GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Jak rozumieć podejście oparte na ryzyku?

Poradnik RODO
Podejście oparte na ryzyku
Część 1.

przygotowujemy do RODO 25.05.2018

grudzień 2017

Poradnik przygotowali pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych:

dr inż. Andrzej Kaczmarek - dyrektor Departamentu Informatyki,

Monika Młotkiewicz - zastępca dyrektora Departamentu Rejestracji,

Agnieszka Łapińska - specjalista w Departamencie Rejestracji,

Agata Miłocha - specjalista w Departamencie Rejestracji,

Michał Mazur - informatyk w Departamencie Informatyki.

Konsultacja naukowa:

dr hab. n. ekon. inż. Janusz Zawiła-Niedźwiecki, prof. Politechniki Warszawskiej.

SPIS TREŚCI

1. Wprowadzenie

Niniejszy poradnik podzielony został na dwie części.

W pierwszej, zatytułowanej *Jak rozumieć podejście oparte na ryzyku według RODO?,* wyjaśniamy istotę zasady podejścia opartego na ryzyku oraz wskazujemy, do czego zasada ta zobowiązuje podmioty stosujące przepisy ogólnego rozporządzenia o ochronie danych, zwanego dalej również „RODO”[1]. Wyjaśniamy też, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą. Wskazujemy, że szacowanie ryzyka to ciągły proces, który powinien być przeprowadzany w oparciu o konkretną metodę. Przedstawiamy przykładowe metody, z których można czerpać inspiracje dla tworzenia własnych metod oceny ryzyka.

W drugiej części, zatytułowanej *Jak stosować podejście oparte na ryzyku?,* proponujemy kolejne etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka (tzw. oceny skutków dla ochrony danych).

2. Do czego zobowiązuje podejście oparte na ryzyku?

Zasada podejścia opartego na ryzyku (*risk based approach*) jest ważną, perspektywiczną koncepcją, stanowiącą trzon ogólnego rozporządzenia o ochronie danych. Zasada ta uzależnia sposób realizacji obowiązków nałożonych na administratora od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów administratora. Wartościami, na jakie RODO kładzie szczególny nacisk w zakresie szacowania ryzyka, są zatem prawa i wolności osób, których dane dotyczą i te wartości należy mieć przede wszystkim na uwadze, oceniając ryzyko związane z przetwarzaniem danych osobowych. Zgodnie z motywem 2 preambuły RODO, zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Prawo to jest bowiem prawem podstawowym gwarantowanym art. 8 Karty Praw Podstawowych i musi być respektowane w przypadku prowadzania każdej bez wyjątku operacji przetwarzania danych.

Zasada podejścia opartego na ryzyku oznacza, że administratorom i podmiotom przetwarzającym nie wskazuje się ściśle określonych środków i procedur w zakresie bezpieczeństwa, np. kontroli dostępu, szyfrowania, rozliczalności czy sposobu monitorowania procesów przetwarzania. Zamiast tego zobowiązuje się ich do samodzielnego przeprowadzania szczegółowej analizy prowadzonych procesów przetwarzania danych i dokonywania samodzielnej oceny ryzyka, na jakie przetwarzanie danych w konkretnym przypadku jest narażone. Takie podejście umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka, przy jednoczesnym zachowaniu odpowiedniego poziomu ochrony, gdy to ryzyko jest niskie i nie wymaga całego instrumentarium środków przewidzianych przez rozporządzenie ogólne o ochronie danych. Przykładowo zatem inne środki ochrony powinny być podjęte w przypadku przetwarzania danych przez sklep prowadzący

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) http://www.giodo.gov.pl/pl/1520284/9745.

sprzedaż internetową, a inne przez sklep prowadzący sprzedaż wyłącznie w lokalu, który nie przetwarza danych swoich klientów przy użyciu systemów teleinformatycznych wykorzystujących sieć Internet.

Zasada podejścia opartego na ryzyku zobowiązuje do:

- Respektowania tego, że RODO szczególny nacisk kładzie na ochronę praw i wolności osób, których dane są przetwarzane.
- Dostosowania środków ochrony przetwarzania danych osobowych do skali ryzyka. Ocenia się je pod kątem utraty poufności, integralności i dostępności danych, biorąc przy tym pod uwagę ich zakres, szczególne znaczenie (wrażliwość) oraz kontekst i cele przetwarzania, a tym samym także kwestie zapewniania bezpieczeństwa usług przetwarzania (niezawodność, integralność i dostępność systemu przetwarzania) oraz zapewniania autentyczności i rozliczalności danych i podmiotów uczestniczących w przetwarzaniu.
- Koncentrowania się na poszukiwaniu środków redukujących prawdopodobieństwo wystąpienia zagrożeń najbardziej dotkliwych oraz środków redukujących skutki ich wystąpienia.

3. Podejście oparte na ryzyku nie jest nowością

Przyjęcie w RODO podejścia opartego na ryzyku ma na celu zapewnienie skutecznego przestrzegania przepisów poprzez zapewnienie administratorom większej „elastyczności" w doborze metod przetwarzania i środków zapewniania bezpieczeństwa danych osobowych. Niemniej model ochrony danych osobowych oparty na założeniu, że przyjmowane przez administratorów środki powinny być dostosowane do zagrożeń i charakteru przetwarzanych danych nie jest nowością. Podejście takie opiera się na dotychczasowym, blisko czterdziestoletnim dorobku legislacyjnym i orzeczniczym rozwijanym w Europie. Art. 17 ust. 1 dyrektywy 95/46 wskazuje przykładowe zagrożenia, które mogą wystąpić podczas operacji przetwarzania danych osobowych oraz wymaga przyjęcia takich zabezpieczeń, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń, mogących wystąpić podczas przetwarzania danych, oraz odpowiednich do charakteru danych objętych ochroną[2]. W Polsce obowiązek przeprowadzenia oceny ryzyka oraz właściwego dobrania środków technicznych i organizacyjnych odpowiedniego do zagrożeń oraz kategorii danych objętych ochroną wynika z art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922).

RODO ugruntowuje dotychczasowy dorobek, z jednej strony koncentrując się na podstawowych, obowiązujących już zasadach ochrony danych osobowych (takich jak: zgodność z prawem, rzetelność, przejrzystość, ograniczenie zakresu danych do celu ich przetwarzania, prawidłowość), z drugiej - dążąc do ich przeniesienia na poziom praktycznych rozwiązań. Realne przestrzeganie zasad ochrony danych osobowych ma być zapewnione przez wymóg indywidualnego dobierania przez administratorów odpowiednich w ich przypadku środków technicznych i organizacyjnych. Temu celowi służyć mają również takie instrumenty, jak: podejście oparte na ryzyku, zasada rozliczalności (art. 5 ust. 2 RODO), uwzględnianie ochrony danych w fazie projektowania czy domyślna ochrona danych (art. 25 RODO). W skutecznej realizacji zasad ochrony danych

[2] Art. 17 ust. 1 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: *„Państwa Członkowskie zapewniają, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania. Uwzględniając stan wiedzy w tej dziedzinie oraz koszt realizacji, przyjęte zostaną takie środki, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną*."

pomocne mogą być również mechanizmy przyjmowane dobrowolnie przez administratorów danych, takie jak: kodeksy postępowania czy certyfikacja (art. 40 – 43 RODO).

- Zasada podejścia opartego na ryzyku nie jest nowością.
- Przyjęcie tej zasady w przepisach RODO ma na celu zapewnienie ochrony przetwarzanym danym osobowym w sposób racjonalny (im większe ryzyko naruszenia praw i wolności – tym bardziej zaawansowane środki ochrony).

4. Jak rozumieć ryzyko naruszenia praw lub wolności osób, których dane są przetwarzane?

W ogólnym rozporządzeniu o ochronie danych pojęcie „ryzyka" nie zostało wprost zdefiniowane. Istotne jest jednak to, że pojęcia tego używa się w odniesieniu do naruszenia praw i wolności osób fizycznych, których dane dotyczą.

Mówiąc o ryzyku naruszenia praw i wolności osób fizycznych na gruncie RODO, konieczne jest uwzględnienie:

1) prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem, oraz
2) powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą[3].

RODO w motywie 76 wskazuje, że:

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić przez odniesienie się do **charakteru, zakresu, kontekstu i celów przetwarzania danych.** Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

O ryzyku lub wysokim ryzyku mowa jest również w wielu innych motywach preambuły RODO (np. motywie 76, 77, 84, 86, 89) oraz jego przepisach (np. art. 34, 35, 36). W motywie 76, 77 i 83 użyto również określeń związanych z „minimalizowaniem" i „szacowaniem" ryzyka (*„ryzyko należy oszacować na podstawie obiektywnej oceny", „najlepsze praktyki pozwalające zminimalizować ryzyko", „administrator i podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko"*), co oznacza, że ryzyko jest pewnego rodzaju miarą wspomnianego naruszenia praw i wolności osób fizycznych. W RODO operuje się w odniesieniu do tego pojęcia niewielką skalą. Jest to miara jakościowa (wskaźnikowa), w której występują następujące wartości: brak ryzyka, ryzyko, poważne ryzyko oraz wysokie ryzyko. Ponadto w wielu przepisach RODO (np. art. 30 ust. 5, art. 32, art. 34) w odniesieniu do skali naruszenia praw i wolności osób fizycznych używa się wyłącznie pojęcia „ryzyka", co oznacza, że szacując poziom ryzyka, należy uwzględnić wymienione wcześniej parametry zdarzenia powodującego naruszenie praw i wolności osoby fizycznej, tj. zarówno prawdopodobieństwo jego wystąpienia, jak i jego powagę (czyli niepożądane skutki/szkodę, jakie spowoduje jego wystąpienie).
Z powyższego wynika, że używane w RODO pojęcie ryzyka można utożsamiać z „ryzykiem" zdefiniowanym w normie ISO/IEC 27005:2011 jako „wpływ niepewności na cele". Oznacza to, że ryzyko jest czymś negatywnym, co może niekorzystnie wpłynąć na osiągnięcie celu przez wywołanie niepożądanych skutków ubocznych, a w

[3] Patrz motyw 75 preambuły RODO.

skrajnym przypadku niezrealizowanie celu przetwarzania. Na przykład: dla prawidłowego wykonania usługi transmisji danych niekorzystnym skutkiem ubocznym może być ujawnienie treści przekazywanych informacji nieuprawnionym osobom, nieuprawniona zmiana przekazywanych informacji, a nawet niewykonanie usługi, tj. niedostarczenie danych do wskazanego adresata. We wskazanej wyżej normie wyjaśnia się ponadto, że ryzyko w bezpieczeństwie informacji jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów, powodując w ten sposób szkodę dla organizacji. Ryzyko to jest często wyrażane jako kombinacja dwóch czynników: następstw zdarzenia bezpieczeństwa informacji i prawdopodobieństwa wystąpienia tego zdarzenia.

W RODO, jak już wspomniano, pojęcie ryzyka odnosi się do naruszenia praw i wolności osób, których dane są przetwarzane. W większości przypadków jednak do naruszenia takiego dochodzi właśnie na skutek naruszenia aktywów, jakimi są przetwarzane przez administratora lub przetwarzającego dane osobowe. W ogólnym rozporządzeniu o ochronie danych - podobnie jak w ww. normie - do określonego ryzyka przypisuje się pewne miary jakościowe, klasyfikujące jego wartość. Miarą taką mogą być np. przymiotniki : znikome, niskie, średnie, wysokie i bardzo wysokie lub liczby całkowite w określonej skali, np. od 0 do 4, odpowiadające wymienionym przymiotnikom.

Ponadto trzeba zauważyć, że urzeczywistnienie się określonego zagrożenia może nie spowodować skutków dla praw i wolności osób, których dane są przetwarzane, spowodować znikome skutki lub skutki katastrofalne. W skrajnych przypadkach, np. w systemach przetwarzania informacji medycznej, nieuprawniona modyfikacja danych lub niedostępność danych w wyniku złego ich zabezpieczenia może skutkować utratą zdrowia, a nawet życia. Dlatego oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, osoby odpowiedzialne za przeprowadzenie tego procesu powinny przyjąć perspektywę osób, których dane są przetwarzane i właśnie z tej perspektywy oceniać stopień dotkliwości w przypadku zmaterializowania się zagrożenia.

W procesach przetwarzania danych osobowych do naruszenia ww. praw i wolności dochodzi najczęściej w wyniku nieprawidłowo skonstruowanych procedur przetwarzania, w tym niewłaściwego (niezgodnego z celem) ich wykorzystania oraz niewłaściwego ich zabezpieczenia (niewłaściwej ochrony przed dostępem osób nieuprawnionych). Częstymi przyczynami naruszeń są też nieodpowiednie zarządzanie uprawnieniami do ich przetwarzania (dostępu do danych) oraz wszelkiego rodzaju zdarzenia losowe lub celowe, w wyniku których dochodzi do nieuprawnionego ujawnienia, zniszczenia, utraty bądź nieuprawnionej modyfikacji danych osobowych. Kolejne przyczyny takich zdarzeń to zaniechanie pełnego działania określonego procedurami czy nieprzestrzeganie przyjętych dobrych praktyk, np. w wyniku rutyny. Skutki każdego z wymienionych wyżej zdarzeń mogą w sposób bezpośredni lub pośredni wpływać na naruszenie praw i wolności osób, których dane są przetwarzane.

Wobec powyższego organizacja przetwarzająca dane osobowe powinna opracować i wdrożyć odpowiednie procedury zapewniające ochronę danych osobowych. Każdy pracownik danej organizacji powinien zostać przeszkolony i dobrze znać swoje zadania w zakresie ochrony danych osobowych. Tylko świadomi swoich obowiązków pracownicy będą mogli prawidłowo stosować obowiązujące ich procedury.

Przykłady sytuacji, w których dochodzi do naruszenia praw i wolności osób, których dane są przetwarzane

Przykład 1. W wyniku włamania na niewystarczająco zabezpieczony serwer poczty elektronicznej korespondencja prywatna użytkownika X z osobą Y została pozyskana przez osobę Z, która wykorzystała zdobyte informacje do czerpania korzyści finansowych, szantażując adresata i nadawcę wiadomości upublicznieniem informacji – *naruszenie prawa do ochrony danych osobowych, prawa do prywatności oraz wolności i prawa do tajemnicy komunikowania się.*

Przykład 2. W wyniku słabo zabezpieczonej ciągłości działania systemu bankowego użytkownik X na skutek niedostępności tego systemu nie mógł dokonać transakcji finansowej na giełdzie w określonym czasie – *naruszenie prawa do ochrony danych osobowych oraz prawa własności.*

Przykład 3. Firma ubezpieczeniowa X w wyniku nabycia informacji o rodzajach kupowanych przez swoich klientów produktów żywnościowych w jednej z sieci supermarketów dokonała analizy tych danych i podniosła składkę ubezpieczenia dla osób, z których profilu można było wywnioskować nieprawidłowe odżywianie się – *naruszenie prawa do prywatności, prawa do ochrony danych osobowych, w tym prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu*.

5. Szacowanie ryzyka to proces

Zgodnie z motywem 76 RODO, ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, należy określić przez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko. Ogólne rozporządzenie o ochronie danych nie odnosi się wprost do procesu zarządzania ryzykiem. Niewątpliwie jednak jednym ze skutecznych, systemowych sposobów przeprowadzania takiej oceny jest wdrożenie procesu zarządzania ryzykiem w danej jednostce. Dla części administratorów stanowić to będzie prawdziwe wyzwanie, ponieważ dotychczas wielu z nich traktowało proces zarządzania ryzykiem jako dobrą, zalecaną praktykę, a nie jako prawny obowiązek i w związku z tym taki proces nie był przez nich prowadzony.

Proces zarządzania ryzykiem powinien być wpisany w proces zarządzania organizacją. Spełnienie tego warunku wymaga ustalenia wszystkich procesów zachodzących w organizacji (w tym dotyczących przetwarzania danych osobowych), uwarunkowań wewnętrznych i zewnętrznych dotyczących środowiska, w którym ona funkcjonuje. Kluczowym elementem w stosowaniu podejścia opartego na ryzyku jest przyjęcie przez organizację określonej systematyki i kolejności działań.

W dużych organizacjach o złożonej strukturze może być potrzebne wyznaczenie zespołu odpowiedzialnego za proces zarządzania ryzykiem. W skład zespołu zwykle powołuje się przewodniczącego (np. prezesa/wiceprezesa lub innego członka zarządu), koordynatora tego zespołu (menedżera ds. ryzyka), właścicieli procesów biznesowych oraz aktywów (np. dyrektorów departamentów), ekspertów dziedzinowych (np. ekspertów ds. bezpieczeństwa informacji, ekspertów ds. bezpieczeństwa fizycznego itp.), a następnie przypisuje się im określony zakres uprawnień i odpowiedzialności, czyli rolę w całym procesie.
Biorąc pod uwagę, że zarządzanie ryzykiem obejmuje wszystkie szczeble organizacji, a także to, że proces zarządzania ryzykiem powinien być częścią procesu zarządzania organizacją, osoby wybrane do zespołu powinny mieć odpowiednio wysokie umocowanie. W przypadku powołania zespołu istotne jest, aby ścieżka raportowania była określona w sposób jasny dla wszystkich członków. W sytuacji, kiedy proces zarządzania

ryzykiem realizuje jedna osoba, raporty oraz pojawiające się nieprawidłowości powinny być zgłaszane bezpośrednio najwyższemu kierownictwu administratora, np. członkom zarządu.

Kluczowym elementem w procesie zarządzania ryzykiem w organizacji jest też włączenie w ten proces wszystkich pracowników i ścisła współpraca z nimi. Pracownicy stanowią cenne źródło informacji, jeżeli chodzi o określanie źródeł ryzyka. Z tego powodu warto stworzyć dla nich efektywną ścieżkę służącą zgłaszaniu wszystkich zauważonych w tym zakresie problemów, w tym naruszeń, oraz propozycji rozwiązań. Muszą oni zostać poinformowani, komu i w jaki sposób mogą dokonać tego typu zgłoszenia oraz z kim mogą się w tej sprawie w razie wątpliwości kontaktować. Warto również (np. w formie ankiet) okresowo zwracać się do nich z prośbą o wskazanie zauważonych problemów. Pracownikom powinny być ponadto przedstawiane wnioski z analizy ryzyka oraz związane z tymi wnioskami rekomendacje.

Wdrożenie podejścia opartego na ryzyku jest w swojej istocie procesem ciągłym, wymagającym stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. Zasada podejścia opartego na ryzyku wymusza na administratorze danych i podmiocie przetwarzającym dbanie o odpowiednią ochronę na wszystkich etapach przetwarzania danych osobowych, tj. podczas całego cyklu życia informacji, od momentu zbierania danych aż do ich usunięcia. Innymi słowy konieczne jest wbudowanie zasad ochrony danych osobowych w każdy projekt zakładający przetwarzanie danych osobowych, a następnie zapewnienie odpowiedniej ochrony danych osobowych na każdym etapie procesu przetwarzania danych, zgodnie z zasadą uwzględniana ochrony danych w fazie projektowania (ang. *privacy by design*)[4]. Zasada *ta* wymaga, aby potrzeby w zakresie ochrony danych uwzględniane były w całym cyklu przetwarzania danych, tj. od momentu pojawienia się koncepcji systemu przetwarzania, przez budowę projektu, stworzenie systemu, następnie jego wdrożenie i eksploatację, kończąc na usunięciu danych. Oznacza to również, że skuteczność przyjętych środków powinna być regularnie monitorowana, zwłaszcza w przypadku większych, bardziej skomplikowanych lub obciążonych większym ryzykiem operacji przetwarzania danych.

- Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy.
- Szacowanie ryzyka należy traktować jako proces ciągły.
- Ochrona danych osobowych powinna być zapewniona na każdym etapie procesu przetwarzania danych i na każdym etapie powstawania systemu przetwarzania danych.
- Skuteczność wdrożonych środków ochrony powinna być monitorowana i doskonalona.

6. Jaką metodę szacowania ryzyka należy zastosować?

Istnieje wiele różnych metod szacowania ryzyka. Najogólniej dzielą się one na metody ilościowe i jakościowe. W odniesieniu do przetwarzania informacji najczęściej stosuje się metody wskaźnikowe ze względu na trudność określania i przypisania zdarzeniom występującym przy przetwarzaniu informacji precyzyjnych miar zarówno w zakresie prawdopodobieństwa wystąpienia, jak i wielkości skutków.

Uwzględnienie zarówno prawdopodobieństwa wystąpienia zdarzenia powodującego naruszenie bezpieczeństwa, jak i jego wagi, w wielu metodach dokonuje się przez wyrażenie poziomu ryzyka jako iloczynu prawdopodobieństwa wystąpienia zdarzenia oraz jego skutku, co pokazano poniżej na przykładzie

[4] Patrz art. 25 RODO.

metody zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w urzędach administracji rządowej w zakresie zagrożeń pochodzących z cyberprzestrzeni, rekomendowanej przez Komitet Rady Ministrów ds. Cyfryzacji w listopadzie 2015 r.[5]

Przykłady szacowania poziomu ryzyka w metodyce zarządzania ryzykiem cyberprzestrzeni:

$R_p = P \times (S_d + S_i + S_p)$

gdzie: R_p – poziom wyliczanego ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia z zakresu {0, 1, 2, 3, 4},

gdzie: 0 – zdarzenie nieprawdopodobne,
1 – zdarzenie prawie nieprawdopodobne,
2 – zdarzenie mało prawdopodobne,
3 – zdarzenie wysoce prawdopodobne,
4 – zdarzenie niemal pewne.

S_d, S_i, S_p – skutki zdarzenia odpowiednio w zakresie **d**ostępności informacji, **i**ntegralności oraz **p**oufności z zakresu {0, 1, 2, 3, 4},

gdzie: 0 – zdarzenie nie powoduje skutku (nie występuje),
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

Na gruncie RODO nie została wskazana jedna określona metodyka przeprowadzania procesu zarządzania ryzykiem. Obecnie znanych jest wiele metod, z których można czerpać inspirację i dobre przykłady dla tworzenia własnych rozwiązań. Wybór metody powinien odpowiadać specyfice danego podmiotu, uwzględniać zakres i cele przetwarzania oraz rodzaj danych, a także wielkość, strukturę oraz możliwości organizacyjne, techniczne i finansowe danej jednostki. Przykłady owych metod można znaleźć m.in. w normach ISO/IEC[6], dokumencie PIA Methodology CNIL June 2015[7] czy dokumentach ISACA[8]. Trzeba pamiętać, że wymienione dokumenty, poza normą *ISO/IEC 29134 Information technology Security techniques Guidelines for privacy impact assessment,* tworzone były przed RODO, niemniej powstawały na gruncie wieloletnich doświadczeń i najlepszych praktyk.

Ważne jest, aby wybrana metoda pozwalała na rzetelną i obiektywną ocenę. Administrator lub podmiot przetwarzający, niezależnie od wybranej metody (jednej spośród gotowych lub stworzonej samodzielnie na podstawie kilku dostępnych), powinien jednolicie w całej organizacji stosować zbiór pojęć. To ważne,

[5] Komitet Rady Ministrów ds. Cyfryzacji 12 listopada 2015 r. przyjął dokument „Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych" i rekomendował administracji rządowej stosowanie określonej w nim metodyki. http://krmc.mc.gov.pl/krm/tryb-obiegowy/rok-2015/pazdziernik-2015-r/3034,Ministerstwo-Administracji-i-Cyfryzacji.html

[6] Norma ISO/IEC 27005:2011 Technika Informatyczna Technika bezpieczeństwa Zarządzanie ryzykiem w bezpieczeństwie informacji – w zakresie dotyczącym analizy ryzyka oraz norma ISO/IEC 29134:2017 Information technology Security techniques Guidelines for privacy impact assessment – w zakresie dotyczącym oceny skutków dla ochrony danych osobowych

[7] https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

[8] Dokumenty dostępne pod adresem https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx. oraz http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-Risk-Assessment-Management-Using-COBIT-5.aspx, a także materiały szkoleniowe „Integrated Risk Management Essentials" oraz „Integrated Risk Management Essentials (Advanced Managerial)" dostępne odpłatnie online (https://www.isaca.org/bookstore/Pages/Risk-IT-and-Related.aspx)

ponieważ metody często różnią się zakresem pojęć w nich stosowanych, np. w normach z rodziny PN-ISO/IEC 27000 jest mowa o zagrożeniach, podczas gdy np. w PIA Methodology CNIL June 2015 są one określane jako źródła ryzyka.

- RODO nie wskazuje określonej metody prowadzenia procesu zarządzania ryzykiem.
- Znane są różne metody, z których można czerpać inspiracje dla tworzenia własnych metodyk.
- Ważne jest, aby zastosowana metodyka dawała rzetelną i obiektywną ocenę ryzyka.

7. Środki ochrony, jakie należy zapewnić przy przetwarzaniu danych osobowych

Artykuł 24 RODO nakłada na administratora obowiązek wdrożenia takich środków technicznych i organizacyjnych w zakresie ochrony danych, które będą uwzględniały charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw i wolności osób, których dane są przetwarzane. Środki te powinny uwzględniać różne prawdopodobieństwo i wagę każdego zidentyfikowanego zagrożenia, aby przetwarzanie odbywało się zgodnie z RODO. Realizacja wskazanego obowiązku oznacza wdrożenie środków i procedur, które zapewnią pełną transparentność operacji przetwarzania danych, tj. wykazanie, kto, kiedy i jakie działania wykonywał. Stosowanie powyższych zasad i środków powinno być tak wdrożone i udokumentowane, aby administrator danych lub przetwarzający mógł to wykazać. Obowiązek administratora danych lub podmiotu przetwarzającego w zakresie wykazania zgodności przetwarzania danych z przepisami ogólnego rozporządzania dotyczy zarówno postępowania przed organem nadzorczym, jak i przed podmiotem danych. Podkreśla to motyw 74 RODO, który przewiduje obowiązek wykazania skuteczności wdrożonych środków. Z powyższego wynika, że zasada podejścia opartego na ryzyku jest ściśle powiązana z drugą, niezwykle ważną zasadą bezpośrednio przyjętą w przepisach RODO: **zasadą rozliczalności** (art. 5 ust. 2 RODO).

- Uzależnienie środków ochrony przetwarzanych danych od poziomu ryzyka wymaga oszacowania ryzyka i zastosowania środków, które je wyeliminują lub zredukują do akceptowalnego poziomu, np. rezygnacja z usługi zdalnego dostępu do bazy danych osobowych.
- Zasada rozliczalności wymaga, aby proces szacowania ryzyka został przeprowadzony i udokumentowany – w celu wykazania, że ryzyko zostało oszacowane i wprowadzono odpowiednie środki ochrony.
- Zasada rozliczalności oznacza wdrożenie wewnętrznych środków (technicznych i organizacyjnych) zapewniających zgodność przetwarzania z RODO oraz pozostawania w gotowości do wykazania tej zgodności organowi nadzorczemu lub podmiotom, których dane są przetwarzane.

7.1. Minimalizowanie ryzyka naruszenia praw i wolności osób, których dane dotyczą, jako obowiązek administratorów i podmiotów przetwarzających

Przepisy RODO nie wskazują wymaganych w konkretnym przypadku środków czy rozwiązań, które należy zastosować w celu minimalizacji ryzyka naruszenia ochrony praw i wolności osób, których dane są przetwarzane. Jak już wspomniano, jednym z istotnych czynników naruszenia ochrony danych może być

niewłaściwe ich zabezpieczenie przed utratą poufności, zniszczeniem, utratą lub nieuprawnioną modyfikacją. Czynniki te mają szczególne znaczenie w przypadku wykorzystywania do przetwarzania danych nowych rozwiązań technologicznych, w tym rozwiązań niesprawdzonych pod względem podatności na nieuprawnione przejęcie, zniszczenie, modyfikację lub niezgodne z celem dodatkowe wykorzystanie przetwarzanych danych. W przypadku nowych technologii często zdarza się, że uzyskuje się lepsze niż w tradycyjnych systemach zabezpieczeń współczynniki bezpieczeństwa, ale ich specyfika może być źródłem słabości, które dla określonych przypadków mogą ograniczać ich zastosowanie.

Przykłady użycia danych biometrycznych do weryfikacji tożsamości i kontroli dostępu

Przykład 1.

- Technologia biometrycznej weryfikacji tożsamości wykorzystująca układ żył krwionośnych palca lub dłoni jest technologią charakteryzującą się bardzo dobrymi parametrami (bardzo mały współczynnik błędnego rozpoznania oraz bardzo mały współczynnik błędnego odrzucenia).
- Technologia ta nie zabezpieczy jednak dostępu do danych zapisanych na pozyskanym przy użyciu przemocy urządzeniu mobilnym, gdyż dostęp do tych danych przestępca może uzyskać przez użycie przemocą palca lub dłoni ofiary.

Przykład 2.

- Technologia biometrycznej weryfikacji tożsamości wykorzystująca rysy twarzy w połączeniu np. z obrazem tęczówki przy zastosowaniu wysokiej jakości sprzętu może charakteryzować się wysokimi wskaźnikami bezpieczeństwa.
- Technologia taka może być środkiem kontroli do strategicznych pomieszczeń banku, ale nie może być wykorzystana np. jako jedyna, do weryfikacji użytkownika w mobilnym systemie płatności elektronicznej, gdyż niezbędne do weryfikacji dane, nieuprawniony użytkownik może uzyskać bez wiedzy i woli weryfikowanej osoby.

Jak wynika z powyższych przykładów, nie jest możliwe wskazanie jednego wspólnego i wyczerpującego zestawu takich środków bezpieczeństwa, których można by było używać w każdym przypadku, gdyż w zależności od konkretnych okoliczności i warunków przetwarzania danych, różne może być prawdopodobieństwo i waga urzeczywistnienia się zagrożeń skutkujących naruszeniem praw i wolności osób fizycznych. Stąd:

- RODO nie wskazuje środków bezpieczeństwa, jakie należy stosować, aby zminimalizować ryzyko naruszenia praw i wolności do określonego poziomu.
- RODO wymaga stosowania środków zmniejszających lub minimalizujących ryzyko naruszenia praw i wolności odpowiednich do okoliczności i skali ryzyka.
- W przypadku wysokiego ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, RODO wymaga zastosowania środków, które ryzyko to skutecznie zmniejszą lub rezygnacji z tych operacji przetwarzania, które są głównym źródłem wysokiego ryzyka.

Dobór odpowiednich środków zapewniających zgodność z przepisami prawa, w tym zapewniających minimalizację ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, zgodnie z przyjętą w RODO koncepcją opartą na ryzyku, należy do administratorów i podmiotów przetwarzających.

7.2. Przykłady środków i działań minimalizujących ryzyko w RODO.

Do rozwiązań i działań, które mogą być wykorzystane w celu minimalizacji ryzyka naruszenia praw i wolności osób, których dane dotyczą, w kontekście zapewnienia bezpieczeństwa przetwarzanych danych przed utratą poufności, zniszczeniem, nieuprawnioną modyfikacją lub brakiem dostępności, w art. 32 ust. 1 RODO zaliczono:

a. pseudonimizację i szyfrowanie danych osobowych;
b. zarządzanie systemem w sposób zapewniający ciągłość poufności, integralności i dostępności przetwarzanych informacji;
c. zarządzanie systemem w sposób zapewniający zdolność do szybkiego przywrócenia dostępu do danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego;
d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Zgodnie z motywem 28 RODO, wskazane przykładowe środki techniczne i organizacyjne nie wykluczają zastosowania innych środków technicznych lub organizacyjnych, jeżeli byłyby one bardziej adekwatne do charakteru ryzyka (skutecznie minimalizowałyby ryzyko lub całkowicie je eliminowały).

Istotnym wsparciem w zakresie doboru odpowiednich do charakteru ryzyka środków i rozwiązań powinien być również kompetentny, dysponujący fachową wiedzą, inspektor ochrony danych. Jednym z podstawowych jego zadań jest bowiem doradzanie administratorowi i podmiotowi przetwarzającemu w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych tak, aby przetwarzanie danych w organizacji odbywało się zgodnie z prawem. Z tego też powodu inspektor ochrony danych powinien być włączany we wszystkie działania związane z przetwarzaniem danych osobowych przez administratora lub podmiot przetwarzający, w tym również w działania związane z dokonywaniem oceny ryzyka. Co również istotne, inspektor ochrony danych zobowiązany jest wykonywać swoje obowiązki z należytym uwzględnieniem ryzyka (art. 39 ust. 2 RODO).

- **RODO nie wskazuje konkretnych środków technicznych lub organizacyjnych**, które należy zastosować, aby wykazać zgodność z określonymi w nim wymaganiami.
- **Wybór środków bezpieczeństwa powinien być determinowany przez okoliczności i warunki przetwarzania danych** oraz prawdopodobieństwo i powagę zdarzeń, które mogą doprowadzić do naruszenia praw i wolności osób, których dane są przetwarzane.
- **Istotne wsparcie** w zakresie doboru odpowiednich do charakteru ryzyka środków i rozwiązań w zakresie zapewnienia zgodności z RODO **powinien zapewnić inspektor ochrony danych.** Dobrym źródłem wsparcia mogą być również rekomendacje audytu certyfikacyjnego ukierunkowanego na weryfikację zgodności z RODO.

7.3. Uwzględnianie stanu wiedzy technicznej

Zasada podejścia opartego na ryzyku stanowi, że administrator danych lub podmiot przetwarzający powinien zastosować takie środki bezpieczeństwa, które w danych okolicznościach przetwarzania minimalizują związane z tym przetwarzaniem ryzyko naruszenia praw i wolności. Jednocześnie art. 32 ust. 1 RODO wymaga, aby przy wyborze tych środków uwzględniać aktualny stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania.

RODO nie odwołuje się jednak do określonych technologii czy narzędzi, które mogą być wykorzystywane do przetwarzania danych, lecz ogólnie wskazuje na cele, jakie należy osiągnąć. Dzięki temu nawet w warunkach stałego rozwoju technologicznego, niezależnie od zastosowanej technologii, nie ma obawy, że wymogi stawiane administratorom staną się nieaktualne.

Wskazany jednak w art. 32 ust. 1 RODO warunek uwzględnienia stanu wiedzy technicznej wymaga, aby administratorzy i podmioty przetwarzające, którzy stosują nowe rozwiązania technologiczne, wdrażali również środki bezpieczeństwa adekwatne do ryzyka naruszenia ochrony danych, które rozwiązania te mogą spowodować. Warunek ten oznacza, że dla administratora, który zastosował nowe rozwiązania, nie będzie usprawiedliwieniem brak wiedzy w zakresie środków bezpieczeństwa, jakie można przy takim rozwiązaniu wykorzystać. Zwłaszcza jeśli środki takie będą rekomendowane przez producenta określonej technologii, normy międzynarodowe, dobre praktyki publikowane przez organizacje specjalizujące się w danej technologii lub stowarzyszenia zrzeszające audytorów i specjalistów w zakresie bezpieczeństwa.

- **RODO jest neutralne technologicznie.**
- Zasada podejścia opartego na ryzyku oraz stosowanie nowych rozwiązań technicznych wymaga od administratorów danych i podmiotów przetwarzających **uwzględniania aktualnego stanu wiedzy technicznej w zakresie środków i metod ochrony danych.**

8. Ocena ryzyka a kontekst, w jakim dane są przetwarzane

Zgodnie z motywem 75 oraz art. 24 ust. 1 i art. 32 ust. 1 RODO, w procesie szacowania ryzyka naruszenia ochrony danych osobowych oraz postępowania z tym ryzykiem należy uwzględniać wiele czynników. Wymieniane są tam między innymi takie elementy, jak waga zagrożeń, wynikająca z rodzaju skutku urzeczywistnienia się zagrożeń, np. uszczerbku fizycznego, dyskryminacji itp.
Proces, w którym należy dokonać analizy wyżej wymienionych czynników, w normie ISO/IEC 27005, odnoszącej się do analizy ryzyka w bezpieczeństwie informacji, nazywany jest ustanowieniem kontekstu, w ramach którego należy dokonać inwentaryzacji potencjalnych (wewnętrznych i zewnętrznych) zdarzeń mogących być źródłem ryzyka oraz określić kryteria oceny poziomu ryzyka i kryteria jego akceptacji.

Szacując poziom ryzyka, należy mieć na uwadze fakt, że środki zastosowane w celu zmniejszenia poziomu skutków dla jednego z czynników mogą jednocześnie powodować zwiększenie skutków dla innego. Np. zastosowanie środka zmniejszającego ryzyko utraty poufności może spowodować podniesienie ryzyka utraty dostępności, jeśli zastosowany środek jest podatny na awarie.

Stąd w procesie zarządzania ryzykiem należy brać pod uwagę wszelkie dokonywane zmiany oraz uwzględniać:

- wszystkie wymagane zasady przetwarzania określone w art. 5 RODO, w tym m.in.: przejrzystość, ograniczenie celu, minimalizację danych,
- zapewnienie respektowania poszczególnych uprawnień podmiotów danych (np. prawa dostępu do danych, prawa do sprostowania, prawa do usunięcia danych, prawa do przenoszenia danych),
- wprowadzenie odpowiednich procedur, środków bezpieczeństwa i dokumentacji,
- ustanowienie kontroli skuteczności wprowadzenia określonych rozwiązań.

Warto zaznaczyć, że na gruncie RODO niewywiązanie się z jednego z obowiązków, bardzo często wpływa na prawidłowość wykonania pozostałych. Tym samym zarówno podejście oparte na ryzyku, jak i zasada rozliczalności powinny w konsekwencji prowadzić do powstania kompleksowych programów zgodności.

- Obowiązki wynikające z RODO są ze sobą powiązane.
- Zmniejszenie podatności procesu przetwarzania wobec jednego z czynników ryzyka może powodować zwiększenie podatności wobec innych czynników ryzyka.
- Niewywiązanie się z jednego obowiązku może wpływać na prawidłowość wykonania pozostałych.
- W podejściu opartym na ryzyku istotnym elementem skuteczności ochrony jest właściwa i kompleksowa analiza kontekstu procesu przetwarzania i identyfikacja wszystkich potencjalnych źródeł ryzyka.
- Skuteczność wdrożonych środków ochrony powinna być monitorowana.

9. Wysokie ryzyko a ocena skutków dla ochrony danych

Zgodnie z art. 35 ust. 1 RODO, jeżeli 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, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Oznacza to, że przeprowadzenie oceny skutków dla ochrony danych jest wymagane zawsze wtedy, gdy:

1) poziom ryzyka określony został jako wysoki w wyniku jego szacowania przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania,
2) dany rodzaj przetwarzania został wskazany w przepisie prawa (np. art. 35 ust. 3 RODO),
3) dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy, zgodnie z art. 35 ust. 4 RODO.

Zgodnie z art. 35 ust. 4, organ nadzorczy będzie miał obowiązek opublikować wykaz rodzajów operacji, które wymagają przeprowadzenia takiej oceny. Wykazy takie organ nadzorczy przekazuje Europejskiej Radzie Ochrony Danych.

Trzeba pamiętać też o ust. 9 tego artykułu, wskazującym, że w stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą lub ich przedstawicieli (mogą to być np. związki zawodowe, organizacje broniące praw człowieka) w sprawie zamierzonego przetwarzania. Warto, aby administrator skorzystał z tej możliwości, bowiem to prawa i wolności tych osób mogą być zagrożone, a wprowadzenie tej praktyki przez administratora pozwoli mu realnie uwzględnić perspektywę osób, których dane przetwarza.

Biorąc pod uwagę wykaz czynności, jakie art. 35 ust. 7 RODO nakazuje wykonać w ramach przeprowadzania oceny skutków dla ochrony danych, należy uznać, że proces ten nie jest niczym innym, jak szczególnym rodzajem szacowania ryzyka, w którym baczną uwagę należy zwrócić na zastosowane środki minimalizacji ryzyka.

Posługując się schematem procesu zarządzania ryzykiem w zakresie zarządzania bezpieczeństwa informacji, określonym w normie ISO/IEC 27005, proces oceny skutków dla ochrony danych, o którym mowa w art. 35 RODO, można określić jako:

1) kolejną iterację procesu zarządzania ryzykiem w przypadku, gdy poziom ryzyka (przy aktualnie stosowanych środkach ochrony) oszacowany został jako wysoki,
2) pierwszą lub kolejną iterację procesu zarządzania ryzykiem w przypadku, gdy ocena dotyczy operacji przetwarzania wstępnie zakwalifikowanych do grupy procesów mogących stanowić wysokie ryzyko dla ochrony danych.

Stwierdzenie wysokiego poziomu ryzyka naruszenia praw i wolności osób, których dane są przetwarzane, wymaga przeprowadzenia oceny skutków dla ochrony danych, podczas której należy dodatkowo uwzględnić:

- czy operacja przetwarzania jest niezbędna,
- czy ingerencja w prywatność związana z przetwarzaniem tych danych jest proporcjonalna do celów przetwarzania.

RODO nie specyfikuje ani struktury, ani zawartości dokumentacji. Wymaga jednak, aby potwierdzała ona zgodność z RODO wszystkich procesów przetwarzania danych u administratora lub podmiotu przetwarzającego.

Warto podkreślić, że przy przeprowadzaniu oceny skutków dla ochrony danych ryzyko powinno być zbadane w szczególności pod kątem sprawdzenia, czy danego celu nie można osiągnąć w sposób mniej ingerujący w prywatność. Jako przykład wskazać można dodatkowe ograniczenie zakresu przetwarzanych danych lub przetwarzanie danych w sposób bardziej ograniczający prawdopodobieństwo naruszenia praw i wolności jednostki przez bezprawne wykorzystanie danych osobowych w innych celach.

10. Dotychczasowy dorobek a nowe podejście do ochrony danych

RODO wymusza ciągły, efektywny nadzór nad przetwarzaniem danych, tak aby przetwarzanie to nie naruszało w jakikolwiek sposób praw i wolności osób, których dane dotyczą. Bez odpowiedniego i solidnego przygotowania się do stosowania nowej regulacji niemożliwe będzie działanie zgodne RODO. Właśnie dlatego, w przejściowym okresie przygotowawczym (rozporządzenie ogólne weszło już w życie, a od 25 maja 2018 r. będzie stosowane i egzekwowane), administratorzy oraz podmioty przetwarzające powinni skupić się na weryfikacji stosowanych przez siebie procedur oraz wdrażaniu rozwiązań wymaganych przez nowe przepisy. Należy sobie uświadomić, że pojęcie „ryzyka naruszenia praw i wolności osoby, której dane dotyczą" różni się od pojęcia „ryzyka w bezpieczeństwie informacji". Niemniej dla podmiotów, które od lat rzetelnie

respektują przepisy o ochronie danych osobowych oraz wypracowały skuteczne systemy zarządzania ochroną danych osobowych, w tym metody szacowania ryzyka, wdrożenie nowej regulacji będzie znacznie łatwiejsze.

- RODO weszło już w życie, a od 25 maja 2018 r. będzie stosowane i egzekwowane.
- **Okres do 25 maja 2018 r. należy wykorzystać do solidnego przygotowania się do stosowania nowej regulacji.**
- Bez takiego przygotowania niemożliwe będzie działanie zgodne z RODO.

Jak zostało już wielokrotnie podkreślone, RODO nie określa sztywnych ram dotyczących sposobu zapewniania i wykazywania przestrzegania przepisów o ochronie danych osobowych. W przepisach tego aktu brak jest wyczerpującego i konkretnego wykazu zabezpieczeń danych osobowych, takich jak np. określona częstotliwość zmiany hasła bądź wdrożenie szczegółowo określonej dokumentacji przetwarzania danych osobowych. Rozporządzenie ogólne nie wskazuje też żadnej normy, rekomendacji czy metodyki postępowania, które mają mieć zastosowanie do każdego administratora lub podmiotu przetwarzającego. Nie oznacza to jednak, że RODO zwalnia administratorów danych i podmioty przetwarzające z obowiązku posiadania dokumentacji przetwarzania, takich jak np. wymagane obecnymi przepisami polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym. Dotychczasowa dokumentacja prowadzona przez administratora lub podmiot przetwarzający nie tracą całkowicie na znaczeniu po rozpoczęciu stosowania RODO. Mogą one stanowić doskonałą bazę do wdrażania nowej dokumentacji, zgodnie z nowymi wymaganiami.

W związku z tym, że na gruncie RODO dokumentacja nie musi odpowiadać sztywnym ramom, będzie ona mogła być lepiej dostosowana do potrzeb i specyfiki danego administratora lub podmiotu przetwarzającego, co wskazane podmioty powinny odbierać jako dużą zaletę tego rozwiązania. Nie można jednak pominąć, że tworzona dokumentacja powinna nie tylko potwierdzać minimalne wymagania niezbędne dla zapewnienia bezpieczeństwa, ale administrator lub podmiot przetwarzający powinien wykazać w niej, że zastosowane środki są adekwatne do ryzyka naruszenia praw lub wolności osób przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania. Ponadto art. 32 ust. 1 RODO stanowi, że przy określaniu środków bezpieczeństwa należy uwzględniać stan wiedzy technicznej, który w zakresie środków bezpieczeństwa dotyczących zapewnienia poufności, integralności i dostępności zawarty jest w normach międzynarodowych z rodziny ISO/IEC seria 27000, a w zakresie środków dotyczących ciągłości działania (dostępności do przetwarzanych danych) w normie ISO/IEC 22301. Informacje dotyczące stanu wiedzy technicznej w powyższym zakresie można znaleźć również w wielu innych opracowaniach, w tym w dobrych praktykach wydawanych przez stowarzyszenia zrzeszające ekspertów zajmujących się bezpieczeństwem informacji (takich jak ISSA, ISACA, IAA), a także w przewodnikach i zaleceniach producentów dostarczających produkty do zabezpieczenia informacji w sieciach i systemach teleinformatycznych.

- **Dotychczasowa, rzetelnie opracowana i wdrożona dokumentacja** przetwarzania danych **może stanowić bazę do wdrożenia nowej dokumentacji**, która w pełni spełniać będzie wymogi dotyczące wykazania zgodności procedur przetwarzania danych **z wymaganiami RODO**.
- **RODO nie specyfikuje ani struktury, ani zawartości dokumentacji.** Wymaga jednak, aby dokumentowała ona zgodność wszystkich procesów przetwarzania danych u administratora lub przetwarzającego z zawartymi w RODO wymaganiami.

Wyjaśnienie użytych terminów

- **Aktywa** - jest to wszystko, co ma wartość dla organizacji (administratora danych lub podmiotu przetwarzającego), np. dane osobowe.
- **Aktywa podstawowe** – są to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem organizacji (w tym dane osobowe).
- **Aktywa wspierające –** są to środki umożliwiające korzystanie z aktywów podstawowych. Przykładem aktywów wspierających jest sprzęt, oprogramowanie, sieć, pracownicy.
- **Anonimizacja –** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.
- **Grupa Robocza Art. 29 -** Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej, i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.
- **Identyfikowanie ryzyka** – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.
- **Kontekst** – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.
- **Kryteria akceptacji ryzyka** – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-2.
- **Kryteria oceny ryzyka** - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.
- **Naruszenie ochrony danych osobowych -** oznacza 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.
- **Ocena ryzyka** – jest to czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.
- **Operacja przetwarzania danych osobowych** - każda czynność wykonywana 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.

- **Podatność** - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

- **Proces przetwarzania danych osobowych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

- **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

- **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.

- **Ryzyko** – wpływ niepewności na cele. W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.

- **Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011)[9].

- **Właściciel aktywów –** jest to osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji.

- **Zabezpieczenie** - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

- **Zagrożenie** - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

[9] Podobna definicja znajduje się w publikacji sfinansowanej przez Narodowe Centrum Badań i Rozwoju w ramach projektu „Zintegrowany system budowy planów zarządzania kryzysowego w oparciu o nowoczesne technologie informatyczne" nr DOBR/0016/R/ID2/003 pod tytułem „Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk" pod redakcją bryg. dra inż. Dariusza Wróblewskiego.
W ramach procesu „szacowanie ryzyka" ujęto takie zadania, jak: ustalenie kontekstu, ocena ryzyka, postępowanie z ryzykiem oraz jego monitorowanie i przegląd. Inny dokument - norma PN-ISO 31000:2012, zamiast pojęciem „szacowania ryzyka", posługuje się pojęciem „oceny ryzyka", które obejmuje proces identyfikacji ryzyka, jego analizę i ewaluację.

Przydatne materiały

1. Komisja Nadzoru Finansowego, Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, stanowiąca załącznik do uchwały nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r., dostępna pod: https://www.knf.gov.pl/dla_rynku/fin_tech/platnosci_elektroniczne/wybrane_stanowiska_i_regulacje?articleId=55482&p_id=18

2. Opinia Grupy Roboczej Art. 29, 3/2010 w sprawie zasady rozliczalności (WP 173), dostępna pod: http://giodo.gov.pl/pl/1520057/3732

3. Opinia Grupy Roboczej Art. 29, 4/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych (WP 205), dostępna pod: http://giodo.gov.pl/pl/1520167/6567

4. Opinia Grupy Roboczej Art. 29, 7/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci (WP 209), dostępna pod: http://giodo.gov.pl/pl/1520167/7546

5. Opinia Grupy Roboczej Art. 29, 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (WP 180), dostępna pod: http://giodo.gov.pl/pl/1520110/4085

6. Opinie i wytyczne Grupy Roboczej Art. 29 dotyczące wdrożenia RODO: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

7. Privacy Impact Assessments - CNIL, dostępne pod: https://www.cnil.fr/fr/node/15798

8. Publikacje przygotowane przez ICO, dostępne pod: https://ico.org.uk/global/request-publications/

9. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dostępne pod: http://www.giodo.gov.pl/pl/1520284/9745

10. Rządowy Zespół Reagowania na Incydenty Komputerowe, dostępne pod: www.cert.gov.pl

11. Stanowisko Grupy Roboczej Art. 29 w sprawie podejścia opartego na ryzyku w ramach prawnych ochrony danych (WP 218), dostępne pod: http://giodo.gov.pl/pl/1520203/7936

12. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować wysokie ryzyko" do celów Rozporządzenia 679/2016 (WP 248), dostępne pod: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

13. Zarządzanie Ryzykiem – Przegląd Wybranych Metodyk; Praca pod redakcją bryg. dra inż. Dariusza Wróblewskiego wydanej przez Narodowe Centrum Badań i Rozwoju, Józefów 2015; ISBN 978-83-61520-18-4; https://www.cnbop.pl/wydawnictwa/ksiazki/zarzadzanie_ryzykiem.pdf"

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Biuro Generalnego Inspektora
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl