urz. UE C 326/391

Traktat o funkcjonowaniu Unii Europejskiej Dz. Urz. UE C 326

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 Dz.U.UE.L.2016.119.1

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych Dz.U.UE.L.1995.281.31

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych Dz.U.UE.L.1995.281.31

Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego Dz. Urz. UE L 345, str.90, ze zm.

Konwencja nr 108 Rady Europy sporządzonej w Strasburgu 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych Dz. U. z 2003 r., nr 3, poz. 25

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Dz. U. z 2002 r., nr 101, poz. 926 z późn zm.

Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. Dz. U. z 2019 r., poz. 1781, t.j.

Ustawa z dnia 7.11.2014 r. o ułatwieniu wykonywania działalności gospodarczej Dz. U. z 2014r., poz. 1662 z późn. zm.

Ustawa kodeks cywilny z dnia 23.04.1964 r. Dz. U. z 2019 r., poz. 1145

Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 5, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.

Ustawa z dnia 21 listopada 2008 r. o *służbie cywilnej* Dz. U. z 2020 r., poz. 265, t. j.

Ustawa z dnia 21 listopada 2008 r. o *pracownikach samorządowych* Dz. U. z 2019 r., poz. 1282, t. j.

1 Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych Dz. U. z 2019 r. poz. 869 z późn. zm., zwana dalej u.o.f.p.

Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych Dz. U. z 2019 r. poz. 1350 z późn.

zm.

Ustawa z dnia 29.8.1997 r. o Narodowym Banku Polskim Dz. U. z 2019 r., poz. 1810 z późn. zm.

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy Dz. U. z 2020 r., poz. 1320 z późn. zm.

Ustawa z dnia 6.09.2001 r. o dostępie do informacji publicznej Dz. U. z 2019 r., poz. 1429 z późn. zm.

Ustawa z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz. U. z 2020 r., poz. 346 z późn. zm.

Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych - Dz. U. z 2020 r., poz. 1842 t. j., z późn.zm.

Rozporządzenie Prezesa Rady Ministrów z dnia 29 stycznia 2016 r. w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej Dz. U. z 2018 r., poz. 807 z późn. zm.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. 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. z 2004 r., nr 100, poz. 1024

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. z 2017 r. poz. 2247, t.j.

Rozporządzenie Ministra Administracji i Cyfryzacji z 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. z 2015 r., poz. 745

Rozporządzenie Prezesa Rady Ministrów z dnia 15 maja 2018 r. w sprawie wynagradzania pracowników samorządowych Dz. U. z 2018 r., poz. 936 z późn. zm.

Orzecznictwo, opinie oraz wytyczne i stanowiska organów i instytucji nadzorczych

Wyrok WSA w Warszawie sygn. akt IV SA/Wa 1817/20 z dnia 26.02.2021 r., https://www.rpo.gov.pl/sites/default/files/Wyrok_uzasadnieniem_26.02.2021.pdf, dostęp z dnia 28.03.2021 r.;

Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., sygn. II SA/Wa 2826/19;
https://www.rpo.gov.pl/pl/content/rpo-minister-cyfryzacji-przekazanie-poczcie-rejestru-pesel-wybory-bezskuteczne , dostęp z dnia 28.03.2021 r.;
Wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r., sygn. I OSK 249/09;
Wyrok Naczelnego Sądu Administracyjnego z dnia 21 lutego 2014 r., sygn. I OSK 2445/12;
Orzeczenie Naczelnego Sądu Administracyjnego z dnia 19.04.2018 r., sygn. II FSK 1171/16;
Wyrok Sądu Najwyższego z dnia 21 sierpnia 2018 r., sygn. IV KK 365/17;
Stanowisko Prezesa UODO w sprawie tabeli grup stanowisk urzędników Służby Cywilnej, https://uodo.gov.pl/pl/138/1193, dostęp z dnia 3 kwietnia 2019 r.;
Wytyczne Grupy Roboczej art. 29 ds. ochrony danych dotyczące inspektorów ochrony danych przyjęte w dniu 13 grudnia 2016 r. z późn. zm., str. 21, https://uodo.gov.pl/pl/10/7 dostęp z dnia 3.04.2019 r.
https://uodo.gov.pl/pl/138/1636, dostęp z dnia 23.02.2021 r.
https://uodo.gov.pl/pl/138/1711 dostęp z dnia 23.02.2020 r.;
https://uodo.gov.pl/pl/138/1791, dostęp z dnia 18.12.2020 r.;
https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/bezpieczenstwo-informacji-woj-podlaskie.html;
https://www.nik.gov.pl/aktualnosci/rodo-w-szpitalu.html, dostęp z dnia 23.02.2020 r.;
https://www.nik.gov.pl/aktualnosci/rodo-w-urzedach-miast.html, dostęp z dnia 23.02.2020 r.;
https://www.nik.gov.pl/aktualnosci/zeby-elektronicznie-znaczylo-bezpiecznie.html, dostęp z dnia 23.02.2020 r.;
Pismo UODO sygn. Z0.0143.104.2019.AK.2 z dnia 3 czerwca 2019 roku;
Poradnik Prezesa Urzędu Ochrony Danych Osobowych, https://sip.lex.pl/#/publication/151350208/prezes-urzedu-ochrony-danych-osobowych-wyznaczenie-i-status-iod-wytyczne-puodo?cm=SREST;
Zasady współpracy audytora wewnętrznego i inspektora ochrony danych przy realizacji zadań w jednostce sektora finansów publicznych, https://uodo.gov.pl/pl/138/445, dostęp z dnia 21.05.2020 r.;
Zasady współpracy audytora wewnętrznego i IOD określone przez Ministerstwo Finansów i Prezesa UODO, https://uodo.gov.pl/pl/138/445 dostęp z dnia 4.04.2019 r.;
Urząd Ochrony Danych Osobowych, Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, Warszawa, czerwiec 2019 r.;
Za nami trzy lata RODO, https://uodo.gov.pl/pl/138/2059 , dostęp z dnia 4.06.2021 r.;

Decyzja Prezesa Urzędu Danych Osobowych z dnia 22 kwietnia 2021 r., znak: DKN.5130.3114.2020;

Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców, październik 2018 r., https://uodo.gov.pl/pl/138/545 dostęp z dnia 13.06.2020 r.

Bibliografia

Analiza wybranych obszarów funkcjonowania nadzoru w administracji rządowej, KPRM Warszawa 2012;

Banyś T. A.J., J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych,* Wrocław 2017;

Bar G., *Inspektor ochrony danych – miejsce w organizacji, rola i zadania*, PME 2018, Nr 4, C.H. Beck, str. 4, Legalis.pl, dostęp z dnia 28.05.2020 r.;

Bielak-Jomaa E., *Administrator i podmiot przetwarzający,* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, WKP, Warszawa 2018;

Bielak-Jomaa E., *Inspektor ochrony danych,* [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, WKP, Warszawa 2018;

Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 44, ausgegeben zu Bonn am 5. Juli 2017, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1589796091814, dostęp z dnia 18.05.2020 r.;

Byczkowski M., *Doświadczenia w wykonywaniu funkcji inspektora ochrony danych*, [w:] M. Kołodziej (red.), *Vademecum Inspektora Ochrony Danych*, C.H. Beck, Warszawa 2020;

Czaplińska M., *IOD dla grupy przedsiębiorstw, komentarz praktyczny*, LEX/el. 2018, dostęp z dnia 4.04.2019 r.;

Czaplińska M., *IOD dla grupy przedsiębiorstw,* Lex/el. 2018, dostęp z dnia 28.05.2020 r.;

Czub-Kiełczewska S., *Okiem IOD-a: dokumentacja ochrony danych zgodna z RODO - zadania IOD-a,* Lex/el. 2019, dostęp z dnia 28.05.2020 r.;

Czub-Kiełczewska S., *Okiem ID-a: ochrona danych osobowych przy pracy zdalnej,* Lex/el. 2020, dostęp z dnia 11.03.2021 r. ;

Czub-Kiełczewska S., *Okiem IOD-a: powierzanie i podpowierzenie danych w praktyce,* Lex/el. 2019, dostęp z dnia 16.03.2021 r.;

Czub-Kiełczewska S., *Okiem IOD-a: status i zadania IOD-a - dobre praktyki*, Lex/el. 2019, dostęp z dnia 16.11.2019 r.;

Dawidowska A., *Jaka jest odpowiedzialność inspektora ochrony danych?,* Lex /el. 2018 dostęp z dnia 3.04. 2019 r.;

Fajgielski P., *Dokumentacja naruszeń ochrony danych osobowych,* [w:] M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, WKP, Warszawa 2019;

Fajgielski P., *Dostosowanie krajowych przepisów do wymogów ogólnego rozporządzenia o ochronie danych* (dodatek MoP 22/2019), Monitor Prawniczy 2019, Nr 22;

Fajgielski P., *Inspektor Ochrony Danych w sektorze publicznym,* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019;

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 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)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* WKP, Warszawa 2018;

Fajgielski P., *Komentarz do ustawy o ochronie danych osobowych*, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Wolters Kluwer 1 lipca 2018 r., LEX/el. 2018, dostęp z dnia 23 listopada 2019 r.;

Fajgielski P., *Ogólne Rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Wolters Kluwer, Warszawa 2018;

Fajgielski P., *Prawo ochrony danych osobowych. Zarys wykładu,* Wolters Kluwer, Warszawa 2019;

Gałaj-Emiliańczyk K., *Inspektor ochrony danych. Kompetencje obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów,* ODDK Gdańsk 2018;

Gawroński M., M. Kibil*, Zadania Inspektora ochrony danych osobowych*, Lex/el. 2018, dostęp 09.02.2019 r. ;

Gawroński M., K. Kloc, M. Wojtas, *Obowiązki i rola administratora oraz podmiotu przetwarzającego,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.;

Glen P., *IOD – kosztowny obowiązek czy luksus,* Oficyna Prawa Polskiego, nr 58/2019;

Gołębiowska A., A. Kociołek – Pęksa, *Kontrola i nadzór w prawie administracyjnym – wybrane zagadnienia teoretycznoprawne i dogmatycznoprawne,* Zeszyty Naukowe SGSP 2018, Nr 67/3/2018;

Gruszczyński M., T. Wącirz, *Cechy dobrego inspektora ochrony danych* [w:] M. Kołodziej (red.), *Vademecum Inspektora Ochrony Danych*, C.H. Beck, Warszawa 2020;

Gumularz M., *Ochrona danych osobowych w sektorze publicznym,* Lex/el. 2018, dostęp z dnia 15.07.2020 r.;

Hady-Głowiak S., *ABI/ IOD - wyspecjalizowany audytor ds. bezpieczeństwa informacji*, Kontroler Info nr 8 z 2017 r.;
Hady-Głowiak S., *Administrator bezpieczeństwa informacji (ABI) jako urzędnik do spraw ochrony danych osobowych*, Kontroler Info nr 5 z 2016r.;
Hady-Głowiak S., K. Kruczek, *Prawne aspekty dotyczące wykorzystania systemu monitoringu wizyjnego w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa jednostk*i, [w:] K. Żarna (red.), Bezpieczeństwo - Prawa człowieka - Stosunki międzynarodowe, t. III, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2021;
S. Hady – Głowiak., D. Kozłowski, *Dekalog ochrony danych osobowych- stosowanie zasad przestrzegania danych osobowych jako podstawa bezpieczeństwa przetwarzanych danych* [w:] red. J. Wołejszo, K. Rejman, M. Wilczyńska, *Bezpieczeństwo informacji w organizacjach*, Kalisz 2021;
Hamelusz K., *Zadania IOD względem ABI - analiza prawno-porównawcza*, Lex/el. 2018, dostęp z dnia 29.11.2019 r.;
Hudzik K., *Inspektor ochrony danych osobowych a audytor wewnętrzny zatrudniony w jednostce sektora finansów publicznych. Łączenie funkcji, zasady współpracy,* IAP nr 4/2019, str. 27, Legalis.pl, dostęp z dnia 28.05.2020 r.;
Jagiełło-Jaroszewska E., *Ochrona danych osobowych a telepraca i praca zdalna* [w:] D. Dörre-Kolasa (red.), *Ochrona danych osobowych w zatrudnieniu*, C.H. Beck, Warszawa 2020 r.;
Jakubik M., P. Wojciechowski, *RODO w IT: atak hakerski a ochrona danych osobowych*, Lex/el. 2020, dostęp z dnia 16.03.2021 r.;
Jakubik M., T. Świętnicki, *Indywidualny monitoring pracownika – zagadnienie monitorowania pracowników i ich danych,* Lex/el. 2020, dostęp z dnia 19.03.2021 r.;
Kaczmarek A., *Wyznaczenie Inspektora Ochrony Danych* [w:] red. B. Marcinkowski, *Ustawa o ochronie danych osobowych, Komentarz*, Wolters Kluwer Warszawa 2018;
Kaczmarek-Templin B., *Prawo do odszkodowania na drodze cywilnej za naruszenie ochrony danych zarówno w sektorze publicznym i prywatnym*, LEX/el. 2018;
Kodeks etyki oraz Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego, Tłumaczenie na język polski, THE INSTITUTE OF INTERNAL AUDITORS, wrzesień 2016, https://www.iia.org.pl/o-nas/standardy, dostęp z dnia 21.05.2020 r.;
Kołodziej M., *Podstawy prawne powołania inspektora ochrony danych* [w:] M. Kołodziej (red.), *Vademecum Inspektora Ochrony Danych*, C.H. Beck, Warszawa 2020;
Kołodziej M., *Powołanie administratora bezpieczeństwa informacji* [w:] Maciej Kołodziej (red.), *Vademecum administratora bezpieczeństwa informacji*, C. H. Beck, Warszawa 2016;

Kołodziej M., *Vademecum IOD*, C.H. Beck, Warszawa 2020;
Kopeć K., P. Strumiński, *Przekazanie danych pracowniczych podmiotom zewnętrznym,* [pod red. M. Mędrala *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami]* WKP, Warszawa 2018;
Korga M., *Z praktyki zespołu audytorów – jak przygotować jednostkę do zmian, które niesie za sobą Rozporządzenie unijne?* IAP nr 3/2017 r., C.H.Beck, str. 16, Legalis.pl, dostęp z dnia 28.05.2020 r.;
Kozieł K., S. Sieniewicz, *Weryfikacja kwalifikacji IOD-a i zadań przez niego realizowanych ze wskazaniem środków kontroli,* Lex/el. 2018, dostęp z dnia 09.02.2019 r.;
Kręcisz – Sarna A., *Kiedy w podmiocie trzeba powołać IOD,* Oficyna Prawa Polskiego, nr 62/2019;
Krzyszkowska-Dąbrowska M., *Praca zdalna. Praktyczny przewodnik,* WKP 2020 dostęp z dnia 11.03.2021 r.;
Kuba M., *Podstawy prawne zatrudnienia Inspektora Ochrony Danych* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019;
Kulesza E., Problem niezależności inspektora ochrony danych [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019;
Gałaj-Emiliańczyk K., *Inspektor ochrony danych. Kompetencje obowiązki i odpowiedzialność. Poradnik praktyka z wzorami dokumentów,* ODDK Gdańsk 2018;
Kulesza E., Problem niezależności inspektora ochrony danych [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019;
Lesińska Joanna, *Harmonogram wdrożenia RODO – krok po kroku,* Lex/el. 2018, dostęp z dnia 28.05.2020 r.;
Lubasz D., W. Chomiczewski, C*ompliance w zakresie ochrony danych osobowych*, [w:] B. Jagura (red.), B. Makowicz (red.), *Systemy zarządzania zgodnością. Compliance w praktyce*, WKP 2020, dostęp z dnia 4.06.2021 r. ;
Lubasz D., *Wyznaczenie Inspektora Ochrony Danych,* [w:] D. Lubasz (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2019;
Łokaj M., *Czy każda placówka medyczna będzie zobowiązana do posiadania Inspektora Ochrony Danych osobowych (IOD)?*, Lex/el. 2017, dostęp z dnia 3.04.2019 r.;
Łokaj M., *Kiedy kilka publicznych placówek medycznych będzie mogło mieć wspólnego IDO?,* Lex/el. 2017, dostęp z dnia 4.04.2019 r.;
Łuczak J., Inspektor ochrony danych w sektorze publicznym, Lex/ el. 2018, dostęp z dnia

04.04.2019 r. ;
Marciniak J., *Praca zdalna,* Lex/el. 2020, dostęp z dnia 11.03.2021 r.;
Mednis A., *Odpowiedzialność Inspektora Ochrony Danych,* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019;
Młotkiewicz M., *Przekształcenie administratora bezpieczeństwa informacji w inspektora ochrony danych*, Informacja w Administracji Publicznej 2018 r., nr 1, str. 10, Legalis.pl, dostęp z dnia 28.05.2020 r.;
Noga-Bogomilska J., *Kto może kontrolować podmioty w zakresie ochrony danych osobowych?* Lex/el. 2019, dostęp z dnia 18.12.2020 r.;
Otto M., *Pozycja prawna inspektora ochrony danych – zarys prawnoporównawczy,* [w:] T. Wyka (red.), M. A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, WKP Warszawa 2019;
Otto M., *Przetwarzanie danych osobowych w kontekście zatrudnienia,* [w:] M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, WKP, Warszawa 2019;
Pielok A., P. Sojka, *Ochrona danych osobowych w oświacie. Poradnik dla administratorów oraz inspektorów ochrony danych*, WKP 2020;
Rzemka M., *Urząd bliżej obywateli*, Newsletter UODO dla Inspektorów Ochrony Danych, nr 9/2019;
Sakowska – Baryła M., *Dokumentacja audytów wewnętrznych*, [w:] M. Jagielski (red.) *Dokumentacja ochrony danych osobowych ze wzorami*], Wolters Kluwer, Warszawa 2019;
Sakowska-Baryła M., F*Ochrona danych osobowych w warunkach pracy zdalnej,* WKP 2020;
Sakowska-Baryła M., *Odpowiedzi na pytania ze szkolenia "Udostępnianie danych osobowych w orzecznictwie Prezesa Urzędu Ochrony Danych Osobowych"*, Lex/el. 2020, dostęp z dnia 16.03.2021 r.;
Sarna M., *Inspektor ochrony danych* [w:] pod red. W. Szczygielska, *RODO przewodnik po kluczowych zmianach*, WiP Warszawa 2008;
Siemieniak P., *RODO w IT: atak hakerski i co dalej?*, Lex/el. 2020, dostęp z dnia 16.03.2021 r.;
Sikora K. *Rola nadzoru w funkcjonowaniu administracji publicznej* [online]. Studia Iuridica Lublinensia, 2004, nr 3. str. 208, 2020-07-23 15:03 [dostęp: 2020-08-23 11:15]. Dostępny w Internecie: https://sip.lex.pl/#/publication/151054671;
Sołtyk P., *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego - wątpliwości interpretacyjne*, Finanse

Komunalne, 2016, nr 1-2. str. 126-133, https://sip.lex.pl/#/publication/151278164, dostęp z dnia 23.08.2020 r.;
Syska K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań* (dodatek MOP 20/2016) MOP 2016, Nr 20, str. 80, Legalis.pl, dostęp z dnia 28.05.2020 r.;
Szymczak-Kamińska P., *Dostęp do danych osobowych kandydatów do pracy i pracowników,* Lex/el. 2018, dostęp z dnia 16.03.2021 r.;
Więckowski P., *Organizacja wypełniania obowiązków dotyczących ochrony danych osobowych w grupie przedsiębiorstw* [w:] M. Kołodziej (red.), *Vademecum Inspektora Ochrony Danych*, C.H. Beck, Warszawa 2020;
Zadorożny M., *Inspektor ochrony danych (IOD) jako następca ABI* [w:] A. Dmochowska (red.), M. Zadorożny (red.) *Unijna reforma ochrony danych osobowych*, C. H. Beck, Warszawa 2018;
Zaleśny J., *Prawo miejscowe* [w:] *Słownik pojęć w administracji publicznej,* red. I.Wieczorek, J.Szymanek, NIST, Łódź 2018;

Źródła internetowe:

https://dataprotection.gov.sk/uoou/sk/content/zodpovedna-osoba-ss-23-nasl, dostęp z dnia 19.11.2020 r.;
https://dsgvo-gesetz.de/bdsg/ , dostęp z dnia 18.05.2020 r.
https://mcodszkodowania.pl/odpowiedzialnosc-abi-administratora-bezpieczenstwa-informacji-i-ado-administratora-danych-osobowych/ dostęp z dnia 29.11.2019 r.;
https://naszkrakow.com.pl/2021/03/10/czy-mamy-do-czynienia-z-seria-atakow-hakerskich/, dostęp z dnia 16.03.2021 r.;
https://prawo.gazetaprawna.pl/artykuly/1445350,jaroslaw-felinski-nie-kazdy-powinien-byc-inspektorem-ochrony-danych.html, dostęp z dnia 19.11.2020 r.;
https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion , dostęp z dnia 19.11.2020 r. ;
https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-delivre-son-premier-agrement, dostęp z dnia 19.11.2020 r. ;
https://www.cyberdefence24.pl/atak-na-urzad-marszalkowski-w-krakowie-nadal-nie-dziala-system-informatyczny, dostęp z dnia 28.03.2021 r.;
https://samorzad.pap.pl/kategoria/aktualnosci/nik-o-wprowadzaniu-rodo-w-urzedach-duzych-miast-pojedyncze-potkniecia, dostęp z dnia 16.03.2021 r. ;

https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjBxJzbtNPvAhWwxIsKHbPpB4sQFjAAegQIBBAD&url=https%3A%2F%2Fuodo.gov.pl%2Fpl%2Ffile%2F2210&usg=AOvVaw1PVnALtheH0KHIb5s325OA , dostęp z dnia 16.03.2021 r.