Michał Kwapisz[1], Adam Pelikant[2]

Zarządzanie zmianą w ujęciu RODO i oceny ryzyka

Streszczenie
Zarządzanie zmianami w systemach informatycznych jest jednym z najistotniejszych elementów inżynierii oprogramowania. Wprowadzenie w organizacji procesu zarządzania zmianami w systemach informatycznych daje możliwość reagowania na potrzeby biznesowe użytkowników końcowych korzystających z systemów informatycznych oraz sprawnego zarządzania zgłoszeniami zmian, przy jednoczesnym określeniu działań, jakie należy podjąć w trakcie ich analizy. Analiza funkcjonalna dostarcza wytyczne w zakresie implementacji oraz warunki wejściowe i wyjściowe do testów implementowanej zmiany w środowisku informatycznym. Wyniki analizy pozwalają oszacować czas potrzebny do wdrożenia zmiany i koszty, jakie zostaną poniesione na jej wykonanie. Dzięki testom można sprawdzić, w jakim stopniu zmiana wpłynęła na system informatyczny i sposób przetwarzania danych osobowych oraz czy jakość wykonania zmiany jest na założonym poziomie, określonym przez klienta. Artykuł ten opisuje proces zarządzania zmianą z uwzględnieniem wymagań RODO w zakresie analizy ryzyka.
Słowa kluczowe: zarządzanie zmianą, proces, inżynieria oprogramowania, RODO, zarządzanie ryzykiem, ocena ryzyka

1. Wprowadzenie

Zasadę *privacy by design* wprowadza art. 25 ust. 1 Rozporządzenia RODO[3], zgodnie z którym „uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia

[1] Politechnika Łódzka, Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki, Instytut Mechatroniki i Systemów Informatycznych, michal.l.kwapisz@gmail.com.
[2] Politechnika Łódzka, Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki, Instytut Mechatroniki i Systemów Informatycznych, adam.pelikant@p.lodz.pl.
[3] 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).

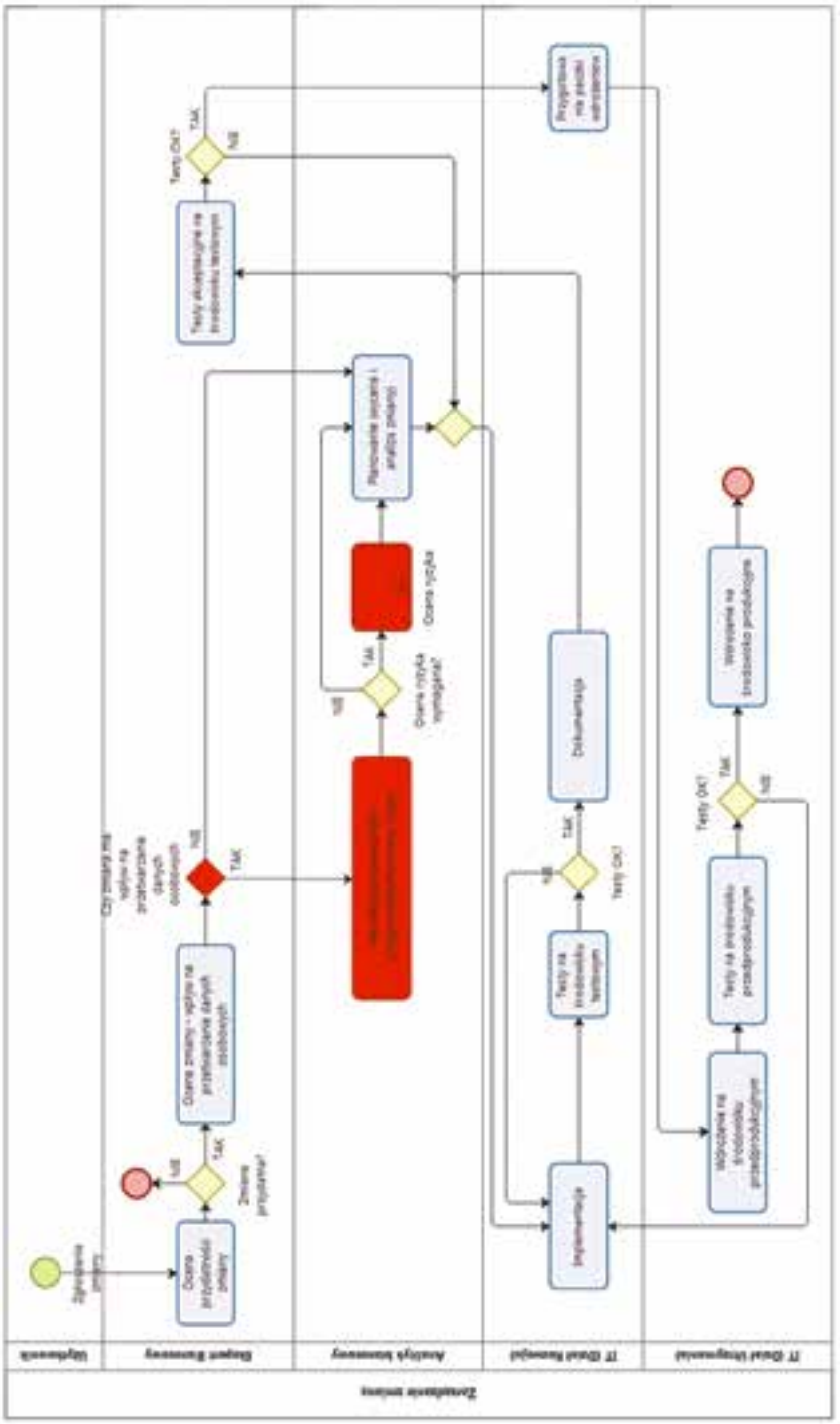
i wadze zagrożenia wynikające z przetwarzania, administrator danych osobowych – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą". Przepis ten wprowadza zasadę, na podstawie której administrator danych będzie zobowiązany zapewnić, aby już na etapie projektowania systemów informatycznych oraz na późniejszym etapie wykorzystywania go do przetwarzania danych osobowych, zostały zastosowane odpowiednie środki techniczne i organizacyjne, które zapewnią ochronę danych osób fizycznych i ich przetwarzanie zgodnie z rozporządzeniem RODO.

Zasadę *privacy by default* określa art. 25 ust. 2, zgodnie z którym administrator będzie zobowiązany wdrożyć takie środki techniczne i organizacyjne, aby domyślnie były przetwarzane wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Dotyczyć to będzie ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Zastosowane środki techniczne i organizacyjne powinny zapewniać w szczególności, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby, nieokreślonej liczbie osób fizycznych.

Oznacza to nic innego, jak konieczność wprowadzenia oceny ryzyka w procesie zarządzania zmianami i jego wpływu na przetwarzane dane osobowe w środowisku administratora. W artykule zostanie zaprezentowany i opisany przykładowy proces zarządzania zmianą z wplecionymi elementami oceny ryzyka dla realizowanych zmian. Należy mieć na uwadze, że zmiana w sposobie przetwarzania danych osobowych to nie tylko zmiany w istniejących już systemach informatycznych, ale również nowe wdrożenia informatyczne oraz przetwarzanie danych osobowych poza systemami informatycznymi (np. zmiana w sposobie archiwizacji dokumentów papierowych zawierających dane osobowe).

2. Proces zarządzania zmianą

Zarządzanie zmianami jest jednym z najistotniejszych elementów inżynierii oprogramowania. Wprowadzenie w organizacji procesu zarządzania zmianami w systemach informatycznych daje możliwość reagowania na potrzeby biznesowe



Rysunek 1. Proces zarządzania zmianami w systemach informatycznych
Źródło: opracowanie własne.

użytkowników końcowych korzystających z systemów informatycznych oraz pozwala na sprawne zarządzanie zgłoszeniami zmian, przy jednoczesnym określeniu działań, jakie należy podjąć w trakcie ich analizy[4]. Analiza funkcjonalna dostarcza wytyczne w zakresie implementacji oraz warunki wejściowe i wyjściowe do testów implementowanej zmiany w środowisku informatycznym. Wyniki analizy pozwalają oszacować czas potrzebny do wdrożenia zmiany i koszty, jakie zostaną poniesione na jej wykonanie[5]. Dzięki testom można sprawdzić, w jakim stopniu zmiana wpłynęła na system informatyczny i sposób przetwarzania danych osobowych oraz czy jakość wykonania zmiany jest na założonym poziomie, określonym przez klienta. Proces zarządzania zmianami w systemach informatycznych został przedstawiony na rysunku 1.

Zaproponowany w tym artykule proces zawiera pięć ról, które w zależności od złożoności organizacyjnej mogą być dalej dzielone (np. IT Dział Rozwoju na osobne role, takie jak Dział Dokumentacji, Dział Kontroli Jakości etc.) – tabele 1 i 2.

Tabela 1. Lista ról biorących udział w procesie zarządzania zmianami

Rola	Opis roli
Użytkownik	Dowolny pracownik lub współpracownik w organizacji, który realizuje procesy biznesowe z wykorzystaniem różnych systemów informatycznych. Założono, że inicjatywy zmian mogą pochodzić od pracowników najniższego szczebla organizacji, które następnie są poddawane weryfikacji przez ekspertów biznesowych odpowiedzialnych za poszczególne procesy
Ekspert biznesowy	Grupa osób odpowiedzialnych za poszczególne procesy biznesowe. Ich zadaniem jest wyłuskanie z grupy zgłoszeń tych zmian, które mają dodatni wpływ na optymalizację procesów
Analityk biznesowy	Analityk biznesowy jest odpowiedzialny za komunikację użytkowników biznesowych z technicznym światem IT. Zadaniem analityka biznesowego jest przetłumaczenie i/lub uszczegółowienie wymagań zarejestrowanych w zleceniu zmiany na język zrozumiały przez informatyków oraz dostarczenie dodatkowych wymagań pochodzących np. z oceny ryzyka. Dodatkowo w ramach prac analityka biznesowego jest realizowane planowanie wydań, ocena pracochłonności i kosztów poniesionych na etapie implementacji zmiany

[4] M.W. Bhatti, F. Hayat, N. Ehsan, A. Ishaque, A. Sohail, M. Ebtisam, *A Methodology to Manage the Changing Requirements of a Software Project*, 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM).

[5] V. Morozov, O. Kalnichenko, A. Timinsky, I. Liubyma, *Proactive Project Management for Development of Distributed Information Systems*, Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) 2017 4th International, s. 25–28.

Rola	Opis roli
IT (Dział Rozwoju)	Dział Rozwoju IT jest odpowiedzialny za wyprodukowanie zamówionej zmiany zgodnie z oczekiwaną jakością, założeniami, funkcjonalnościami, kosztami oraz zakładanym harmonogramem
IT (Dział Utrzymania)	Dział Utrzymania IT jest odpowiedzialny za wdrożenie zamówionej zmiany na środowisko produkcyjne w godzinach ograniczonej eksploatacji systemu (lub w wyznaczonym oknie serwisowym przewidzianym do tego typu prac). Po wdrożeniu zmiany Dział Utrzymania IT weryfikuje stabilności systemu po wprowadzeniu zmiany do systemu produkcyjnego (testy regresyjne). W przypadku braku stabilności systemu spowodowanymi błędami, które ujawniły się po wdrożeniu zmiany, należy zmianę wycofać i odtworzyć działającą konfigurację

Źródło: opracowanie własne.

Tabela 2. Opis ról biorących udział w procesie zarządzania zmianami

Rola	Realizowane zadania w procesie zarządzania zmianami
Użytkownik	Zgłoszenie zmiany do systemu
Ekspert biznesowy	Ocena przydatności zmiany – weryfikacja, czy zmiana jest uzasadniona lub czy daje wartość dodatnią dla optymalizacji poszczególnych procesów. Testy akceptacyjne na środowisku testowym – weryfikacja poprawności wytworzenia zmiany. Celem tego zadania jest ocena, czy dostarczone rozwiązanie działa zgodnie z oczekiwaniami i spełnia kryteria jakościowe założone na początku. Ocena zmiany (wpływ na przetwarzanie danych osobowych) – zadaniem eksperta biznesowego jest określenie, w jakim stopniu zgłoszona zmiana wpływa na przetwarzanie danych osobowych. Klasyfikację taką można zrealizować za pomocą ankiety, gdzie udzielenie choć jednej twierdzącej odpowiedzi, klasyfikuje zmianę oceny konieczności przeprowadzenia oceny ryzyka. Przykład pytań ankietowych: • Czy zmiana dotyczy elementów dostępnych poza systemami informatycznymi (wydruki/raporty/e-mail)? • Czy zmiana dotyczy danych osobowych (w szczególności: numer klienta/PESEL/dane adresowe/dane kontaktowe)? • Czy zmiana dotyczy zgód klienta lub procesów obsługi RODO (prawa osób fizycznych, których dane dotyczą)? • Czy zmiana dotyczy systemu udostępnionego do internetu? • Czy proponowana zmiana jest zmianą masową (dotyczy więcej niż 5% bazy klientów)?
Analityk biznesowy	Weryfikacja konieczności przeprowadzenia oceny ryzyka – w ramach tej czynności analityk biznesowy ma za zadanie zweryfikować, czy zamówiona zmiana oraz wyniki ankiety uzupełnionej przez eksperta biznesowego mogą skutkować zmianą wartości ryzyka. Jeśli na podstawie wyników ankiety można wnioskować, że dochodzi do zmiany wartości ryzyka przetwarzania danych osobowych, należy przeprowadzić pełną ocenę ryzyka oraz ocenę skutków dla ochrony danych.

cd. tabeli 2

Rola	Realizowane zadania w procesie zarządzania zmianami
	Wiedza, jaką dysponuje analityk biznesowy, pozwala mu na stwierdzenie, czy ocena ryzyka jest wymagana dla przeprowadzonej zmiany. Ocena ryzyka – podproces uruchamiany w przypadku, gdy dla zamówionej zmiany zachodzi konieczność przeprowadzenia analizy ryzyka. Szczegółowy opis metody oceny ryzyka został opisany w części niniejszego artykułu zatytułowanej *Ocena ryzyka w zarządzaniu zmianą*. Planowanie zmiany – w ramach tego zadania jest przeprowadzana analiza szczegółowa zmiany. Wynikiem analizy jest oszacowanie pracochłonności, budżetu, harmonogramu oraz dodefiniowanie wymagań zarejestrowanych w zleceniu. Jeśli, w skutek przeprowadzonej oceny ryzyka przetwarzania danych osobowych oraz oceny skutków dla ochrony danych, jest konieczne zrealizowanie szerszego zakresu prac niż opisany w zleceniu (minimalizacja ryzyka), należy odwzorować dodatkowe prace w czasochłonności, budżecie i harmonogramie prac wynikających ze zlecenia. W ramach tego kroku mogą być stosowane przeróżne metodyki rozwoju systemów informatycznych (np. metodyki zwinne i planowanie sprintów)
IT (Dział Rozwoju)	Implementacja – zadanie mające na celu wytworzenie zamówionej zmiany w oczekiwanym terminie i zgodnie z ustalonym budżetem. Testy na środowisku testowym – kontrola jakości wykonanej zmiany względem wymagań zarejestrowanych w zleceniu zmiany przed przekazaniem jej do udokumentowania. Dokumentacja – udokumentowanie wprowadzonej zmiany przed przekazaniem jej do testów akceptacyjnych. W ramach tego zadania powinna zostać stworzona lub uaktualniona dokumentacja, tj.: • instrukcja użytkownika końcowego, • instrukcja dla administratora, • dokumentacja wdrożeniowa, • dokumentacja systemu informatycznego, • analiza ryzyka dla zmiany (jeśli wymagana). Przygotowanie wdrożenia – przygotowanie paczki wdrożeniowej zawierającej zamawianą zmianę wraz z dokumentacją
IT (Dział Utrzymania)	Wdrożenie na środowisku przedprodukcyjnym. Testy na środowisku przedprodukcyjnym – testy zmiany na środowisku przedprodukcyjnym, których celem jest weryfikacja, czy wszystkie usługi dostarczane przez system informatyczny po wdrożeniu zmiany działają poprawnie. Zalecane jest stosowanie pełnych automatycznych testów regresyjnych. Wdrożenie na środowisko produkcyjne – uruchomienie zmiany na środowisku produkcyjnym i oddanie jej do użytkowników biznesowych

Źródło: opracowanie własne.

3. Ocena ryzyka w zarządzaniu zmianą z uwzględnieniem RODO

O konieczności przeprowadzenia oceny skutków dla ochrony danych osobowych mówi art. 35, którego treść brzmi następująco: „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. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę".

Zgodnie z art. 35 ust. 7 ocena ryzyka zawiera co najmniej:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1, oraz
- środki planowane w celu uniknięcia ryzyka, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.

Oczekiwany rezultat został opisany w art. 24 ust. 1, który brzmi: „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane".

3.1. Role i odpowiedzialność w procesie zarządzania ryzykiem według modelu RACI

Model RACI[6] opisuje role i kompetencje poszczególnych ról w procesie zarządzania ryzykiem ochrony danych osobowych (tabela 3).

Tabela 3. Lista ról w procesie oceny ryzka oraz ich odpowiedzialność

Krok	Etap	Rola					
		Administrator danych osobowych	Inspektor danych osobowych	Właściciel zasobów	Właściciel procesów	Organ nadzorczy	Eksperci
1	Określenie kontekstu przetwarzania	A	R	C	I		
2	Ocena, czy rodzaj operacji przetwarzania danych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych	A	R	C	I		
3	Ocena, czy rodzaj operacji przetwarzania danych jest zwolniony z przeprowadzenia oceny skutków dla danych osobowych	A	R				
4	Ocena konieczności i proporcjonalności przetwarzania danych	A	R	C	I	C	C
5	Ocena ryzyka naruszenia praw i wolności osób fizycznych	A	R	R	C	C	C
6	Ocena, czy ryzyko jest akceptowalne	A, R	R	I	C	C	C
7	Zarządzanie ryzykiem	A	R	R	C		C
8	Ocena, czy ryzyko szczątkowe jest akceptowalne	A, R	R	I	C	C	C
9	Informowanie o ryzyku lub/i przeprowadzenie konsultacji	A	R	R	R	R	R
10	Ocena, czy jest potrzeba przeprowadzenia oceny skutków dla ochrony danych osobowych	A, R					
11	Monitorowanie i przegląd ryzyka	A	R	R	R		

Źródło: Data Protection Impact Assessment (DPIA) FBI Polska.

[6] Data Protection Impact Assessment (DPIA) FBI Polska.

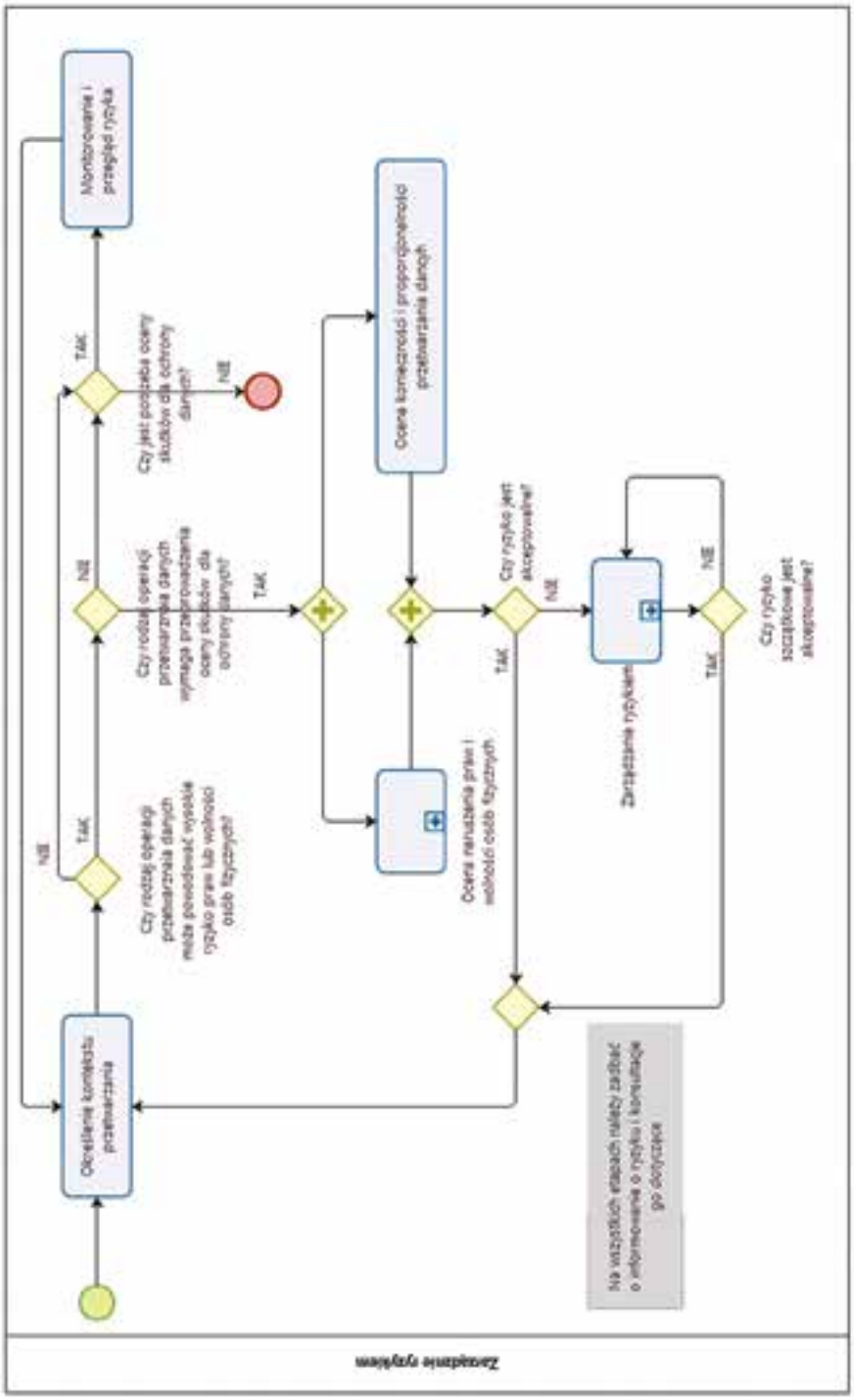
W modelu tym wyróżniamy następujące role:
- R (*responsible*) – rola odpowiedzialna za realizację zadań,
- A (*approver*) – rola zatwierdzająca realizację zadań pełniąca funkcję nadzorczą,
- C (*consultant*) – rola odpowiedzialna za konsultacje i doradztwo przy realizacji zadań,
- I (*informed*) – rola otrzymująca informacje o realizowanych zadaniach.

3.2. Proces zarządzania ryzykiem

Celem kontekstu przetwarzania danych jest określenie i udokumentowanie:
- charakteru przetwarzania danych osobowych,
- zakresu przetwarzania w stosunku do celów, w których dane osobowe są przetwarzane,
- kontekstu, w którym zebrano dane osobowe,
- celu przetwarzania danych osobowych,
- odbiorców i przetwarzających dane osobowe,
- okresu przechowywania danych osobowych,
- operacji przetwarzania danych osobowych,
- aktywów używanych w operacjach przetwarzania danych osobowych.

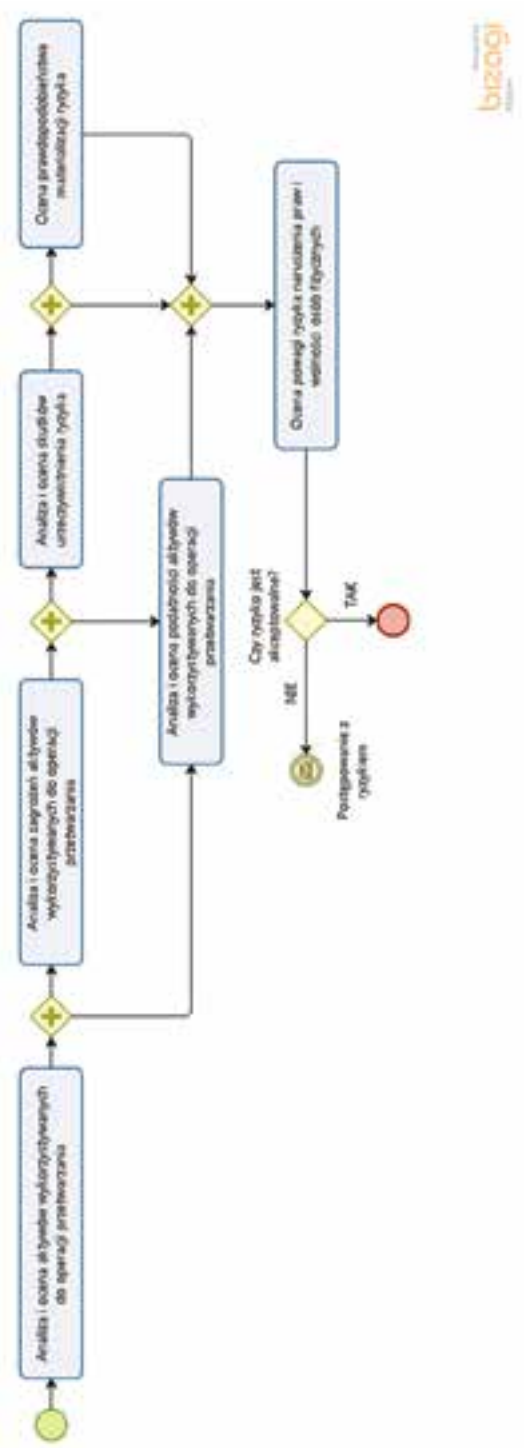
Przykłady rodzajów operacji przetwarzania danych mogących skutkować wzrostem ryzyka przetwarzania danych osobowych są następujące:
- ocena lub punktacja, w tym profilowanie i przewidywanie,
- automatyczne podejmowanie decyzji o skutku prawnym lub podobnym,
- systematyczne monitorowanie,
- dane osobowe wrażliwe,
- dane przetwarzane na dużą skalę,
- zestawy danych, które zostały dopasowane lub połączone,
- pozbawienie osób fizycznych przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
- innowacyjne wykorzystanie lub stosowanie rozwiązań technologicznych lub organizacyjnych,
- przesyłanie danych poza granice Unii Europejskiej,
- uniemożliwienie osobie fizycznej korzystania z prawa lub korzystania z usługi lub umowy.

Proces oceny ryzyka w ujęciu globalnym został przedstawiony na rysunku 2.



Rysunek 2. Proces oceny ryzyka (ujęcie globalne)

Źródło: opracowanie własne.



Rysunek 3. Proces oceny ryzyka naruszenia praw i wolności osób fizycznych
Źródło: opracowanie własne.

W celu oceny konieczności i proporcjonalności przetwarzania danych należy zweryfikować i udokumentować, czy:

- dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach,
- dane osobowe są przetwarzane zgodnie z obowiązującym prawem,
- dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
- został ograniczony czas przechowywania i przetwarzania danych osobowych,
- w przypadku zbierania danych osobowych są zapewnione odpowiednie środki, aby udzielić osobie, której dane dotyczą, wszelkich informacji,
- ograniczono liczbę odbiorców danych do niezbędnego minimum,
- ograniczono liczbę podmiotów przetwarzających dane osobowe (procesorów) do niezbędnego minimum,
- przeprowadzono konsultacje z organem nadzorującym.

Ocena ryzyka naruszenia praw i wolności osób fizycznych może zostać zdefiniowana przez proces przedstawiony na rysunku 3.

W ramach przetwarzania danych należy zidentyfikować i zinwentaryzować aktywa lub grupy aktywów wykorzystywane do realizacji operacji przetwarzania danych osobowych[7] (tabela 4).

Tabela 4. Kategorie aktywów

Aktywa	Opis
Procesy biznesowe	Seria powiązanych ze sobą działań lub zadań, które realizują operacje przetwarzania danych osobowych lub prowadzą do osiągnięcia celu przetwarzania danych
Personel	Wszystkie grupy osób zaangażowane w przetwarzanie danych, tj.: decydenci, użytkownicy, personel eksploatacji/utrzymania, twórcy oprogramowania
Sprzęt	Wszelkie urządzenia fizyczne w organizacji, tj.: urządzenia przenośne, stacjonarne, peryferyjne, nośniki danych
Lokalizacje	Wszelkie lokalizacje wykorzystywane do przetwarzania danych oraz środki fizyczne potrzebne do ich funkcjonowania, tj. siedziba, strefy bezpieczeństwa, usługi komunalne i techniczne
Oprogramowanie	Wszelkie programy wykorzystywane w operacjach przetwarzania danych, tj.: systemy operacyjne, aplikacje biznesowe, oprogramowania usługowe, utrzymaniowe lub administracyjne

[7] R. Heimes, *Global InfoSec and Breach Standards*, „IEEE Security & Privacy" 2016, Volume 14, Issue 5.

Aktywa	Opis
Sieć informatyczna	Wszystkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego, tj.: media i usługi wspierające, przekaźniki aktywne lub pasywne, interfejsy komunikacyjne
Organizacja	Wszystkie struktury ludzkie przypisane do przetwarzania danych osobowych oraz procedury sterujące tymi strukturami, tj.: organy władzy, struktura organizacji, podwykonawcy (procesorzy), dostawcy, producenci
Dane	Dane przetwarzanie w wersji elektronicznej lub papierowej

Dla zidentyfikowanych aktywów (grup aktywów) wykorzystywanych do operacji przetwarzania danych należy przypisać zagrożenia, które mogą mieć wpływ na naruszenie praw i wolności osób fizycznych (tabela 5). Zagrożenie należy rozumieć jako potencjalną przyczynę niepożądanego incydentu, która może wywołać naruszenie praw i wolności osób fizycznych.

Tabela 5. Tabela zagrożeń

Nazwa grupy	Zagrożenie
Zniszczenie fizyczne	Pożar – brak systemu przeciwpożarowego
	Zalanie
	Zniszczenie danych na nośnikach papierowych lub elektronicznych
Naruszenie praw i wolności osób fizycznych	Przypadkowe lub niezgodne z prawem zniszczenie danych osobowych
	Utracenie danych osobowych
	Nieuprawnione zmodyfikowanie danych osobowych
	Nieuprawnione ujawnienie danych osobowych
Naruszenie bezpieczeństwa informacji	Przechwycenie sygnałów na skutek zjawiska interferencji
	Szpiegostwo zdalne
	Kradzież nośników elektronicznych lub papierowych
	Manipulowanie urządzeniami
	Sfałszowanie oprogramowania
	Przejęcie uprawnień
Awarie urządzeń technicznych	Awaria urządzenia
	Błędne działanie urządzeń
	Błędy oprogramowania
Brak autoryzacji działań	Nieautoryzowane użycie urządzeń
	Nieuprawnione kopiowanie oprogramowania
	Użycie fałszywego lub nielegalnie skopiowanego oprogramowania

cd. tabeli 5

Nazwa grupy	Zagrożenie
Naruszenie bezpieczeństwa funkcji	Nielegalne przetwarzanie danych
Zagrożenia osobowe	Haker
	Sabotaż lub desperacja pracownika

Źródło: opracowanie własne.

Dla każdego zagrożenia zidentyfikowanego w ramach aktywów lub/i grupy aktywów wykorzystywanych do operacji przetwarzania danych należy przypisać podatności (tabele 6 i 7). Podatność należy rozumieć jako źródło zagrożenia, słabość lub lukę aktywów lub zabezpieczania, która może być wykorzystana do zmaterializowania się zagrożenia.

Tabela 6. Ocena możliwości wykorzystania podatności

Wartość	Nazwa	Opis
3	Bardzo podatne	Podatność występuje regularnie lub często w określonym roku
2	Podatne	Podatność ujawniła się w roku lub ujawnia się nieregularnie
1	Mało podatne	Podatność występuje nie częściej niż raz na 2–3 lata
0	Brak podatności	Nie odnotowano wystąpienia podatności

Źródło: opracowanie własne.

Tabela 7. Tabela podatności dla aktywów

Rodzaj aktywów	Podatność
Organizacja	Brak opracowanych, aktualizowanych lub testowanych planów ciągłości działania
	Brak dokumentacji wymaganej prawem
	Brak listy osób upoważnionych do dostępu do przetwarzania danych osobowych
	Niedostateczne procedury kontroli zmian
Sieć informatyczna	Brak wymuszenia szyfrowania transmisji danych w sieci
	Przesyłanie haseł w jawnej postaci
Oprogramowanie	Brak aktualizacji oprogramowania (usługi sieciowe i systemy operacyjne)
	Brak lub niewystarczające procedury testowania oprogramowania
	Brak mechanizmów identyfikacji i uwierzytelniania

Rodzaj aktywów	Podatność
	Brak mechanizmów monitorowania aktywności użytkowników (logowania zdarzeń)
	Niewłaściwie skonfigurowane aplikacje, usługi lub systemy operacyjne
	Znane błędy (dziury), podatności w oprogramowaniu lub bazach danych
Personel	Brak wykonywanych regularnie procedur nadzoru
	Niewłaściwy przydział uprawnień dostępu
	Przechowywanie kopii w miejscu wytworzenia
	Brak stosowania „polityki czystego biurka i ekranu"
	Brak szkoleń w zakresie bezpieczeństwa
Sprzęt	Brak testowania urządzeń zasilających
	Brak kopii zapasowych/archiwalnych
	Niewłaściwe wycofywanie nośników z użycia
Lokalizacja	Brak elektronicznej kontroli dostępu
	Brak gwarantowanego zasilania

Źródło: opracowanie własne.

Dla każdego zagrożenia zidentyfikowanego w ramach aktywów (grupy aktywów) wykorzystywanych do operacji przetwarzania danych osobowych należy przeanalizować skutki, jakie się pojawią w przypadku zmaterializowania się zagrożeń w kontekście naruszenia praw i wolności osób fizycznych (tabele 8 i 9).

Tabela 8. Tabela skutków naruszeń praw i wolności osób fizycznych

Lp.	Skutek naruszenia
1	Dyskryminacja
2	Kradzież tożsamości
3	Strata finansowa
4	Naruszenie dobrego imienia
5	Naruszenie poufności danych osobowych objętych tajemnicą zawodową
6	Nieautoryzowane przywrócenie danych po pseudoanonimizacji
7	Wszelka inna szkoda gospodarcza lub przemysłowa

Źródło: opracowanie własne.

Każde ryzyko zidentyfikowane w ramach aktywów (grup aktywów) wykorzystywanych do przetwarzania danych osobowych, przy uwzględnieniu podatności i istniejących zabezpieczeń, należy ocenić pod kątem prawdopodobieństwa materializacji ryzyka (tabela 10).

Tabela 9. Ocena skutków naruszenia praw i wolności osób fizycznych

Wartość	Nazwa	Opis
3	Wysokie	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych
2	Niskie–średnie	Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych, jednak nie są one wysokie
0	Brak	Wskazane skutki w kontekście materializacji analizowanego ryzyka nie występują

Źródło: opracowanie własne.

Tabela 10. Tabela prawdopodobieństwa materializacji ryzyka

Wartość	Nazwa	Opis
5	Niemal pewne	Istnieją racjonalne przesłanki, by ocenić, że zagrożenie zmaterializuje się w najbliższym czasie (prawie na 90%)
4	Wysoce prawdopodobne	Istnieją racjonalne przesłanki, by ocenić, że zagrożenie raczej się zmaterializuje, istnieje więcej niż połowa szans na wystąpienie. Materializowało się w ciągu ostatniego roku
3	Bardzo prawdopodobne	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa. Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 2 lat)
2	Średnio prawdopodobne	Zagrożenie może wystąpić sporadycznie. Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 3 lat)
1	Mało prawdopodobne	Zagrożenie raczej nie wystąpi lub możliwość jego wystąpienia jest znikoma (bliska zera). Zagrożenie nie materializowało się w przeszłości

Źródło: opracowanie własne.

W celu zapewnienia ograniczenia ryzyka naruszenia praw i wolności osób fizycznych, których dane są przetwarzane, należy dobrać odpowiednie zabezpieczenia wynikające z dobrych praktyk opisanych w normie PN-ISO/IEC 27002:2014–12[8]. Norma ta opisuje zabezpieczenia techniczne i organizacyjne, które mogą pomóc w ochronie informacji w podziale na:

- cele stosowania zabezpieczeń,
- zabezpieczenia,
- wskazówki dotyczące wdrożenia,
- inne informacje pomocnicze.

[8] giodo.gov.pl/234/id_art/9276/j/pl (data odczytu: 05.11.2018).

Ocenę ryzyka naruszenia praw i wolności osób fizycznych przeprowadza się, stosując następujący wzór:

$$R = S * P_{\text{Podatności}} * P_{\text{Prawdopodobieństwa}},$$

gdzie:

R – ocena powagi ryzyka naruszenia praw i wolności osób fizycznych,

S – ocena skutków naruszenia praw i wolności osób fizycznych,

$P_{\text{Podatności}}$ – ocena podatności aktywów wykorzystywanych do operacji przetwarzania,

$P_{\text{Prawdopodobieństwa}}$ – ocena prawdopodobieństwa urzeczywistnienia się zagrożenia.

Na skutek przeprowadzonej analizy otrzymujemy zestawienie tabelaryczne (tabela 11) prezentujące poziom ryzyka według następującej skali:

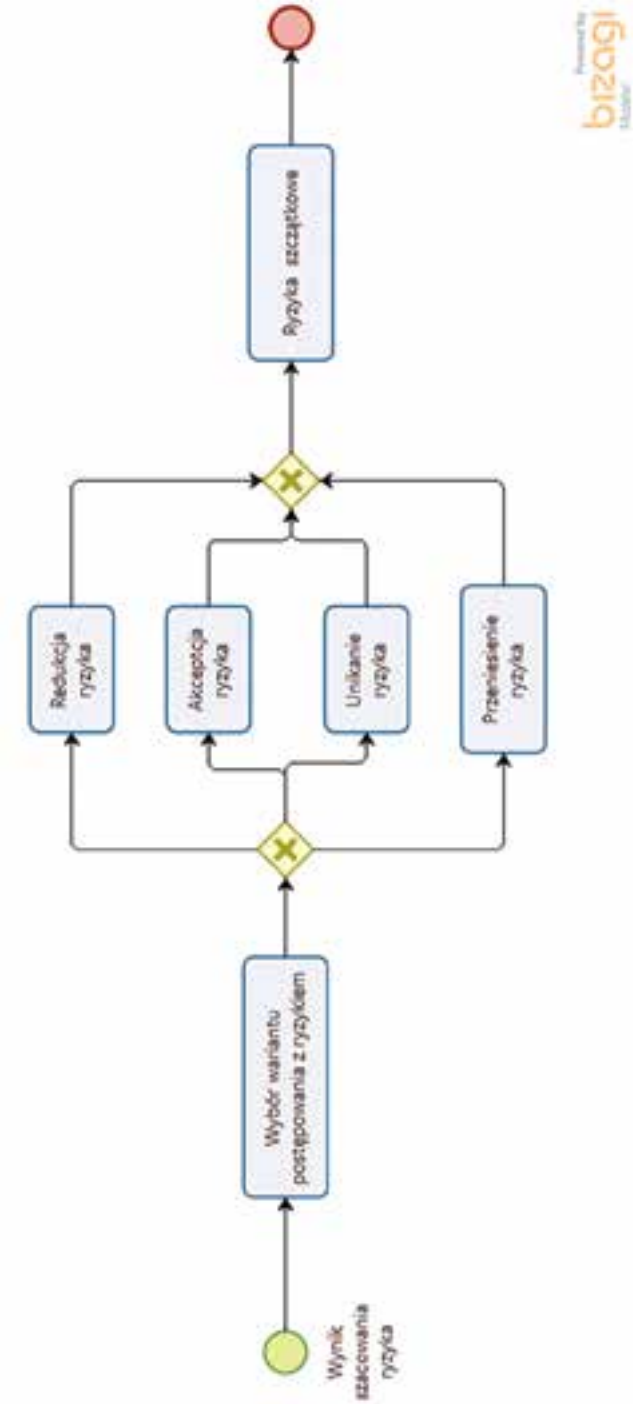
a) wartości od 2 do 16 oznaczają „ryzyko niskie" akceptowalne, niewymagające dalszego postępowania,
b) wartości od 18 do 45 oznaczają „ryzyko wysokie" nieakceptowalne, wymagające zastosowania dalszych kroków postępowania z ryzykiem.

Tabela 11. Tabela oceny powagi ryzyka naruszenia praw i wolności osób fizycznych

		$S * P_{\text{Podatności}}$				
		2	3	4	6	9
$P_{\text{Prawdopodobieństwa}}$	1	2	3	4	6	9
	2	4	6	8	12	**18**
	3	6	9	12	**18**	**27**
	4	8	12	16	**24**	**36**
	5	10	15	**20**	**30**	**45**

Źródło: opracowanie własne.

Ryzykiem można zarządzać na kilka sposobów (rysunek 4). Celem zarządzania ryzykiem jest wybór wariantu postępowania na wypadek materializacji ryzyka oraz zaplanowanie odpowiednich środków organizacyjnych i technicznych mających zapewnić ochronę danych osobowych i wykazać zgodność z RODO w zakresie praw i interesów osób fizycznych, których dane są przetwarzane przez podmiot.



Rysunek 4. Proces zarządzania ryzykiem w przypadku jego identyfikacji

Źródło: opracowanie własne.

Może zaistnieć sytuacja, że mimo zastosowana środków redukujących ryzyko przetwarzania danych lub ryzyko naruszenia praw i wolności osób fizycznych, wartość ryzyka przewyższa akceptowalny poziom (brak zgodności z wymaganiami RODO). W opisanym przypadku przed rozpoczęciem przetwarzania danych osobowych administrator danych osobowych musi dokonać konsultacji z organem nadzorczym. Przegląd i monitorowanie mechanizmów przewidzianych do ochronnych danych osobowych należy realizować na wszystkich etapach zarządzania ryzkiem. Zakres weryfikacji powinien uwzględniać następujące zagadnienia:

- Czy nie uległ zmianie kontekst przetwarzania danych osobowych?
- Czy nie jest planowana zmiana kontekstu przetwarzania danych osobowych, co może skutkować nowymi czynnościami przetwarzania oraz wpłynąć na listę zasobów?
- Czy operacje przetwarzania danych osobowych, które zostały wyłączone z analizy ryzyka aktualnie nie generują ryzyka naruszenia praw i wolności osób fizycznych?
- Czy organ nadzorczy ustanowił nowy lub uaktualnił wykaz rodzajów operacji przetwarzania danych osobowych, które należy uwzględnić w ocenie ryzyka?
- Czy nie uległy zmianie lub czy w najbliższym czasie nie ulegną zmianie warunki przyczyniające się do konieczności i proporcjonalności przetwarzania danych?
- Czy zidentyfikowane ryzyko nadal jest aktualne?
- Czy stosowane zabezpieczenia techniczne i organizacyjne nadal zmniejszają ryzyko przetwarzania danych osobowych oraz czy jednocześnie są skuteczne?

O ryzyku powinny być informowane wszystkie zainteresowane strony na wszystkich etapach procesu zarządzania ryzykiem ochrony danych osobowych. Te same osoby powinny być zaangażowane w proces konsultacyjny. W ramach tych działań należy wziąć pod uwagę następujących aktorów:

- administratora danych osobowych,
- inspektora danych osobowych,
- właścicieli zasobów wykorzystywanych podczas przetwarzania danych osobowych,
- właścicieli procesów, którzy będą weryfikować zgodność z prawem i regulacjami wewnętrznymi,
- organ nadzorczy odpowiedzialny za ochronę danych osobowych w organizacji,
- osoby fizyczne, których dane dotyczą,
- zewnętrznych, niezależnych ekspertów.

3.3. Lista norm do uwzględnienia w procesie oceny ryzyka

W tabeli 12 została zaprezentowana lista norm, które należy uwzględnić w procesie oceny ryzyka.

Tabela 12. Lista norm do uwzględnienia w ocenie ryzyka

Norma	Opis
PN/ISO/IEC 27001	Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji
PN/ISO/IEC 27002	Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zabezpieczania informacji
PN/ISO/IEC 27005	Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji
PN/ISO 31000	Zarządzanie ryzykiem. Zasady i wytyczne
ISO 22301 (BS 25999)	Zarządzanie ciągłością działania

Źródło: opracowanie własne.

4. Podsumowanie i kierunki dalszych badań

Instytucje państwowe, przedstawiciele biznesowi i wszyscy, którzy prowadzą przedsięwzięcia związane z przetwarzaniem danych osobowych, są zobowiązani do dostosowania środowiska przetwarzania danych osobowych (systemów informatycznych, procesów, procedur) do nowych wytycznych wynikających z obowiązujących wymagań prawa do dnia 25 maja 2018 r. RODO jest dokumentem obszernym i niełatwym w interpretacji. Stąd też im krótszy zostaje czas na dostosowanie, tym więcej powstaje szumu medialnego, związanego ze skutkami wejścia w życie nowych przepisów.

Dostosowanie do nowych przepisów wymaga nakładu pracy wprost proporcjonalnego do złożoności analizowanej organizacji. Konsekwencje braku zgodności z RODO mogą w skrajnych przypadkach być bolesne ze względu na kary przewidziane regulacją (do 20 mln euro lub do 4% wartości rocznego światowego obrotu podmiotu). Należy wziąć pod uwagę, że w Polsce obowiązują już przepisy dotyczące ochrony danych osobowych. Podmioty, które tych przepisów przestrzegały w znaczącym stopniu będą wypełniały wymogi RODO. W ramach dalszych prac badawczych będą analizowane następujące zagadnienia:

- wpływ RODO na środowiska bazodanowe z zakresu *Big Data*,
- opracowanie autorskiego zestawu różnych rodzajów polityki z zakresu *Data Governance* realizujących rozporządzenie RODO[9].

Bibliografia

Al-Ruithe M., Mthunzi S., Benkhelifa E., *Data Governance for Security in IoT & Cloud Converged Environments*, 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA).

Bhatti M.W., Hayat F., Ehsan N., Ishaque A., Sohail A., Ebtisam M., *A Methodology to Manage the Changing Requirements of a Software Project*, 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM).

Castillo L.F., Raymundo C., Domingues F., *Information Architecture Model for the Successful Data Governance Initiative in the Peruvian Higher Education Sector*, 2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing.

Data Protection Impact Assessment (DPIA) FBI Polska.

Heimes R., *Global InfoSec and Breach Standard,* „IEEE Security & Privacy" 2016, Volume 14, Issue 5.

Pulkkis G., Karlsson J., Westerlund M., Tana J., *Secure and Reliable Internet of Things Systems for Healthcare*, 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud).

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)

Yulfitri A., *Modeling Operational Model of Data Governance in Government*, 2016 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung-Bali, October 24–27, 2016.

Źródło internetowe

giodo.gov.pl/234/id_art/9276/j/pl (data odczytu: 05.11.2018).

[9] Al-Ruithe M., Mthunzi S., Benkhelifa E., *Data Governance for Security in IoT & Cloud Converged Environments*, 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA); A. Yulfitri, *Modeling Operational Model of Data Governance in Government*, International Conference on Information Technology Systems and Innovation (ICITSI), Bandung-Bali, October 24–27, 2016.

* * *

Change management in terms of GDPR and risk management

Abstract
Change management in information systems is one of the most important elements of software engineering. Development of the change management process in IT systems gives organisations an opportunity to respond to the business needs of end-users and efficient management of change requests. Functional analysis provides implementation guidelines as well as input and output conditions for testing process to quality check of the implemented change in the IT environment. The results of the analysis allow for estimating the time needed to implement the change and the costs of its implementation. Doing tests gives a possibility of quality checks on how the change affects the IT system and processing personal data, and if quality of the change performance is at the assumed level defined by the client. This article describes the change management process, taking into account the GDPR requirements in the area of risk analysis.
Keywords: change management, process, software engineering, GDPR, risk management, risk protection