PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU
RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS nr 521 • 2018

ISSN 1899-3192
e-ISSN 2392-0041

Marek Jasztal
Komenda Wojewódzka Policji w Szczecinie, Uniwersytet Szczeciński
e-mail: jasztal@op.pl

ROLA AUDYTU WEWNĘTRZNEGO W OGRANICZENIU RYZYKA W OBSZARZE OCHRONY DANYCH OSOBOWYCH PO WPROWADZENIU RODO

THE ROLE OF INTERNAL AUDIT IN REDUCING RISK RELATED TO PERSONAL DATA PROTECTION FOLLOWING GDPR IMPLEMENTATION

DOI: 10.15611/pn.2018.521.07
JEL Classification: H83

Streszczenie: Dokonano analizy ryzyka w obszarze wymagań proceduralnych i prawnych dotyczących ochrony danych osobowych w odniesieniu do przepisów międzynarodowych i krajowych uwzględniających wejście w życie Rozporządzenia Parlamentu Europejskiego i Rady nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO). Badania zostały przeprowadzone metodą identyfikacji ryzyka w zakresie ochrony danych osobowych – identyfikacji wymagań, diagnozowania ryzyka, zapewnienia odpowiedzi na ryzyko. Na podstawie analizy przeprowadzonej z wykorzystaniem analizy ryzyka uzyskano dane o potencjalnych rodzajach ryzyka i ich wpływie na organizację w zakresie ochrony danych osobowych. Dane badawcze i analityczne zaprezentowane w artykule pozwoliły na obiektywne i niezależne zapoznanie się z zagadnieniem ochrony danych osobowych po wejściu w życie RODO oraz wyciągnięcie merytorycznych wniosków dotyczących wdrożenia praktycznego zarządzania ryzykiem do wymagań rozporządzenia.

Słowa kluczowe: audyt wewnętrzny, ryzyko, ochrona danych.

Summary: To analyse the risk related to procedural and legal requirements for the protection of personal data with respect to international and domestic regulations resulting from the implementation of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). Risk identification within personal data protection was the method of choice, which involved: identifying requirements, diagnosing the risk and ensuring an appropriate response to the risk. As a result of the analysis, based on risk analysis, potential risk types and their influence on the organisation in terms of personal data protection were identified. Research and analytical data presented in the paper allowed an objective and independent examination of issues related to personal data

protection following the implementation of GDPR thus allowing conclusions to be drawn on the implementation of practical risk management in compliance with the regulation.

Keywords: internal audit, risk, data protection.

1. Wstęp

W dniu 25 maja 2018 r. weszło w życie Rozporządzenie Parlamentu Europejskiego w związku z przetwarzaniem danych osobowych. Ogólne rozporządzenie o ochronie danych osobowych wprowadza dla wszystkich obywateli Unii Europejskiej pełne prawo do rozporządzania danymi – informacjami o sobie. Jednocześnie przedsiębiorcy, którzy do obecnej chwili gromadzili jak największą ilość danych o klientach, w tym danych niezwiązanych z realizacją obsługi klienta, będą mogli gromadzić i przetwarzać dane wyłącznie w zakresie niezbędnym do obsługi obywateli w zakresie realizowanych funkcji gospodarczych. Dodatkowo w przypadku zakończenia obsługi klienta jednostki gospodarcze oraz organy administracji będą zobowiązane do usunięcia danych zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych wykorzystywanych danych.

Geneza potrzeby wdrożenia nowych rozwiązań dotyczących ochrony danych osobowych dotyczyła agresywnego pozyskiwania danych przez podmioty gospodarcze w skali generującej ryzyka i niebezpieczeństwa dotyczące wykorzystania danych osobowych bez wiedzy osób, których te dane dotyczą, w celach handlowych, przestępczych oraz kryminalnych, w tym terrorystycznych, szczególnie w zakresie działań w cyberprzestrzeni. Unijne rozwiązania mają na celu zapewnienie obywatelom państwa europejskich możliwie jak największej ochrony, jednocześnie nie ograniczając im dostępu do nowoczesnych cyfrowych usług technologicznych.

W Polsce przepisy dotyczące ochrony danych osobowych obowiązują od ponad 20 lat. Należy jednak zwrócić uwagę, że do chwili obecnej nasz rząd, podobnie jak rządy większości krajów członkowskich Unii Europejskiej, nie wprowadził przepisów wewnętrznych w pełni dostosowujących rozwiązania krajowe do norm europejskich.

Celem artykułu jest określenie źródeł obowiązków, kierunków wdrożenia i realizacji procesu zarządzania ryzykiem w obszarze ochrony danych osobowych przetwarzanych przez upoważnione podmioty w związku z realizacją zadań.

2. Źródła, cele i podstawy prawne ochrony danych osobowych

Prawa człowieka to podstawowe normy przysługujące każdemu człowiekowi na każdym etapie jego życia, w każdym jego aspekcie. Niezbywalne prawa to prawo do życia, wolność słowa, zrzeszania się czy prawo do edukacji. Źródłem wszystkich

praw i wolności jest godność każdego człowieka. Prawa człowieka są takie same dla każdego człowieka niezależnie od wyznawanych wartości, poglądów czy religii i istnieją niezależnie od woli władzy czy przepisów prawa, państwo jedynie tworzy system ich ochrony [www1].

Charakter praw człowieka jest niezbywalny, co oznacza, że żadna władza nie może ich odebrać, nie można się ich zrzec, oraz jest nienaruszalny. Istnieją niezależnie od władzy i nie mogą być przez nią dowolnie regulowane. Podmiotem praw człowieka jest zazwyczaj jednostka, co oznacza, że są to prawa indywidualne. Prawa człowieka dają możliwość korzystania z wszelkich innych praw, dlatego ich przestrzeganie powinno być gwarantowane i chronione przez państwo.

Nadrzędną międzynarodową organizacją dbającą o przestrzeganie praw człowieka jest Organizacja Narodów Zjednoczonych. Instytucja została powołana jako następczyni Ligi Narodów w dniu 24 października 1945, kiedy postanowienia konferencji ratyfikowało pięciu przyszłych stałych członków Rady Bezpieczeństwa – Chiny, Francja, ZSRR, Wielka Brytania i USA oraz większość pozostałych państw członkowskich. ONZ stawia sobie za cel zapewnienie pokoju i bezpieczeństwa międzynarodowego, rozwój współpracy między narodami oraz popieranie przestrzegania wszelkich praw człowieka.

Organizacja Narodów Zjednoczonych 26 czerwca 1985 r. pod patronatem Komisji Praw Człowieka ONZ przygotowała projekt wytycznych, dotyczący regulacji odnoszących się do elektronicznych banków danych zawierających m.in. dane osobowe. Dokument ten, przyjęty w 1988 r., ogłoszony został 14 grudnia 1990 r. jako rezolucja zawierająca wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych. Powyższe wytyczne nie mają charakteru wiążącego. Stanowią jedynie zalecenia odnośnie do gwarancji, jakie powinny być zapewnione w przepisach krajowych w zakresie komputerowego przetwarzania danych osobowych.

Należy jednak zauważyć, że najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych, jest Konwencja Rady Europy nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych [Konwencja nr 108 Rady Europy]. Konwencja nałożyła na kraje członkowskie zobowiązanie stworzenia ustawodawstwa w zakresie ochrony danych osobowych, wskazując jednocześnie, w jakim kierunku ustawodawstwo to ma zmierzać. Celem konwencji jest zapewnienie, na obszarze państw członkowskich, każdemu – niezależnie od obywatelstwa i zamieszkania – ochrony jego praw i wolności, a w szczególności prawa do poszanowania sfery osobistej, w związku z automatycznym przetwarzaniem danych osobowych. Konwencja określiła minimalny zakres tych praw i skorelowanych z nimi obowiązków. Konwencja weszła w życie 1 października 1985 r.

Uwzględniając ogólnych charakter Konwencji, w 1990 r. rozpoczęto prace nad stosowną dyrektywą. Efektem tych prac było wydanie Dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony

osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych [Dyrektywa Parlamentu Europejskiego i Rady nr 95/46/WE]. Termin na jej implementację do porządków prawnych państw członkowskich wyznaczono na 23 października 1998 r. Zgodnie z przepisami dyrektywy dane osobowe to wszystkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przetwarzaniem zaś określono wszystkie – wymieniając je – operacje dokonywane na danych osobowych.

W polskim kanonie prawnym gwarancje ochrony danych osobowych zapewniła Konstytucja z 1997 r. [Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997]. Przepis artykułu 47 ustawy zagwarantował obywatelom prawo do prywatności, a przepis artykułu 51 – każdej osobie prawo do ochrony dotyczących jej informacji. Dodatkowo zobowiązania Polski, związane z akcesją do Unii Europejskiej, wymusiły konieczność zapewnienia ochrony danych osobowych takiej, jaką na swoim terytorium zapewniały państwa Unii. Zasady ochrony danych ustanowione Dyrektywą 95/46/EC wprowadzone zostały do polskiego porządku prawnego ustawą o ochronie danych osobowych. Ustawa o ochronie danych osobowych wprowadziła szczegółowe normy służące ochronie danych osobowych w Polsce, a do 1 maja 2004 r., czyli wstąpienia Polski do Unii Europejskiej, przeniosła do polskiego porządku prawnego wszystkie zasady określone w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady.

Wprowadzenie przepisów dotyczących ochrony danych osobowych do polskiego systemu prawnego pozwoliło na podpisanie przez Polskę w kwietniu 1999 r. i ratyfikowanie w maju 2002 r. Konwencji nr 108 Rady Europy. Działania te stanowiły przejaw postępującej demokratyzacji życia publicznego w Polsce i troski o ochronę prywatności każdego jej obywatela. Ustawa o ochronie danych osobowych [Ustawa z 29 sierpnia 1997] określiła prawne ramy obrotu danymi osobowymi, a także zasady, jakie należy stosować przy przetwarzaniu danych osobowych, sprecyzowała też prawa i obowiązki organów, instytucji i osób prowadzących zbiory danych osobowych oraz prawa osób, których dane dotyczą, w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej oraz poszanowanie jej życia prywatnego. Ustawa, realizując wymagania stawiane przez Wspólnotę, skonkretyzowała konstytucyjnie zagwarantowane prawo do decydowania o tym, komu, w jakim zakresie i w jakim celu przekazujemy nasze dane osobowe, dając ustawowe gwarancje przestrzegania tego prawa, poprzez wyposażenie osób, których dane dotyczą w środki służące realizacji tego prawa, a odpowiednie organy i służby w środki prawne gwarantujące jego przestrzeganie. Podstawowym jej założeniem jest przyznanie każdej jednostce prawa do ochrony dotyczących jej danych.

Ustawa określa zasady, jakie należy stosować przy przetwarzaniu danych osobowych, precyzuje prawa i obowiązki organów, instytucji i osób prowadzących zbiory danych osobowych oraz prawa osób, których dane dotyczą, w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej oraz poszanowanie jej życia prywatnego. Dodatkowo szczegółowe obowiązki odnośnie

do zabezpieczenia danych określone są w rozdziale 5 ustawy oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 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 [Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004].

Dane osobowe mogą dotyczyć również informacji na temat kodu genetycznego człowieka. Zgodnie z przepisami Powszechnej Deklaracja (UNESCO) w sprawie genomu ludzkiego i praw człowieka z 11 listopada 1997 r. danym genetycznym – dającej się zidentyfikować osoby zgodnie z artykułem 7 Powszechnej deklaracji – należy zapewnić poufność. Jak wynika z treści tego aktu, taką ochroną objęte są dane genetyczne bez względu na cel, w jakim są one gromadzone. Przykładowo wskazano, iż takie dane mogą być gromadzone w celach badawczych. Ograniczenie powyższej zasady poufności może nastąpić wyłącznie w granicach przewidzianych przepisami prawa [Universal Declaration on The Human Genome and Human Rights 1997].

3. Zasady ochrony danych osobowych według RODO

Mianem RODO określa się nowe unijne rozporządzenie, które od 25 maja 2018 r. reguluje ochronę danych osobowych w całej Unii Europejskiej.

Obowiązek wdrożenia rozporządzenia ma każdy przedsiębiorca i instytucja, którzy przetwarzają dane osobowe mieszkańców UE. Każdy podmiot niezależnie od miejsca ulokowania jego serwerów czy siedziby może być ścigany i karany za naruszenie postanowień RODO w każdym z państw członkowskich, których obywateli dane naruszono [www3].

Przepisy artykułu 5 RODO wprowadziły zasady, którymi powinien się każdorazowo kierować administrator przy przetwarzaniu danych.

Wyróżniamy następujące zasady:

1. Zasadę zgodności z prawem, rzetelności i przejrzystości, dotyczącą obowiązku stosowania przepisów prawnych powszechnie obowiązujących i wewnętrznych krajowych w zakresie przetwarzania danych oraz w sposób rzetelny i przejrzysty dla osoby, której dotyczą.
2. Zasadę ograniczenia celu przetwarzania, która oznacza, że zbieranie danych powinno odbywać się w konkretnych, wyraźnych i prawnie uzasadnionych celach, z wyłączeniem zakazu ich dalszego przetwarzania do celów archiwalnych w interesie publicznym, celów naukowych oraz statystycznych i historycznych.
3. Zasadę minimalizacji dotyczącą ograniczenia gromadzenia danych do zakresu niezbędnego do osiągnięcia celów ich przetwarzania.
4. Zasadę prawidłowości wymagającą, aby dane były prawidłowe, okresowo uaktualniane, a dane nieprawidłowe powinny być usunięte lub sprostowane.

5. Zasadę ograniczenia przechowywania dotyczącą możliwości identyfikacji osoby, której dotyczą, tylko przez okres niezbędny do celów, w których są przetwarzane.

6. Zasadę integralności i poufności dotyczącą obowiązku zachowania bezpieczeństwa podczas przetwarzania, w szczególności ochronę przed niedozwolonym lub niezgodnym z prawem ich przetwarzaniem.

7. Zasadę rozliczalności wyrażającą się w odpowiedzialności administratora danych w zakresie ich przetwarzania zgodnie z obowiązującymi regułami.

4. Zarządzanie ryzykiem ochrony danych osobowych

Zgodnie z postanowieniami Międzynarodowych Standardów Praktyki Zawodowej Audytu Wewnętrznego audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów: zarządzania ryzykiem, kontroli i ładu organizacyjnego, i przyczynia się do poprawy ich działania. Pomaga organizacji osiągnąć cele, dostarczając zapewnienia o skuteczności tych procesów, jak również poprzez doradztwo [*Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego*].

Zarządzanie ryzykiem ma na celu wyeliminowanie lub ograniczenie do akceptowalnego poziomu zdiagnozowanego ryzyka. Jest to podejmowanie decyzji i realizacja działań prowadzących do osiągnięcia przez podmiot akceptowalnego poziomu ryzyka. W praktyce zarządzanie ryzykiem utożsamiane jest z procesami diagnozy i sterowania ryzykiem, których celem jest intencjonalne zapewnienie stabilnych wyników finansowych oraz stworzenie uwarunkowań dalszego rozwoju. W ramach zarządzania ryzykiem należy odpowiedzieć na następujące pytania:

- Jakie są cele jednostki w obszarze ochrony danych osobowych?
- Co może pójść nie tak (czyli jakie ryzyka można zidentyfikować)?
- Jakie jest tego prawdopodobieństwo?
- Co się stanie, jeśli coś pójdzie nie tak?
- Kto jest „właścicielem" ryzyka?
- Kto poniesie konsekwencje, jeśli ryzyko wystąpi?
- Jaki jest „apetyt na ryzyko"?
- Co należy zrobić, by usunąć zagrożenie, by sprowadzić ryzyko do akceptowalnego poziomu?
- Co można zrobić, by zmniejszyć prawdopodobieństwo ponownego wystąpienia zagrożenia?

5. Mechanizmy identyfikacji i analizy ryzyka ochrony danych osobowych

Termin „ochrona danych osobowych" został szczegółowo zdefiniowany w przepisach ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Jednostki organizacyjne funkcjonujące w przestrzeni prawno-gospodarczej są zobowiązane do realizacji zadań w sposób rzetelny, legalny, celowy, oszczędny, jawny oraz efektywny i skuteczny. Określone powyżej mechanizmy realizacji działań dotyczą wszystkich obszarów działalności, w tym obszaru dotyczącego przetwarzania danych osobowych. Właściwe wykonywanie zadań wymaga więc zapewnienia odpowiednich i skutecznych mechanizmów powierzania uprawnień i odpowiedzialności, zasad realizacji zadań oraz zapewnienia właściwego systemu nadzoru i ochrony danych. Instrumentem wspierającym kierownika jednostki w tych działaniach jest obiektywny i niezależny audyt wewnętrzny.

Przez wiele lat audyt wewnętrzny określano jako „oczy i uszy zarządu". Jest to częściowo prawdziwe, ponieważ audytor powinien umieć rozpoznawać, czego potrzebuje zarząd, co prezes firmy lub dyrektor jednostki sektora finansów publicznych by zrobił, jeśli miałby czas i wiedział, jak to zrobić [Winiarska 2017, s. 77].

Niezależnie od sektora gospodarki istnieje silna potrzeba ograniczenia ryzyka, nieprawidłowości i oszustw w obszarze przetwarzania danych osobowych. Istnieje również zapotrzebowanie na fachowy personel kierowniczy oraz pracowniczy potrafiący zarządzać działaniami, w tym ryzykiem związanym z realizacją przetwarzania danych.

Zarządzanie ryzykiem w obszarze ochrony danych osobowych może pomóc oceniać prawdopodobieństwo zajścia zdarzeń, które mogą mieć niekorzystny wpływ na realizację celów oraz ponoszone koszty. Jednym z elementów zarządzania ryzykiem jest przygotowanie planów awaryjnych, które w przypadku wystąpienia zagrożeń pozwolą skutecznie wykonywać zadania. Analiza ryzyka nie ma na celu szukania błędów pracowników, ale zlokalizowanie takich miejsc (obszarów), które prędzej czy później mogą doprowadzić do zaistnienia (pojawienia się) nieprawidłowości lub też sytuacji zaskakujących, nieoczekiwanych.

Audyt wewnętrzny dokonuje oceny systemu zarządzania ryzykiem i przyczynia się do jego usprawnienia.

Dokonując oceny ryzyka w zakresie systemu ochrony danych osobowych, należy wskazać na następujące zidentyfikowane ryzyka, będące determinantami możliwości pojawienia się błędów i nieprawidłowości w obszarze RODO:

- determinanty prawne ryzyka – rozumiane jako brak działań w zgodzie z obowiązującymi przepisami prawa w zakresie RODO, brak wewnętrznych mechanizmów prawnych i proceduralnych (np. brak kompletnej, aktualnej i rzetelnej wymaganej przepisami rozporządzenia polityki ochrony danych osobowych),
- determinanty osobowe ryzyka – dotyczą spełnienia wymagań i obowiązków w zakresie powołania inspektora ochrony danych (strażnika przestrzegania reguł RODO w jednostce), wyznaczenia administratora, czyli podmiotu, który ustala cele i sposoby przetwarzania danych osobowych, oraz procesora, który przetwarza dane w imieniu administratora na podstawie stosownej umowy,
- determinanty informatyczne ryzyka – wynikają z niespełnienia określonych w rozporządzeniu RODO wymagań dotyczących funkcji systemu ochrony danych, wad i błędów oraz niedoskonałości systemu informatycznego w zakresie rozliczalności algorytmów ich ochrony oraz archiwizacji,
- determinanty ryzyka dotyczące uzyskania zgody na przetwarzanie danych – dotyczą błędów i nieprawidłowości w uzyskaniu zgody na przetwarzanie danych osobowych dotyczących naruszenia zasad dobrowolności, konkretności, świadomości oraz jednoznaczności w zakresie uzyskania zgody na przetwarzanie danych,
- determinanty ryzyka dotyczące spełnienia obowiązków w zakresie dokumentacji przetwarzania danych osobowych wynikają z braku posiadania w jednostce rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania danych,
- determinanty ryzyka dotyczące organizacji przetwarzania danych w poszczególnych komórkach, nadawania i cofania uprawnień do przetwarzania danych, przypisania odpowiedzialności w zakresie informacji osobowych,
- determinanty analityczne ryzyka – dotyczą oceny skutków przetwarzania danych osobowych realizowanej dla ochrony danych osobowych przez firmy i administrację publiczną w szczególnych przypadkach,
- determinanty umowne ryzyka – odnoszą się do wymagań dotyczących treści umowy powierzania przetwarzania danych osobowych,
- determinanty ryzyka dotyczące uprawnień osób, których dane osobowe są przetwarzane – brak zapewnienia wymaganej kontroli nad przetwarzaniem ich danych osobowych,
- determinanty dotyczące ryzyka kar w przypadku naruszenia przepisów rozporządzenia RODO – odnoszą się do obszernego katalogu sankcji w razie naruszenia przepisów, w szczególności w zakresie kar pieniężnych.

6. Zakończenie

Pojęcie danych osobowych należy rozumieć jako wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, które z racji swojej wrażliwości powinny podlegać należytej ochronie. Ochrona ma szczególne znaczenie w obecnych czasach rewolucji technologicznej i elektronicznego (cybernetycznego) wykorzystania danych o osobie w transakcjach i przetwarzanych informacjach.

Wprowadzenie szczegółowych mechanizmów kontrolnych dotyczących przetwarzania danych osobowych nie może być w jednostce publicznej lub prywatnej realizowane bez wprowadzenia systemu zarządzania ryzykiem. Wdrożenie zarządzania ryzykiem w obszarze ochrony danych przyczyni się do wzmocnienia nadzoru nad prawidłowością, celowością i legalnością ich wykorzystania oraz osiągnięcia legalności i efektywności działania.

Szczególne znaczenie w zakresie ograniczenia ryzyka nieprawidłowości w obszarze wprowadzenia wymagań Rozporządzenia Parlamentu Europejskiego i Rady nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) ma audyt wewnętrzny. Wiedza i doświadczenie audytora wewnętrznego w ramach funkcji prewencyjnych audytu może wielu problemom zaradzić, pod warunkiem że odpowiednio wcześniej je zauważymy. Okresowe przeglądy dotyczące procesów i procedur w ramach RODO mogą ujawnić odpowiednio wcześnie problemy, zidentyfikować braki, nieprawidłowości i nieefektywności.

Literatura

Dyrektywa Parlamentu Europejskiego i Rady nr 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dziennik Urzędowy Wspólnot Europejskich z dnia 23.11.1995, nr L 281/31.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz.U. z 1997, nr 78, poz. 483.

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

Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego. Załącznik do komunikatu Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. (poz. 28).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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, nr 100, poz. 1024.

Universal Declaration on The Human Genome and Human Rights, 1997.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 1997, nr 133, poz. 883.
Winiarska K., 2017, *Audyt wewnętrzny – teoria i zastosowanie*, Difin, Warszawa.
[www1] https://amnesty.org.pl/co-robimy/prawa-czlowieka/.
[www2] https://giodo.gov.pl/pl/147/709.
[www3] https://gazetaprawna,pl/co to jest RODO.