BEZPIECZEŃSTWO DANYCH OSOBOWYCH W ŚWIETLE NOWYCH PRZEPISÓW (RODO) – PRZEGLĄD HISTORYCZNY

Monika ODLANICKA-POCZOBUTT[1*], Aleksandra SZYSZKA-SCHUPPIK[2]

[1]Politechnika Śląska, Wydział Organizacji i Zarządzania; monika.odlanicka-poczobutt@polsl.pl
[2]Politechnika Śląska
*Autor do korespondencji

Streszczenie: W artykule przedstawiono założenia obowiązującego od dnia 25 maja 2018 roku 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 sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwane dalej RODO). Omówiono także zmiany, które Rozporządzenie to wprowadziło, a które z jednej strony dają nowe prawa osobom, których dane są przetwarzane, a z drugiej strony nakładają na Administratorów nowe obowiązki z tym związane. Celem artykułu jest prezentacja podstawowych różnic wynikających z obu w/w aktów prawnych, ze szczególnym uwzględnieniem nowych obowiązków administratorów, którzy odpowiedzialni są za prawidłowe, czyli zgodnie z prawem, przetwarzanie posiadanych danych osobowych. Wskazano jakie działania należy podjąć aby zapewnić, że przetwarzanie danych osobowych jest zgodne z obowiązującym stanem prawnym zapewniając jednocześnie legalność, rzetelność i przejrzystość przetwarzania danych osobowych.

Słowa kluczowe: bezpieczeństwo informacji, RODO, ryzyko, przetwarzanie danych osobowych.

SECURITY OF PERSONAL DATA IN A LIGHT OF NEW REGULATIONS (RODO) – HISTORICAL REVIEW

Abstract: The article presents the assumptions of Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data and the repeal of Directive 95 / 46 / WE (hereinafter referred to as RODO). Changes were also discussed, which the Regulation introduced, and which on the one hand give new rights to persons whose data is processed, and on the other hand impose new obligations on the Administrators. The aim of the article is to present the basic differences resulting from both legal acts, with particular emphasis on the new obligations of administrators who are responsible for the correct, that is, the lawful processing of personal data. It was indicated what actions should be

taken to ensure that the processing of personal data is consistent with the current legal status while ensuring the legality, reliability and transparency of personal data processing.

Keywords: information security, RODO, risk, information security, RODO, risk, processing of personal data.

1. Wprowadzenie

Tematyka związana z bezpieczeństwem informacji nie jest nowym zagadnieniem, jednakże próby podejmowane w zakresie systemowej standaryzacji praktyk bezpieczeństwa informacji trwają dopiero od początku lat dziewięćdziesiątych ubiegłego wieku. W praktyce gospodarczej kompleksowa dbałość o bezpieczeństwo informacji jest zagadnieniem nowym, jednak skala i zakres problemów powstających w wyniku nieuwzględniania ryzyka wynikającego m.in. z utraty aktywów informacyjnych nie może zostać niezauważona przez kadrę zarządzającą.

Niestety, niewiele podmiotów w Polsce na dzień dzisiejszy spełnia wymagania nowych przepisów, część firm rozpoczęła proces wdrażania systemu ochrony danych osobowych, który ze względu na złożoność tematu potrwa jeszcze parę miesięcy, inne firmy, głównie te, które dostosowały swoją działalność do wymagań Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2016, poz. 922 ze zm.) nadal bazują na wdrożonych już rozwiązaniach i powoli rozpoczynają proces aktualizacji obowiązujących procedur. Zdarzają się także firmy, które nie rozpoczęły jeszcze żadnych działań związanych z wejściem w życie nowych przepisów.

RODO niewątpliwie jest dużym wyzwaniem dla wszystkich przedsiębiorców przetwarzających dane osobowe, zmienia ono dotychczasowe podejście oparte o sztywny schemat. Wprowadza nakaz takiego doboru środków technicznych i organizacyjnych w przetwarzaniu danych osobowych, aby zagwarantować ich bezpieczeństwo przy jednoczesnym uwzględnieniu realnego ryzyka utraty lub nieautoryzowanego przetwarzania tych danych.

W artykule zaprezentowano podstawowe zasady przetwarzania danych osobowych zgodnie z nieobowiązującą już ustawą o ochronie danych osobowych wskazując jednocześnie wymagania nowego 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 sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Celem artykułu jest prezentacja podstawowych różnic wynikających z obu w/w aktów prawnych, ze szczególnym uwzględnieniem nowych obowiązków administratorów, którzy odpowiedzialni są za prawidłowe, czyli zgodnie z prawem, przetwarzanie posiadanych

danych osobowych. Wskazano także istotne rozwiązania, które muszą Administratorzy wdrożyć aby zagwarantować bezpieczeństwo przetwarzanych danych przy jednoczesnym zapewnieniu wszystkich praw osób, których dane są przetwarzane.

2. Historyczny rys kształtowania się ochrony danych

Od dnia 25 maja 2018 roku w Polsce oraz w pozostałych krajach Unii Europejskiej obowiązuje RODO. Rozporządzenie to zastąpiło obowiązującą w Polsce od roku 1997 ustawę o ochronie danych osobowych, która była pierwszym aktem prawnym, ustalającym normy, zasady przetwarzania ale także zasady ochrony danych osobowych. Ustawa ta, zwana dalej UODO, wzorowana była na dyrektywie Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Celem tej dyrektywy było określenie minimalnych ram, zasad przetwarzania danych osobowych we wszystkich krajach Unii.

Podstawowym prawem wynikającym z Dyrektywy jest prawo do przejrzystej informacji. Przede wszystkim osoby, których dane osobowe są przetwarzane, muszą zostać poinformowane o tym, kto administruje ich danymi osobowymi, dodatkowo muszą znać cel przetwarzania tych danych oraz kategorie odbiorców ich danych osobowych (artykuł 10 Dyrektywy). Obowiązkiem przetwarzającego dane, administratora, jest poinformowanie o konieczności lub dobrowolności przekazania danych. Reguły określone w tym zakresie w Dyrektywie obowiązują nadal. Na gruncie UODO był to tzw. obowiązek informacyjny określony w art. 24 oraz 25 wprowadzony także przez RODO w art. 13 oraz 14.

Dyrektywa wskazywała ramy prawne przetwarzania danych osobowych. To właśnie w artykule 7 określono kiedy dane osobowe mogą być przetwarzane zgodnie z prawem wymieniając m.in. zgodę osoby, konieczność realizacji umowy, wykonanie obowiązku prawnego czy ochronę żywotnych interesów osób. Podobne kryteria regulujące przetwarzanie danych osobowych można znaleźć zarówno w UODO jak i w RODO. Dyrektywa ta określała także odpowiedzialność i możliwe sankcje za przetwarzanie danych niezgodnie z obowiązującymi przepisami oraz zasady przekazywania danych do państw trzecich tzn. tych spoza Unii Europejskiej (Barta, et al., 2007, s. 85-87).

Ochrona podstawowych interesów obywateli została ustanowiona także w Konstytucji RP z 1997 roku. To Konstytucja w art. 47 oraz art. 51 reguluje ogólne prawa Polaków. Art. 47 gwarantuje „prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Uszczegółowieniem tego artykułu są zapisy w art. 51, które gwarantują, iż tylko i wyłącznie na podstawie ustawy obywatele mogą być zmuszani do ujawniania informacji o sobie. Ponadto państwo polskie nie może pozyskiwać,

gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym, na koniec wskazuje, że każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Zapisy te są więc powieleniem zasad określonych w Dyrektywie (Błotny, 2017).

W oparciu o wytyczne dyrektywy, opracowano i wdrożono UODO, która to wprowadzała podstawowe definicje oraz określała ramy prawne ochrony danych osobowych. Ustawa ta, wprowadzona w roku 1997, przez następne 21 lat, regulowała zasady przetwarzania danych osobowych, powołała do życia urząd Generalnego Inspektora Ochrony Danych Osobowych (dalej GIODO), ustalała zasady prowadzenia kontroli poprawności przetwarzania danych osobowych oraz wprowadzała przepisy karne za nieprzestrzeganie w/w przepisów.

Art. 2 UODO określał zakres przedmiotowy stosowania ustawy – ustawą objęte były dane osobowe przetwarzane niezależnie od formy, mogły to być kartoteki, skorowidze, księgi, wykazy, inne zbiory ewidencyjne, mogły to być także dane przetwarzane w systemach informatycznych. Z kolei zaś RODO przedstawia inne podejście wskazując, że ma ono zastosowanie do „przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych" (artykuł 2).

W art. 3 UODO zawarty został zakres podmiotowy. Zapisami ustawy objęte były organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne oraz podmioty niepubliczne realizujące zadania publiczne oraz osoby fizyczne i osoby prawne oraz jednostki organizacyjne niebędące osobami prawnymi, jeżeli przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Ze stosowania ustawy wyłączone zostały osoby fizyczne, przetwarzające dane osobowe we własnym celu (domowym lub osobistym) oraz podmioty mające siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych.

Tabela 1.
Zestawienie obowiązków Administratora

ZAKRES OBOWIĄZKÓW	PODSTAWA PRAWNA UODO	PRZEPISY KARNE
Obowiązki informacyjne	Art. 24-25	Art. 54
Obowiązek udzielenia informacji	Art. 32-33	Art. 54
Obowiązek przetwarzania danych osobowych w sposób zgodny z prawem	Art. 26	Art. 49 – 50
Obowiązek zapewnienia poufności	Art. 37-39	Art. 51
Obowiązek zapewnienia bezpieczeństwa przetwarzanym danym osobowym	Art. 36	Art. 52
Obowiązek zarejestrowania zbiorów danych osobowych lub administratora bezpieczeństwa informacji	Art.40, Art. 46b	Art.53

Źródło: opracowanie własne na podstawie Barta, et al., 2007.

Ustawa nakładała szereg obowiązków na Administratorów danych osobowych, Administratorów czyli na organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych. W poniższej tabeli przedstawiono te obowiązki wraz ze wskazaniem artykułu ustawy:

W roku 2016 zostało uchwalone RODO, którego wejście w życie w krajach Unii Europejskiej zaplanowano na dzień 25 maja 2018 roku, dając tym samym dwuletni czas na dostosowanie się do nowych wymagań związanych z przetwarzaniem danych osobowych. Cel wdrożenia RODO najlepiej obrazuje motyw 6, który wskazuje, że potrzeba uregulowania zasad przetwarzania danych osobowych wynika z szybkiego postępu technicznego i globalizacji, które to spowodowały pojawienie się nowych zagrożeń. Ponadto wzrasta ilość przetwarzanych danych osobowych nie tylko przez przedsiębiorstwa prywatne ale także państwowe, w związku z tym system ochrony danych osobowych oparty na RODO musi odpowiadać pojawiającym się nowym technologiom, stąd zapis w motywie 15 RODO, że Rozporządzenie to musi być neutralne pod względem technicznym tzn. nie może wskazywać konkretnych rozwiązań technicznych, które Administratorzy powinni wdrożyć (Kawecki, et al., 2017, s. 21).

W dniu 25 maja 2018 roku weszła także w życie nowa Ustawa z dnia 10 maja 2018 o ochronie danych osobowych (Dz.U. 2018, poz. 1000). Ustawa ta ustala m.in. tryb zawiadamiania o powołaniu Inspektora Ochrony Danych (IOD), tryby zatwierdzania kodeksów postępowania czy zasady postępowania w sprawie naruszenia obowiązujących przepisów z zakresu ochrony danych osobowych. Niestety, ustawa ta, zgodnie z zasadą neutralności technologicznej przyjętą przez RODO, nie zawiera praktycznie żadnych wskazówek, które Administratorzy mogliby wykorzystać przy budowaniu własnego modelu systemu ochrony danych osobowych, muszą więc bazować na własnych doświadczeniach lub korzystać z usług specjalizujących się w tym zakresie firm.

3. Istota RODO, przesłanki stosowania, podstawowe pojęcia

Wejście w życie RODO ogłaszane jest niejednokrotnie jako „rewolucja” w ochronie danych osobowych. Czy jednak słusznie? Czy RODO faktycznie wprowadza rewolucyjne rozwiązania, które dotychczas nie były stosowane w Polsce? W dalszej części artykułu zostaną omówione podstawowe wymagania RODO stawiane podmiotom przetwarzającym dane osobowe, wskazane zostaną także różnice wynikające z UODO i RODO.

Przede wszystkim RODO zmienia model budowanego przez przedsiębiorstwa systemu ochrony danych osobowych, nowy model oparty jest na analizie ryzyka związanego z przetwarzaniem danych osobowych, dotychczas system ten był oparty o wymaganą prawem dokumentację, której treść została uregulowana odpowiednimi przepisami. Podstawą do

budowy systemu ochrony danych osobowych w przedsiębiorstwie lub podmiocie państwowym ma być obecnie przeprowadzenie szczegółowej analizy ryzyka związanego z przetwarzaniem danych osobowych, na podstawie której dobierane są odpowiednie środki techniczne i organizacyjne gwarantujące bezpieczeństwo danych, analiza ta poprzedzona musi być przeprowadzeniem inwentaryzacji przetwarzanych danych czyli zidentyfikowaniem jakie dane (czyje) i w jakim zakresie są przetwarzane i czy ich przetwarzanie nie jest prowadzone z naruszeniem prawa (Greser, 2018).

Podobnie jak pod rządami UODO tak i RODO, nakazuje wdrożenie przez Administratorów odpowiednich środków. UODO, jako jeden ze środków organizacyjnych, w art. 36a, ust. 1 dawało Administratorom prawo do powołania Administratora Bezpieczeństwa Informacji (ABI), osoby odpowiedzialnej za ustalenie i przestrzeganie zasad przetwarzania danych osobowych. Ustawa określała jednocześnie podstawowe obowiązki ABI, były to:

- zapewnienie przestrzegania przepisów o ochronie danych osobowych poprzez prowadzenie sprawdzeń poprawności przetwarzania danych, nadzorowanie aktualności opracowanej dokumentacji, tj. Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- prowadzenie rejestru zbiorów danych przetwarzanych przez Administratora danych.

Zgodnie z art. 46b UODO Administrator był zobowiązany do zarejestrowania Administratora Bezpieczeństwa Informacji w rejestrze prowadzonym przez GIODO. Po wejściu w życie RODO rejestr ten nie jest już prowadzony, a w miejsce ABI Administrator ma prawo do powołania Inspektora Ochrony Danych IOD, zwanego także DPO (Data Protection Officer). Art. 37 RODO wskazuje, że powołanie IOD jest obligatoryjne gdy:

- przetwarzania dokonują organ lub podmiot publiczny,
- 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,
- główna działalność Administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Jednakże Grupa Robocza art. 29 zaleca w swoich wytycznych powołanie IOD także w przypadku innych organizacji – Grupa Robocza art. 29 ds. Ochrony danych osobowych – „Wytyczne dotyczące inspektorów ochrony danych („DPO") przyjęte w dniu 13 grudnia 2016 r. ostatnio zmienione przyjęte w dniu 5 kwietnia 2017 r. Grupa ta jest organem doradczym w zakresie poprawności przetwarzania danych i jej stanowiska są bardzo często brane przez Administratorów przy budowie systemu ochrony danych osobowych (GIODO, 19.05.2018).

RODO, podobnie jak UODO, wprowadza także podstawowe definicje (art. 4), które wraz z krótkim komentarzem zostały zaprezentowane poniżej:

- Dane osobowe – to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Z kolei „możliwa do zidentyfikowania osoba fizyczna" to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Definicja ta bardzo zbliżona jest do definicji ustalonej w art. 6 UODO z tą różnicą, że RODO zawiera szerszy katalog przykładowych danych osobowych. Nie zawsze jednak każda informacja będzie dla drugiej osoby daną osobową np. numer pojazdu VIN będzie daną osobową dla podmiotów, które mają dostęp do Centralnej Ewidencji Pojazdów i Kierowców (CEPiK), dla innych osób daną taką nie będzie. Podobnie jest także z numerem pracownika lub numerem jego konta bankowego – dla osób, które posiadają dostęp do odpowiednich narzędzi będzie to dana osobowa – dla pozostałych już nie, numer pacjenta – dla przychodni, która przesyła próbkę materiału do badań do laboratorium jest to dana osobowa ponieważ posiada ona narzędzia do wskazania konkretnej osoby, dla laboratorium nie będzie to dana osobowa ponieważ nie ma możliwości wskazania konkretnej osoby i nie wie czyją próbkę bada.
- Dane osobowe sensytywne, wrażliwe w rozumieniu UODO lub dane szczególne w rozumieniu RODO – w świetle obowiązujących dzisiaj przepisów zabronione jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej. Dane te jednak można przetwarzać sytuacji, gdy zachodzi jedna z przesłanek, tj. m.in.:
  - Zgoda osoby, której dane są przetwarzane. Dotychczas zgoda ta musiała być wyrażona pisemnie, teraz RODO zwalnia z tego obowiązku.
  - Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą.

- Podobnie jak na kanwie UODO – przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą (…).
- Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.
- (…).

Tutaj znowu RODO nie ma innego podejścia niż UODO.

- Przetwarzanie – to operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Podobnie jak przy definicji danych osobowych – także tutaj RODO jest bardziej precyzyjne niż dotychczas obowiązujące przepisy, mowa jest np. o niszczeniu danych – w rozumieniu RODO już sama możliwość usunięcia, zniszczenia danych jest także ich przetwarzaniem.
- Pseudonimizacja – to definicja, której dotychczas nie było w polskim ustawodawstwie. RODO określiło psedonimizację jako – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Bardzo dobrym przykładem pseudonimizacji jest wspomniane powyżej zastępowanie imienia i nazwiska pacjenta – numerem, kodem, który bez użycia odpowiednich środków, nie jest daną osobową.
- Administrator – w rozumieniu RODO – Administrator to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Z kolei ustawa wspominała o Administratorze danych – czyli o organie, jednostce organizacyjnej, podmiocie lub osobie, które decydują celach i środkach przetwarzania danych osobowych. Tutaj ponownie widać, że definicje te są zbieżne. Administratorem jest więc sama spółka, a nie jej organy czy osoby ją reprezentujące.
- Podmiot przetwarzający – zwany także procesorem, to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora. Najlepszym przykładem podmiotu przetwarzającego dane na zlecenie Administratora jest zewnętrzny dział informatyczny, który świadczy usługi pomocy, utrzymania serwerów, obsługi programu itp. Firma ta zapewniając usługi serwisowe ma dostęp do praktycznie wszystkich danych osobowych, które przetwarza Administrator. Przykładem procesora może także być podmiot świadczący

usługi w ramach outsourcingu działu księgowo-finansowego lub kadrowo-płacowego. Na gruncie UODO brak było precyzyjnej definicji procesora.

– Zgoda osoby (wg RODO), której dane dotyczą oznacza dobrowolne, konkretne, świadome i jedno-znaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Na gruncie UODO zgoda wyraźnie była określona jako „oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie". UODO określało także, że zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W stosunku do UODO widać wyraźną zmianę wprowadzoną przez RODO, które dopuszcza domniemanie, dorozumianie zgody z oświadczenia woli o innej treści. Podobne stanowisko można znaleźć także w Wytycznych Grupy Art. 29 z dnia 13 lipca 2011 roku – Opinia 15/2011 w sprawie definicji zgody (str. 24) wskazując, że zgoda to „działania prowadzą do niebudzącego wątpliwości wniosku, że udzielono zgody". Takim przykładem świadomie udzielonej zgody może być zapisanie się do opcji newslettera oferowanej przez większość portali czy stron internetowych (GIODO, 20.05.2018)

Dane osobowe, zarówno pod rządami RODO jak i UODO muszą być przetwarzane zgodnie z obowiązującym prawem. Wg UODO każdy Administrator miał obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które zagwarantują poufność, integralność i rozliczalność przetwarzanych danych. Te trzy pojęcia zostały zdefiniowane w 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 (Dz.U. z 2004 r. Nr 100, poz. 1024). Pod pojęciem integralności należy rozumieć, że dane nie zostały zmienione w sposób nieautoryzowany (dotyczy także zniszczenia danych), z kolei poufność to zagwarantowanie, że dane nie są udostępniane osobom, podmiotom nieupoważnionym do ich dostępu. Na koniec rozliczalność to możliwość przypisania konkretnych działań konkretnej osobie, w praktyce oznacza to, iż każdy użytkownik, osoba przetwarzająca dane posługuje się własnym loginem i własnym hasłem. RODO także zawiera informacje o konieczności zapewnienia integralności i poufności przetwarzanych danych osobowych (art. 5, ust. 1, pkt. f). Wprowadza jednak odmienną definicję rozliczalności – w rozumieniu RODO rozliczalność to możliwość wykazania przez Administratora przestrzeganie przepisów, a nie jak to było dotychczas – przypisanie działań konkretnej osobie.

Na gruncie RODO mamy więc do czynienia z „domniemaniem winy", to Administrator ma udowodnić, że system ochrony danych osobowych zbudowany przez niego jest odpowiedni do kategorii i skali przetwarzania danych osobowych oraz możliwych zagrożeń związanych z tym przetwarzaniem (Gawroński, et al., 2018, s. 37).

Art. 5, ust. 1 RODO określa więc podstawowe zasady przetwarzania danych osobowych, do których Administrator musi dostosować swoje procedury. Artykuł ten wskazuje, że dane zwykłe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość") – jest to tak zwana zasada legalności przetwarzania danych osobowych. Wyjaśnienie kiedy dane można przetwarzać zgodnie z prawem znajduje się w art. 6 RODO. Dane można przetwarzać:
  - na podstawie zgody, która w przeciwieństwie do UODO może być dorozumiana;
  - w związku z wykonaniem umowy lub do podjęcia działań przed zawarciem umowy;
  - w celu wykonania obowiązku prawnego np. zawarcie umowy o pracę;
  - gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotne interesy to przede wszystkim zdrowie i życie osoby, której dane są przetwarzane jednak zgodnie z przyjętą doktryną żywotne interesy mogą dotyczyć także kwestii majątkowych, przetwarzanie na podstawie tej przesłanki dopuszczalne jest jeżeli można założyć, że zainteresowany udzieliłby takiego zezwolenia (Barta, i Litwiński, 2009, s. 211);
  - gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
  - gdy przetwarzanie jest niezbędne do osiągnięcia celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
- Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami – („ograniczenie celu"). Na gruncie UODO była to zasada „celowości" czyli związania z celem.
- Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celów, w których są przetwarzane („minimalizacja danych") – zasada ta nakazuje zbieranie danych tylko i wyłącznie w takim zakresie w jakim w danym momencie są nam niezbędne. Zakazuje zbierania danych na „zapas".
- Prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"). Pod rządami UODO zasada ta nazywana była zasadą „merytorycznej poprawności".
- Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Na gruncie UODO była to tzw. zasada ograniczenia czasowego.

W praktyce oznaczała konieczność usunięcia danych po ustaniu okresu ich przydatności np. zniszczenie otrzymywanych w procesie rekrutacji CV po określonym czasie. Jeżeli chodzi o CV brak jest unormowań ustawowych określających termin przydatności danych więc to Administrator musi określić maksymalny okres przetwarzania tego typu danych. W praktyce Administratorzy stosują okres 3 do 6 miesięcy. Z kolei jeżeli chodzi o przetwarzanie danych osobowych pracowników to Administrator zobowiązany jest do przechowywania akt osobowych pracownika przez okres 50 lat od daty ustania stosunku pracy (Dz.U. 1996, nr 62, poz. 286).

RODO znosi obowiązujący dotychczas sztywny model ochrony danych osobowych oparty na konieczności opracowania dokumentacji wg narzuconego schematu. Rozporządzenie z roku 2004 wskazywało na konieczność posiadania odpowiedniej dokumentacji, która opisywała reguły, zasady przetwarzania danych osobowych. Były to Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym (§ 4 Rozporządzenia). Pierwszy dokument, tj. Polityka (PB) zawierać musiała m.in.:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- sposób przepływu danych pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Drugi dokument, tj. Instrukcja Zarządzania Systemem Informatycznym (IZSI) zawierała m.in.:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Obecnie, punktem wyjścia do opracowania optymalnego systemu ochrony danych osobowych jest wspomniana powyżej analiza ryzyka, która powinna odpowiedzieć na podstawowe pytania: co i jak powinniśmy chronić. W poniższej tabeli wskazano

najistotniejsze obszary, których identyfikacja niezbędna jest do przeprowadzenia poprawnej analizy ryzyka.

Tabela 2.
Kluczowe obszary RODO

Analiza ryzyka	Dostosowanie środków technicznych i IT
• określenie punktu wyjścia dla wdrożenia zabezpieczeń zgodnych z RODO, • zdefiniowanie procesów zachodzących w organizacji, • zidentyfikowanie zagrożeń, podatności, prawdopodobieństwa, skutków i obecnych zabezpieczeń, • opracowanie planu postępowania z ryzykiem.	• określenie jakie środki techniczne przy uwzględnieniu oszacowanego ryzyka będą odpowiednie, • określenie jakie środki IT przy uwzględnieniu oszacowanego ryzyka będą spełniały wymogi RODO, • ocena adekwatności zastosowanych zabezpieczeń, • stworzenie procedury m.in.: szyfrowania danych osobowych i pseudonimizacji, zapewnienia ciągłości działania, regularnego testowania zastosowanych środków.

Źródło: http://gfx-consulting.pl/rodo-obsluga-firm.html.

4. Podsumowanie

Celem artykułu było przeanalizowanie stanu prawnego wprowadzonego przepisami ustawy o ochronie danych osobowych z roku 1997 w stosunku do wprowadzonych zmian wynikających z RODO. W związku z uchyleniem Rozporządzenia z 2004 roku pojawia się pytanie – co w zamian? Jakie dokumenty musi posiadać każdy Administrator? Czy w ogóle musi posiadać jakieś dokumenty? Jak sama nazwa wskazuje RODO ma charakter „ogólny". Wskazówkę dotyczącą dokumentacji możemy znaleźć tylko i wyłącznie w art. 24, ust. 2 RODO „Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez Administratora odpowiednich polityk ochrony danych". Z zacytowanej treści wynika wprost, że to Administrator podejmuje decyzję o opracowaniu i wdrożeniu odpowiedniej dokumentacji. Czy jednak w obecnej sytuacji Administrator może pozwolić sobie na brak dokumentacji opisującej zasady przetwarzania danych? Raczej nie. Zatem w jaki sposób Administrator powinien udokumentować prowadzone przez siebie działania? Przede wszystkim powinien rozpocząć od wspomnianej już powyżej analizy ryzyka. Aby jednak przeprowadzić prawidłowo analizę ryzyka należy zidentyfikować jakie dane są przetwarzane – niezbędnym narzędziem do tego procesu jest Rejestr Czynności przetwarzania, który zgodnie z wytycznymi RODO, stanowi narzędzie do inwentaryzacji posiadanych zbiorów.

Analiza ryzyka powinna stanowić oddzielny dokument, w którym zespół powołany przez Administratora określi możliwe ryzyka związane z przetwarzaniem danych osobowych. Członkami zespołu powinny być osoby, które znają podstawowe zasady przetwarzania danych osobowych, dobrze, aby posiadały także ukończone kursy w tej dziedzinie.

Członkiem tego zespołu bez wątpienia powinien być także informatyk, który najlepiej zna zagrożenia związane z przetwarzaniem danych w sieci oraz zna możliwości obrony przed tymi zagrożeniami. Całość prac zespołu powinien koordynować Inspektor Ochrony Danych Osobowych, który zastąpił dotychczasowego Administratora Bezpieczeństwa Informacji lub, w przypadku braku jego powołania, osoba odpowiedzialna z ramienia Administratora za system ochrony danych osobowych danego podmiotu. Oczywiście do prac zespołu mogą być także zaproszone inne osoby np. kierownicy poszczególnych działów, którzy będą nieocenionym źródłem informacji o praktycznych sposobach przetwarzania danych a także możliwych zagrożeniach z tym związanych.

Dopiero po przeprowadzonej szczegółowej analizie Administrator, a raczej zespół osób wskazanych przez niego, jest w stanie rozpocząć budowanie systemu ochrony danych osobowych obejmującego wszystkie czynności związane z przetwarzaniem danych począwszy od ich zbierania, poprzez właściwe przetwarzanie, po archiwizację a na końcu zniszczenie danych niezależnie od sposobu ich przetwarzania.

Bibliografia

1. Barta, J., Fajgielski, P., i Markiewicz, R. (2007). *Ochrona danych osobowych, komentarz*. Warszawa: Wolters Kluwer Polska Sp. z o.o.
2. Barta, P., i Litwiński, P. (2009). *Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: C.H. Beck.
3. Błotny, M. (2017). *Prawo do ochrony danych osobowych w Konstytucji RP na tle prawa Unii Europejskiej oraz orzeczenia Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/114 Schrems v. Data Protection Commissioner*. Poznań: Wydział Prawa i Administracji Uniwersytetu im. Adama Mickiewicza.
4. Generalny Inspektor Ochrony Danych Osobowych. *Wytyczne dotyczące inspektorów ochrony danych (WP 243, rew. 01)*. Warszawa: GIODO, https://giodo.gov.pl/pl/1520296/10056, 19.05.2018.
5. Generalny Inspektor Ochrony Danych Osobowych. *Opinia 15/2011 w sprawie definicji zgody (WP 187)*. Warszawa: GIODO, https://giodo.gov.pl/pl/1520110/4214, 20.05.2018.
6. GFX – Consulting, Czy jesteś gotowy na RODO, *http://gfx-consulting.pl/rodo-obsluga-firm.html* [dostęp online: 21.05.2018].
7. Gresel, J. (2018). Obowiązki organizacji pozarządowych jako administratorów danych osobowych w świetle RODO. *Trzeci Sektor, 2*.
8. Grzelak, A. (2017). Główne cele ogólnego rozporządzenia o ochronie danych osobowych. W M. Kawecki, i T. Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*. Warszawa: Beck.

9. Kloc, K., i Gawroński, M. (2018). Zgodność podstawowa. W M. Gawroński (red.), *RODO przewodnik ze wzorami*. Warszawa: Wydawnictwo Wolters Kluwer.
10. Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483).
11. PWC Polska. *10 najważniejszych zmian, które wprowadza RODO*, https://www.pwc.pl/pl/artykuly/2017/10-najwazniejszych-zmian-ktore-wprowadza-rodo.html, 21.05.2018.
12. *Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika*. Dz.U. 1996, nr 62, poz. 286.
13. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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).
14. *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 sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*.
15. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz.U. 2016, poz. 922).
16. *Ustawa z dnia 25 maja 2018 r. o ochronie danych osobowych* (Dz.U. 2018, poz. 1000).