A C T A U N I V E R S I T A T I S N I C O L A I C O P E R N I C I
DOI:http://dx.doi.org/10.12775/AUNC_ZARZ.2017.032 ZARZĄDZANIE XLIV–NR3(2017)

Pierwsza wersja złożona 25.03.2017
Ostatnia wersja zaakceptowana 29.05.2017

ISSN (print) 1689-8966
ISSN (online) 2450-7040

*Natalia Bender**

DPO - PRZYKRY OBOWIĄZEK, CZY REALNE WSPARCIE PROCESÓW ZARZĄDZANIA DANYMI OSOBOWYMI

Zarys treści: Idea powołania osoby odpowiedzialnej za ochronę danych osobowych w organizacji nie jest koncepcją nową. Ustawodawca europejski wskazał taką możliwość przepisami dyrektywy 95/46/WE, a praktyka ta, pomimo nieobligatoryjnego charakteru, wykształciła się w szeregu państw członkowskich (Francja, Niemcy, Holandia, Szwecja). Celem niniejszego opracowania jest przedstawienie genezy ustanowienia oraz powodów transformacji funkcji „urzędnika" zajmującego się ochroną danych w organizacji. Artykuł zawiera analizę podstawowych zadań, które ustawowo zostały przypisane administratorom bezpieczeństwa informacji, a od 25 maja 2018 r. zostaną powierzone DPO (Data Protection Officer). Przedmiotem pracy jest również przegląd wymagań oraz zasobów, w które należy „urzędnika" wyposażyć by zapewnić rozliczalność procesów zarządzania danymi osobowymi w jednostce, adekwatnie do potrzeb organizacji i wymagań nowego Ogólnego Rozporządzenia o ochronie danych osobowych.

Słowa kluczowe: RODO; przetwarzanie danych osobowych; DPO; wymagania; obowiązki

Klasyfikacja JEL: L 21; L26;

WSTĘP

Materia, energia i informacja - to trzy żywioły, których kompozycja wyznacza paradygmaty cywilizacyjne [Krzystofek, Szczepański, 2002, s. 176]. Obecna rzeczywistość, to rzeczywistość zdominowana przez dane. „Skala pozyskiwania, gromadzenia i wymiany informacji osiągnęła niebotyczne rozmiary. Dociera ich do nas coraz więcej, coraz intensywniej ich doświadczamy(…).

* Adres do korespondencji: Natalia Bender, Uniwersytet Warszawski, Wydział Zarządzania, ul. Szturmowa 1/3, 02-678 Warszawa, e-mail: natalia.bender@gazeta.pl;

Fundamentalnymi czynnikami konstytuującymi obecną rzeczywistość jest zalew informacji, rosnące tempo życia i rosnąca liczba zmian" [Ball, 2000, s. 10–12]. Rozwój globalnego społeczeństwa informacyjnego sprawia, że jest ona traktowana jako dobro ekonomiczne, główny zasób i podstawowa kategoria ekonomiczna [Dziekański, 2012, s. 387], a cechą charakterystyczną nowej gospodarki jest wykładniczy wzrost produkcji i przepływu informacji wszelkiego rodzaju [Oleksiejczuk, Oleksiejczuk, 2009, s. 57-58]. Informacja traktowana jest coraz częściej we współczesnej gospodarce oraz nowocześnie zarządzanych firmach jako czwarty czynnik produkcji obok ziemi, kapitału i pracy ludzkiej [Dziekański, 2012, s. 389; Pomykalski, 2001, s. 169; Penc, 1994, s. 82].

To nowoczesne technologie informacyjne - metody i urządzenia techniczne służące do generowania, gromadzenia, przetwarzania, przechowywania, przekazywania i udostępniania informacji stanowią istotny czynnik, dzięki któremu współczesna cywilizacja jest autentycznie cywilizacją informacyjną [Porter, 2001, s. 93]. Jednakże wraz z ciągłym ich rozwojem rozróżniamy coraz nowsze zagrożenia związane z bezpieczeństwem informacji, w szczególności obrotem danymi osobowymi. Korzystanie z nowoczesnych usług nierozerwalnie łączy się bowiem z udostępnianiem danych osobowych - swoistego rodzaju „waluty cyfrowej". Pozostawiamy je w sieci już podczas samego wejścia do niej - geolokalizacja, wyszukiwane usługi, zakupione produkty, opublikowane informacje - rejestrowane są w postaci cyfrowych śladów, źródeł informacji. Do zidentyfikowania konkretnej osoby nie jest już niezbędne poznanie jej imienia i nazwiska, adresu zamieszkania czy numeru PESEL. Pojęcie danych osobowych rozpatrywane jest szerzej. W myśl ustawy o ochronie danych osobowych[1] są to bowiem wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy obecnym poziomie rozwoju technologicznego oraz zastosowaniu odpowiedniej metody, możliwość zidentyfikowania osoby nawet za pomocą szczątkowych informacji staje się coraz łatwiejsza, zwłaszcza wobec coraz powszechniejszego łączenia danych pochodzących z różnych źródeł i wykorzystywania ich do nowych, w stosunku do pierwotnych, celów[2].

Nic więc dziwnego, że obowiązujące w zakresie ochrony danych osobowych prawo unijne[3] przestało nadążać za rzeczywistością. Profilowanie, biometria, Internet rzeczy, big data, prawo do bycia zapomnianym to przedmiot rozważań reformy unijnego prawa ochrony danych osobowych, opublikowanego w kwietniu 2016 r. To w równorzędnym stopniu akcentowanie roli osób

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.922 j.t.).

[2] Raport o ochronie danych osobowych, opracowany przez Biuro Generalnego Inspektora Ochrony Danych Osobowych (http://www.giodo.gov.pl/487/id_art/9146/j/pl/ [05.03.2017 r.]).

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995).

funkcyjnych, warunkujących rozliczalność procesów przetwarzania danych na poziomie jednostki.

Niniejsze opracowanie ma na celu w sposób usystematyzowany przedstawić genezę ustanowienia osoby, której rolą jest nadzorowanie procesów przetwarzania danych osobowych. W publikacji analizie poddano zakres zadań, wymagań oraz zasobów, w które osoba ta powinna zostać „wyposażona", by system operował sprawie oraz w zgodzie z wymaganiami prawa.

1. URZĘDNIK ODPOWIEDZIALNY ZA OCHRONĘ DANYCH OSOBOWYCH

Fakultatywność wyznaczenia osoby odpowiedzialnej za ochronę danych osobowych po raz pierwszy wprowadzona została przepisem 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, dalej jako dyrektywa 95/46/WE. Wytyczne w zakresie procedury upraszczającej rejestrację czynności przetwarzania danych określiły zakres zadań „urzędnika" ds. ochrony danych osobowych. Do czynności tych należy zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy przedmiotowej dyrektywy oraz prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych[4]. Jak wskazuje prawodawca europejski, jeżeli administrator danych zdecyduje się powołać osobę funkcyjną, istotnym jest zapewnienie niezależności „urzędnika" w pełnieniu jego działań. W konsekwencji oznacza to, że w ramach wypełniania powierzonych czynności nie może on otrzymywać instrukcji dotyczących sposobów rozpoznawania procesów, nie może też poddawany być naciskom, w jaki sposób czynności te wykonywać.

Zasady ochrony danych ustanowione dyrektywą 95/46/WE wprowadzone zostały do polskiego porządku prawnego ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5][6], dalej jako u.o.d.o. Tymczasem możliwość wyznaczenia osoby funkcyjnej, odpowiedzialnej za ochronę danych osobowych po raz pierwszy w przepisach krajowych wprowadziła ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe[7]. Jednakże, jak wskazano

[4] Art. 18 ust. 2 tiret drugie Dyrektywy 95/46/WE.

[5] Dz.U.1997.133. 883 - tekst pierwotny.

[6] Ustawa zawiera szczegółowe normy służące ochronie danych osobowych w Polsce, a do dnia 1 maja 2004 r., tj. wstąpienia Polski do Unii Europejskiej, przeniosła do polskiego porządku prawnego wszystkie zasady określone w dyrektywie 95/46/WE. Przepisy ustawy w pełni obowiązują od dnia 30 kwietnia 1998 roku.

[7] Dz.U.2004.33.285.

w uzasadnieniu kolejnej nowelizacji u.o.d.o. „ustawodawca polski do tej pory nie skorzystał (w sposób efektywny) z możliwości uregulowania instytucji urzędnika ds. ochrony danych osobowych. Przewidziany w polskiej ustawie administrator bezpieczeństwa informacji nie spełniał warunków uznania go za urzędnika ds. ochrony danych osobowych w rozumieniu dyrektywy. Ustawa nie gwarantowała mu bowiem niezależności, zbyt wąsko określała jego zadania w odniesieniu do uregulowań dyrektywy w tym zakresie, jak również nie przyznawała kompetencji w zakresie uproszczonej rejestracji”[8].

Nowelizacja u.o.d.o., za sprawą ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[9] spowodowała odmienny sposób postrzegania roli oraz wymiaru zadań ABI. W ramach proponowanych rozwiązań określony został jego status, na który składają się m.in.: wymogi stawiane osobie mającej pełnić omawianą funkcję, organizacyjne usytuowanie stanowiska - bezpośrednią podległość administratorowi danych[10] oraz zapewnienie środków i organizacyjnej odrębności niezbędnej do niezależnego wykonywania zadań powierzonych ABI. Dopuszczenie nałożenia na ABI innych zadań niż określonych w u.o.d.o., możliwe jest wyłącznie pod warunkiem, że nie naruszy to prawidłowego wykonywania przez niego zadań.

2. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Funkcję ABI może pełnić osoba, która posiada pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych, posiada odpowiednią wiedzę w zakresie ochrony danych osobowych oraz nie była karana za umyślne przestępstwo. Warto jednak wskazać, iż przesłanka posiadania przez ABI odpowiedniej wiedzy w zakresie ochrony danych osobowych[11] jest oceniana przez samego administratora danych. I choć przepisy u.o.d.o. nie wprowadzają wymogu posiadania przez ABI poświadczeń czy certyfikatów ukończenia odpowiednich szkoleń, kursów, czy studiów, administartor danych, działając we własnym interesie powinien powołać osobę, która ma rzeczywistą wiedzę w powyższym zakresie. Z uwagi na zakres powierzonych czynności,
wydaje się być to szczególnie istotne.

Głównym zadaniem ABI, nadzorcy procesów przetwarzania danych osobowych w organizacji, jest zapewnianie przestrzegania przepisów o ochronie danych osobowych[12]. W szczególności dokonuje tego poprzez sprawdzanie

[8] Rządowy projekt ustawy o ułatwieniu wykonywania działalności gospodarczej, druk Nr 2606, s. 20 (http://www.sejm.gov.pl/Sejm7.nsf/PrzebiegProc.xsp?nr=2606 [05.03.2017 r.]).

[9] Dz.U.2014.1662.

[10] Ilekroć w ustawie mowa jest o administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę (…), decydujące o celach i środkach przetwarzania danych osobowych – art. 7 pkt. 4 u.o.d.o.

[11] Art. 36a ust. 5 pkt 2 u.o.d.o.

[12] Art. 36a ust. 2 pkt 1 lit. a u.o.d.o.

zgodności przetwarzania danych osobowych z przepisami u.o.d.o. Czynności te mają charakter kontroli wewnętrznej, której tryb oraz sposób dokumentowania opisany został w u.o.d.o. [13] oraz rozporządzeniu[14]. Przeprowadzenie czynności kontrolnych ma na celu usunięcie ewentualnych nieprawidłowości, ich przyczyn i źródeł oraz pobudzenie działań naprawczych, a sporządzone w konsekwencji sprawozdanie stanowi raport, udokumentowane zestawienie podjętych czynności.

Do podstawowych zadań ABI (administrator bezpieczeństwa informacji) należy również nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych[15]. I tak, ABI weryfikuje zarówno samo opracowanie dokumentacji, jak i jej kompletność, a także zgodność dokumentacji z obowiązującymi przepisami prawa. Powyższe nadzorować może w ramach wspomnianych sprawdzeń, zgłoszenia osoby trzeciej, jak i własnego udziału w procedurach przewidzianych w dokumentacji. W przypadku wykrycia nieprawidłowości ABI zawiadamia o brakach lub nieopracowaniu dokumentacji administratora danych, wskazując jednocześnie działania niezbędne do przywrócenia dokumentacji do wymaganego stanu.

Obowiązkiem ustawowym ABI[16] jest również zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami u.o.d.o. I choć mogłoby się wydawać, że przepis jest zrozumiały, to w doktrynie interperetowany jest różnie. Z jednej strony wskazuje się, że w praktyce powinność ta będzie polegała na przeprowadzeniu przez ABI szkoleń z zakresu prawa ochrony danych osobowych [Barta, Litwiński, 2016, s. 424; Mendis, 2015, s. 21-22]. Z drugiej strony przyjmuje się, jako właściwe, podejście że rolą ABI jest podjęcie decyzji, w jaki sposób zadanie nałożone na niego przez ustawodawcę wypełni, np. może on ograniczyć się wyłącznie do udostępnienia pracownikowi treści przepisów wraz z pouczeniem o konieczności zapoznania się z nimi [Barta, Fajgielski, Markiewicz, 2015, s. 562]. Wydaje się jednak, że działanie ABI polegające jedynie na odebraniu oświadczenia od pracownika o zapoznaniu się z normami w powyższym zakresie nie spełnia wymagań ustawowych. To zadaniem ABI jest podnoszenie świadomości pracowników w zakresie zasad i praktycznych aspektów związanych z ich ochroną.

Powołanie ABI wymaga zgłoszenia tego faktu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, dalej jako GIODO. Zgłoszeni i zarejestrowani ABI wpisywani są do ogólnokrajowego, jawnego rejestru administartorów bezpieczeństwa informacji (rejestru ABI), prowadzonego obok

[13] Art. 36c u.o.d.o.

[14] Rozporządzenie Ministra Administarcji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U.2015.745).

[15] Art. 36a ust. 2 pkt 1 lit. b u.o.d.o.

[16] Art. 36a ust. 2 pkt 1 lit. c u.o.d.o.

rejestru zbiorów danych osobowych przez urząd nadzorczy (GIODO). Dostępność danych zawartych w rejestrze, służyć ma, zgodnie z założeniami dyrektywy 95/46/WE, spełnieniu postulatu transparentności operacji przetwarzania danych osobowych. Celem takiego systemu ewidencji jest kontrola administratora danych, czy faktycznie spełnił warunki niezbędne do zwolnienia go z obowiązku rejestracyjnego. W myśl bowiem przepisu art. 43 ust. 1a obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane wrażliwe, nie podlega administrator danych, który powołał ABI i zgłosił go do rejestracji.

Wobec ABI, wpisanego do ogólnokrajowego, jawnego rejestru, ustawodawca przewidział również możliwość powierzenia mu przez GIODO dokonania sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych[17]. Należy jednocześnie wskazać, iż sprawdzenie, o którym mowa powyżej oraz sprawdzenie wynikające z art. 36a ust. 2 pkt 1 lit. a, to dwie różne instytucje prawne. W pierwszym przypadku ABI dokonuje sprawdzenia u administratora danych, który go powołał, na zlecenie GIODO, a dokument w postaci sprawozdania przedstawiany jest organowi nadzorczaemu (GIODO). W drugim przypadku – sprawdzenie przeprowadzone przez ABI ma charakter kontroli własnej, a powstałe w jego wyniku sprawozdanie jest dokumentem wewnętrznym administratora danych.

3. INSPEKTOR OCHRONY DANYCH (DPO)

Ogólne rozporządzenie o ochronie danych, dalej RODO, które zacznie obowiązywać od 25 maja 2018 r. zapewni zmodernizowane, oparte na rozliczalności, ramy ochrony danych osobowych w Europie. Dla wielu jednostek inspektor ochrony danych, dalej DPO, będzie ważnym punktem w dostosowaniu do tych ram. W myśl art. 37 ust. 1 RODO administrator[18] i podmiot przetwarzający[19] wyznaczają DPO, zawsze gdy: przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości; 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 lub gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii

[17] Art. 19b ust. 1 u.o.d.o.

[18] Administrator, w rozumieniu art. 4 ust. 7 RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

[19] Podmiot przetwarzający w rozumieniu art. 4 ust. 8 RODO oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Obowiązki przyszłego DPO w większości tożsame są z zakresem zadań powierzonych obecnie ABI. Jest to wciąż działalność informacyjna w zakresie obowiązków spoczywających na administratorze, podmiocie przetwarzającym, czynności doradcze, w zakresie procesów przetwarzania i zabezpieczania danych, wynikających z przepisów prawa - RODO oraz innych przepisów Unii lub państw członkowskich. Działania edukacyjne, zwiększające świadomość personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty (sprawdzenia).

Nową, istotną rolą DPO będzie udział w procesie przeprowadzania oceny skutków dla ochrony danych[20]. Zgodnie z zasadą ochrony danych w fazie projektowania[21], administrator danych ma obowiązek konsultowania się z DPO przy dokonywaniu takiej oceny. Czynności te polegać będą między innym na podjęciu decyzji, czy taka ocena jest niezbędna, a jeśli tak, jaką metodologię przyjąć by zabezpieczyć ewentualne zagrożenia związane z przetwarzaniem danych, względnie w jaki sposób proces ten ograniczyć lub zakończyć.

Dodatkowo DPO będzie pełnił również funkcję punktu kontaktowego. Dla organu nadzorczego[22] w kwestiach związanych z przetwarzaniem, prowadzeniem konsultacji czy zgłaszaniem naruszeń. Wobec osób, których dane dotyczą w zakresie transparentności podejmowanych przez administratora, czynności. A w stosunku do pracowników organizacji w ramach działań edukacyjnych i uświadamiających, nadzorczych i korygujących. Podmioty te muszą bowiem mieć możliwość łatwego i sprawnego komunikowania się z DPO, jeżeli nadzór ten oceniony ma być za efektywny.

4. DPO - WYMAGANIA DLA EFEKTYWNEGO WYKONYWANIA FUNKCJI

DPO 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[23]. Motyw 97 przewiduje, że niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe[24]. Po raz kolejny

[20] Art. 35 ust. 1 RODO.

[21] Art. 35 ust. 2 RODO.

[22] W myśl art. 39 ust. 1 lit. 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.

[23] Art. 37 ust. 5 RODO.

[24] Grupa robocza art. 29 ds. Ochrony Danych, Wytyczne dotyczące inspektorów ochrony danych

nie został on jednak wyraźnie określony. Musi być natomiast współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Dla przykładu, przy zastosowaniu wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnej kategorii, niezbędnym może okazać się potrzeba legitymowania się przez niego wiedzą biznesową czy sektorową, a w przypadku organów i podmiotów publicznych dodatkowo wiedzą z zakresu procedur administracyjnych i funkcjonowania jednostki. Choć przepis RODO nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę wyznaczając DPO, to jednak istotne jest, by posiadał on odpowiednią wiedzę z zakresu europejskich i krajowych przepisów o ochronie danych osobowych[25], w szczególności w odniesieniu do prawa konstytucyjnego i prawa do prywatności, a także z zakresu teleinformatyki (systemów informatycznych) oraz praktyczną znajomość przeprowadzania czynności kontrolnych (audytów).

Możliwość efektywnego wykonywania zadań powierzonych DPO powinna być interpretowana zarówno przez pryzmat jego wiedzy, umiejętności i kwalifikacji, jak również jego pozycji w strukturach podmiotu[26]. Niezmiernie istotne jest więc zakomunikowanie i zaakcentowanie jego roli w organizacji przez najwyższe kierownictwo. Motyw 97, a dalej art. 38 ust. 3 RODO akcentuje zakres gwarancji, których celem jest umożliwianie DPO wykonywanie obowiązków z odpowiednim stopniem niezależności. Administrator, podmiot przetwarzający zapewnić mają by DPO nie otrzymywał instrukcji dotyczących wykonywania zadań. W praktyce niezależność ta oznacza brak instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte czy celu jaki powinien zostać osiągnięty, w tym potrzeby skontaktowania się z organem nadzorczym[27]. Wykonywanie zadań w sposób niezależny wiąże się również ściśle z artykułem 38 ust. 6 RODO, który umożliwia DPO wykonywanie „innych zadań i obowiązkówów" pod warunkiem jednak, że zadania i obowiązki te nie będą powodowały „konfliktu interesów".

Sprawnie funkcjonujący system, na czele którego stoi DPO, to również potrzeba niezwłocznego włączania i zaangażowania go we wszelkie kwestie związane z przetwarzaniem danych już od najwcześniejszego etapu - projektowania. W związku z tym angażowanie DPO powinno stać się standardową procedurą w organizacji. Nieodzownym wydaje się być jego udział w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji czy uczestnictwo przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych. Skuteczność działania DPO uwarunkowana jest również

('DPO'), przyjęte w dniu 13 grudnia 2016 r.,16/EN WP 243 – tłumaczenie nieoficjalne, s. 10-11, (http://giodo.gov.pl/pl/259/9718 [05.03.2017 r.]).

[25] Ibid., s. 11.

[26] Ibid., s. 11.

[27] Ibid., s. 14.

zapewnieniem zasobówów niezbędnych do wykonywania powierzonych mu czynności, np. dostępu do poszczególnych procesów - działu HR, prawnego czy IT, wymiaru czasu pracy, umożliwiającego wykonywanie zadań czy dostępu do szkoleń, udział w warsztatach i konferencjach.

PODSUMOWANIE

Świadomość znaczenia informacji w organizacji skłania podmioty przetwarzające do wdrażania systematycznie rozwijanych i stosunkowo efektywnych mechanizmów jej ochrony. Zasób, który ma być źródłem przewagi konkurencyjnej dla organizacji musi bowiem podlegać ochronie. Dotyczy to zarówno ochrony przed zagrożeniami zewnętrznymi, jak i - wewnętrznymi, losowymi i intencjonalnymi (pasywnymi oraz aktywnymi) [Żebrowski, 2004, s. 421-446]. Skutecznie działający system zarządzania bezpieczeństwem informacji, ze szczególnym uwzględnieniem procesów związanych z przetwarzaniem danych osobowych, z jednej strony powinien gwarantować osiągnięcie statutowego celu działania podmiotu, z drugiej społecznej odpowiedzialności biznesu, wyrażonej m.in. gwarancją poszanowania konstytucyjnych praw osób, których dane dotyczą.

Do korzyści wynikających z powołania ABI, w przyszłości DPO należy zaliczyć m.in. uzyskanie przez administratora danych efektywnego wewnętrznego nadzoru nad prawidłową realizacją obowiązków wynikających z przepisów w zakresie ochrony danych osobowych oraz zwiększenie autokontroli i podniesienie poziomu bezpieczeństwa danych osobowych. Wzmocnienie zaufania do administratorów lub podmiotów przetwarzających ze strony osób, których dane dotyczą oraz innych administratorów i podmiotów współpracujących. Warto jednak podkreślić, iż nawet jeśli RODO bezpośrednio nie nakłada obowiązku powołania DPO, niejednokrotnie korzystnym dla podmiotów może być dobrowolne jego wyznaczenie[28].

Zapewnienie przestrzegania rozporządzenia, przez wyznaczonego przez administratora DPO oznaczać w praktyce będzie dostosowanie dotychczas obowiązujacych regulacji z zakresu ochrony danych osobowych w organizacji do wytycznych zawartych w RODO i przepisach prawa krajowego, tym samym wymagać będzie implementacji zapisów w zakresie zasad przetwarzania danych osobowych, praw osób, których dane dotyczą, ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania danych, wymogów bezpieczeństwa przetwarzania oraz zgłoszenia naruszeń.

Powyższe możliwe jest do spełnienia pod warunkiem wyznaczenia osoby, wobec której stawia się wysokie wymagania w zakresie wiedzy, umiejętności oraz

[28] Article 29 Data Protection working party guidelines on Data Protection Officers (‚DPOs'), adopted on 13 December 2016, 16/EN WP 243, s. 5-6, (http://ec.europa.eu/justice/data-protection/index_en.htm [05.03.2017 r.])

kwalifikacji, a dodatkowo, której organizacyjne usytuowanie zapewni niezależne wykonywanie powierzonych zadań, a czynności wspierane będą przez najwyższe kierownictwo. To w interesie administratora, podmiotu przetwarzającego jest zapewnienie, by DPO był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych oraz by zapewnił mu zasoby niezbędne do wykonania powierzonych zadań.

LITERATURA

Ball R., (2000), *The scientific information environment in the next millennium*, „Library Management", vol. 21, no. 1.

Barta J., Fajgielski P., Markiewicz R., (2015), *Ochrona danych osobowych*, Wolters Kluwers S.A., Warszawa.

Barta P., Litwiński P., (2016), *Ustawa o ochronie danych osobowych*. Komentarz, C.H.Beck,Warszawa.

Dziekański, P., (2012), *Informacja jako dobro ekonomiczne będące źródłem przewagi konkurencyjnej*, „Nierówności społeczne a wzrost gospodarczy", nr 24.

Duliniec E., (1999), *Badania marketingowe w zarządzaniu przedsiębiorstwem*, PWN, Warszawa.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995).

http://ec.europa.eu/justice/data-protection/index_en.htm. Article 29 Data Protection Working Party Guidelines on Data Protection Officers (‚DPOs'), adopted on 13 December 2016, 16/EN WP 243. [05.03.2017].

http://giodo.gov.pl/pl/259/9718 Grupa robocza art. 29 ds. Ochrony Danych, Wytyczne dotyczące inspektorów ochrony danych ('DPO'), przyjęte w dniu 13 grudnia 2016 r., 16/EN WP 243 – tłumaczenie nieoficjalne, [05.03.2017 r.].

http://www.giodo.gov.pl/487/id_art/9146/j/pl/ Raport o ochronie danych osobowych. [05.03.2017].

http://www.sejm.gov.pl/Sejm7.nsf/druk.xsp?nr=2606 Projekt ustawy o ułatwieniu wykonywania działalności gospodarczej, Druk Nr 2606. [05.03.2017].

Krzystofek K, Szczepański M.S., 2002, *Zrozumieć rozwój – od społeczeństw tradycyjnych do informacyjnych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice.

Mednis A., (2015), *Administrator bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych z 7.11.2014 r. – ocena rozwiązań*, „Monitor Prawniczy", nr 6.

Oleksiejczuk E., Oleksiejczuk A., (2009), *Rola technologii informacyjnej w zarządzaniu oraz jej wpływ na kształtowanie się społeczeństwa informacyjnego*, „Przedsiębiorczość – Edukacja", tom 5.

Penc J., (1994), *Strategie zarządzania. Perspektywiczne myślenie systemowe działanie*, Placet, Warszawa.

Pomykalski A., (2001), *Zarządzanie innowacjami*, PWN, Warszawa - Łódź.

Porter M.E., (2001), *Porter o konkurencji*, PWE, Warszawa.

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).

Rozporządzenie Ministra Administarcji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych

osobowych przez administratora bezpieczeństwa informacji (Dz.U.2015.745).
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.1997.133.883 ze zm.).
Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U.2004.33.285).
Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U.2014.1662).
Żebrowski, A. (2004). *Bezpieczeństwo wiedzy – nowy atrybut działalności przedsiębiorstwa,* [w:] Borowiecki R., Kwieciński M. (red.) *Informacja i wiedza w zintegrowanym systemie zarzadzania*, Zakamycze, Kraków.

DPO - ANNOYING UNAVOIDABLE DUTY, WHETHER REAL MANAGEMENT SUPPORT IN PERSONAL DATA PROCESSING

Abstract: The idea of setting up a position where a person who is responsible for personal data protection within an organisation is not a new concept. The European legislature has indicated such a possibility by means of the provisions of Directive 95/46/WE, and this practice, in spite of being non-mandatory, has been developed in a number of Member States (France, Germany, Netherland, Sweden). The aim of this work is to present the history of establishing and causes of transformation of an "officer" function dealing with the data protection of an organisation. The article contains an analysis of the fundamental tasks, which according to the Act have been attributed to the information security administrator, but from 25th of May 2018 will be entrusted to the DPO (Data Protection Officer). The subject of this work is to review the requirements and resources with which the officer needs to be equipped in order to ensure accountability of the management processes and of personal data protection within the entity. It is also to show how the officer can adequately organise the needs and requirements of the new General Regulation of personal data protection within the entity.

Keywords: GDPR; processing personal data; DPO; requirements; responsibilities.