Agnieszka Dornfeld, Ewa Kulińska

Zastosowanie zarządzania ryzykiem w przetwarzaniu danych osobowych w systemach informatycznych

Ekonomiczne Problemy Usług nr 117, 497-506

2015

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

EWA KULIŃSKA
Politechnika Opolska[1]

AGNIESZKA DORNFELD
Urząd Kontroli Skarbowej[2]

ZASTOSOWANIE ZARZĄDZANIA RYZYKIEM W PRZETWARZANIU DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

Streszczenie

W publikacji przedstawiono zarządzanie ryzykiem w obszarze przetwarzania danych osobowych oraz realizowane w tym zakresie mechanizmy kontrolne w jednostkach sektora finansów publicznych. W zakresie mechanizmów kontrolnych uwzględniono zmiany, jakie zaszły w ustawie o ochronie danych osobowych, które weszły w życie 1 stycznia 2015 roku. Zmiany te dotyczą nowej roli administratora bezpieczeństwa informacji.
Słowa kluczowe: zarządzanie ryzykiem, identyfikacja i analiza ryzyka, dane osobowe, przetwarzanie danych osobowych, systemy informatyczne.

Wprowadzenie

Cel publikacji to przeanalizowanie zastosowania zarzadzania ryzykiem w przetwarzaniu danych osobowych w systemach informatycznych. Inspiracją do rozpoczęcia badań w tym zakresie są zmiany, jakie zaszły w ustawie o ochronie danych osobowych, które weszły w życie 1 stycznia 2015 roku.

---

[1] Wydział Inżynierii Produkcji i Logistyki.
[2] UKS w Opolu.

Zmiany dotyczą w przeważającym zakresie nowej roli administratora bezpieczeństwa informacji (ABI), któremu powierzono większy zakres obowiązków. Część obowiązków, realizowanych do tej pory przez GIODO (Generalnego Inspektora Ochrony Danych Osobowych), przeniesiona zostanie bowiem na administratorów danych osobowych (ADO) i w konsekwencji na powołanych przez nich ABI.

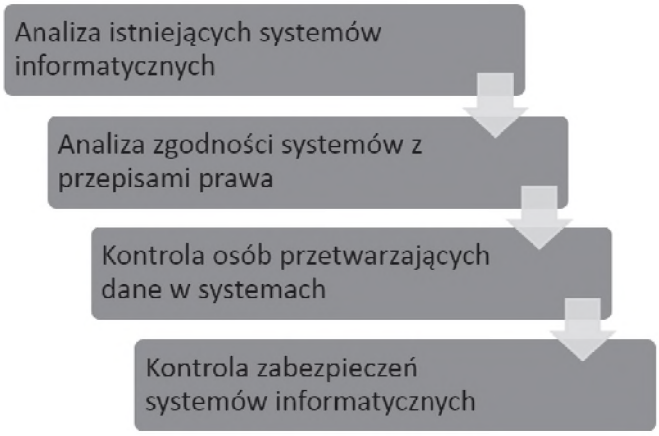
Te zmiany pociągają za sobą konsekwencje w funkcjonowaniu mechanizmów kontrolnych w procesie zarządzania ryzykiem w przetwarzaniu danych osobowych w systemach informatycznych.

1. Zarzadzanie ryzykiem w obszarze przetwarzania danych osobowych

Pojęcie systemu informatycznego określone zostało w art. 7 pkt 2a ustawy o ochronie danych osobowych. Zgodnie z brzmieniem tego artykułu systemem informatycznym jest zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych (DzU z 2014, poz. 1182).

Każdy system, aby został oceniony jako „bezpieczny", musi przejść analizę zgodności z przepisami prawa oraz kontrolę zabezpieczeń systemu.

Na rys. 1. przedstawiono zakres analiz i kontroli systemów.



Rys. 1. Kontrola zabezpieczenia systemów informatycznych

Źródło: opracowanie własne.

Analiza danych osobowych przetwarzanych w systemach informatycznych odnosi się do zasad przetwarzania danych osobowych. Wyróżnia się następujące zasady przetwarzania danych osobowych:

1. zasady legalności – odnosi się do przetwarzania danych zgodnie z prawem;

2. zasady celowości – która dotyczy zbierania danych dla oznaczonych, zgodnych z prawem celów i niepoddawania ich dalszemu przetwarzaniu niezgodnemu z tymi celami;
3. zasady merytorycznej poprawności – czyli dbałości o merytoryczną poprawność danych;
4. zasady adekwatności – odnoszącej się do adekwatności danych w stosunku do celów, w jakich są przetwarzane;
5. zasady ograniczenia czasowego – w zakresie przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Stosowanie zasad w zakresie przetwarzania danych osobowych znajduje odzwierciedlenie w prowadzonym procesie zarządzania ryzykiem w zabezpieczeniach systemów informatycznych w obszarze przetwarzania danych osobowych.

Proces zarządzania rozpoczyna się od identyfikacji ryzyka w obszarze przetwarzania danych osobowych. W obszarze tym identyfikuje się szereg zagadnień (czynników ryzyka), które są poddawane szczegółowej analizie. Jako najważniejsze należy wymienić:

- obchodzenie się użytkowników z dokumentami,
- ujawnienie informacji dotyczących danych osobowych,
- nadawanie upoważnienia do przetwarzania danych osobowych
- przetwarzanie danych osobowych.

Do każdego z wymienionych zagadnień należy odnieść analizę ryzyka procesu, celem zabezpieczenia całego obszaru danych osobowych.

Drugi etap to analiza ryzyka w obszarze przetwarzania danych osobowych. Dotyczy ona:

- znajomości aktów prawnych,
- uregulowań wewnętrznych,
- sprawdzenia, czy każda osoba przetwarzająca dane osobowe posiada stosowane upoważnienie,
- sprawdzenia, czy sprawowana jest właściwa kontrola ADO, ABI, ASI,
- sprawdzenia, czy dane w jednostce są właściwie zabezpieczone,
- sprawdzenia, czy systemy informatyczne są właściwie zabezpieczone,
- sprawdzenia, czy zagrożenia w systemach informatycznych są analizowane,
- sprawdzenia, czy stosowane są następujące normy:
  - Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.
  - PN-SIO/IEC-17799:2005: Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007.

- PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.
- PN-I-02000: Zabezpieczenia w systemach informatycznych – Terminologia, PKN, 1998.
- PN-SIO/IEC-17799:2005: Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007.

Kolejnym etapem analizy ryzyka jest odniesienie czynników warunkujących negatywne zdarzenia do czynników ryzyka w danym obszarze. Czynniki ryzyka zostały skategoryzowane w ramach następujących kategorii:

- ekonomiczne i finansowe,
- nadużycia,
- organizacja i zarządzanie,
- polityczne i społeczne,
- prawne,
- środowiskowe i działania sił wyższych,
- techniczne i związane z infrastrukturą.

Każdej z kategorii przypisuje się konkretne parametry warunkujące powstanie czynnika ryzyka. Przykład przypisanych paramentów do obszaru ryzyka znajduje odzwierciedlenie w rejestrze ryzyka. Fragment rejestru ryzyka dotyczący obszaru ochrony danych osobowych przedstawiono w tabeli 1.

Tabela 1

Rejestr ryzyka obszaru ochrona danych osobowych

Ochrona danych osobowych (ABI)	
Obszar ryzyka	Ochrona danych – obchodzenie się użytkowników z dokumentami, ujawnianie informacji dotyczących danych osobowych. Ochrona danych – nadawanie uprawnień i przetwarzanie danych.
Ryzyko w obszarze	Wypłynięcie danych na zewnątrz, trafienie danych w niewłaściwe ręce, przetwarzanie danych przez osoby nieuprawnione, nienadanie odpowiednich uprawnień do przetwarzania danych osobowych w systemach informatycznych, w formie papierowej, ujawnienie prawnie chronionych informacji, udostępnianie dokumentacji dotyczących pracowników, nieprawidłowe obchodzenie się z dokumentami, przechowywanie dokumentów na ogólnodostępnych dyskach, na prywatnych komputerach lub nie zabezpieczonych fizycznie lub kryptograficznie nośnikach, niewłaściwe obchodzenie się z danymi osobowymi.
Czynniki ryzyka	1.3, 3.5, 3.12, 6.4, 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10
Ocena	4 X 4 = 16
Poziom istotności	wysoki
Skutek ryzyka	Organizacyjny. Odpowiedzialność karna, odpowiedzialność odszkodowawcza, wyciek danych, ujawnienie danych osobowych, naruszenie przepisów w zakresie ochrony danych osobowych.
Funkcjonujące mechanizmy kontrolne	Polityka Danych Osobowych, Instrukcja Zarządzania Systemami Informatycznymi, wykaz systemów informatycznych, właściwy podział zadań między ABI i ASI, analiza zagrożeń w systemach informatycznych, akty prawne.
Strategia	redukcja
...	...

Źródło: opracowanie własne.

Kolejnym etapem analizy jest ustalenie wartości punktowej każdego czynnika ryzyka przy uwzględnieniu stopnia oddziaływania i stopnia prawdopodobieństwa wystąpienia danego ryzyka w obszarze danych osobowych. Wartość ryzyka obliczana jest wg wzoru (1).

$$IR = PR \text{ x } SR \quad (1)$$

gdzie:
IR – to współczynnik istotności ryzyka,
PR – to prawdopodobieństwo wystąpienia ryzyka,
SR – to potencjalne oddziaływanie wystąpienia ryzyka.

Przy obliczaniu wartości ryzyka wzięto pod uwagę parametry z tab. 2 i tab. 3.

Tabela 2

Skala punktowa czynników ryzyka dla rejestru ryzyka

Stopień oddziaływania wystąpienia ryzyka	**Opis szczegółowy**	**Wartość punktowa skutku**
nieznaczny	• znikomy wpływ na realizację celów i zadań, • brak skutków prawnych, • nieznaczny skutek finansowy, • brak wpływu na bezpieczeństwo pracowników, • brak wpływu na wizerunek urzędu	1
mały	• mały wpływ na realizację celów i zadań, • brak skutków prawnych, • mały skutek finansowy, • brak wpływu na bezpieczeństwo pracowników, • niewielki wpływ na wizerunek urzędu	2
średni	• średni wpływ na realizację celów i zadań, • umiarkowane konsekwencje prawne, • średni skutek finansowy, • brak wpływu na bezpieczeństwo pracowników, • średni wpływ na wizerunek urzędu	3
poważny	• poważny wpływ na realizację zadania, w tym poważne zagrożenie terminu jego realizacji, jak i osiągnięcia celu, • poważne konsekwencje prawne, • zagrożenie bezpieczeństwa pracowników, • poważne straty finansowe, • poważny wpływ na wizerunek urzędu	4
katastrofalny	• brak realizacji zadania i brak realizacji celu, • bardzo poważne i rozległe konsekwencje prawne, • naruszenie bezpieczeństwa pracowników (ujemne konsekwencje dla ich życia i zdrowia), • wysokie straty finansowe, • utrata dobrego wizerunku urzędu w środowisku oraz w opinii publicznej	5

Źródło: opracowanie własne.

Tabela 3

Punktowe prawdopodobieństwo wystąpienia czynników ryzyka dla rejestru ryzyka

Prawdopodob. wystąpienia ryzyka	**Opis szczegółowy**	**Wartość punktowa skutku**
bardzo rzadkie lub prawie niemożliwe	• zdarzenie może zaistnieć jedynie w wyjątkowych okolicznościach, • wystąpi sporadycznie raz na 5 lat, a najprawdopodobniej w ogóle nie zaistnieje, • nie wystąpiło dotychczas, • dotyczy jednostkowych spraw, • prawdopodobieństwo wystąpienia określa się na 1–20%	1
małe	• istnieje małe prawdopodobieństwo, że wystąpi kilka razy w ciągu 3 lat, • dotyczy nielicznych spraw, • prawdopodobieństwo wystąpienia określa się na 21–40%	2
średnie	• zaistnienie zdarzenia jest średnio możliwe, może wystąpić częściej niż kilka razy w ciągu 3 lat, • dotyczy niektórych spraw, • prawdopodobieństwo wystąpienia określa się na 41–60%	3
wysokie	• zaistnienie zdarzenia jest bardzo prawdopodobne, • wystąpi regularnie przynajmniej raz w roku, • dotyczy większości spraw, • prawdopodobieństwo wystąpienia określa się na 61–80%	4
prawie pewne	• oczekuje się, że zdarzenie takie nastąpi na pewno, • wystąpi regularnie co miesiąc lub częściej, • dotyczy wszystkich lub prawie wszystkich spraw, • prawdopodobieństwo wystąpienia określa się na 81–100%	5

Źródło: opracowanie własne.

Kolejnym etapem analizy ryzyka jest ustalenie poziomu ryzyka poprzez odniesienie go do matrycy ryzyka, rys. 2.

SKUTEK					
katastrofalny	5	10	15	20	25
poważny	4	8	12	16	20
średni	3	6	9	12	15
mały	2	4	6	8	10
nieznaczny	1	2	3	4	5
	bardzo rzadkie lub prawie niemożliwe	małe	średnie	wysokie	prawie pewne
	PRAWDOPODOBIENSTWO				

Rys. 2. Matryca 5 x 5 – ustalenie poziomu ryzyka w jednostce

Źródło: opracowanie własne.

2. Mechanizmy kontrolne w zarządzaniu ryzykiem w obszarze przetwarzania danych osobowych

Po przeprowadzonej analizie czynników ryzyka należy zweryfikować funkcjonujące mechanizmy kontrolne. Należy wskazać wszystkie funkcjonujące mechanizmy kontrolne z podziałem na zewnętrzne i wewnętrzne.

W zakres mechanizmów kontrolnych zewnętrznych wchodzą uregulowania prawne i zarządzenia. Natomiast do mechanizmów kontrolnych wewnętrznych należą zarządzenia wewnętrzne oraz zakresy obowiązków. Weryfikuje się w nich aktualność uregulowań, zgodność z aktami prawnymi, regulacje najważniejszych kwestii zabezpieczenia obszaru bezpieczeństwa danych, sprawdza, czy wymagane są korekty.

Funkcjonowanie mechanizmów kontrolnych podporządkowane jest według zadań do konkretnych obszarów kierownikom jednostek organizacyjnych. W tabeli 4 wskazano zadania, jakie zostały zidentyfikowane i wskazane przez właścicieli procesu w ramach realizacji mechanizmów kontrolnych.

Tabela 4

Zadania do realizacji po przeprowadzeniu analizy ryzyka

Lp.	Zakres zadania do realizacji	Osoba odpowiedzialna
1	Zakres obowiązków ABI, ASI: • Dokonać szczegółowego podziału zadań na ABI i ASI. • Uwzględnić aspekt prowadzenia kontroli ASI przez ABI. • Uwzględnić aspekt prowadzenia kontroli ABI przez ADO. • Składanie rocznych raportów w zakresie sprawowania kontroli i zabezpieczenia procesu ochrony danych osobowych.	Dyrektor / kierownik komórki
2	Upoważnienia do przetwarzania danych osobowych dla pracowników: • Przeprowadzenie analizy potrzeb w zakresie nadania uprawnień. • Nadanie właściwych uprawnień poszczególnym pracownikom. • Uaktualnienia zakresu nadanych uprawnień w upoważnieniach. • Zarejestrowanie nadanych upoważnień.	ABI, ASI
3	Polityka bezpieczeństwa danych osobowych: • Opracowanie lub uaktualnienie. • Zweryfikowanie istniejących dokumentów pod kątem zgodności z przepisami (podstawowych wymagań zawartych w przepisach).	ABI, ASI
4	Instrukcja zarządzania systemami informatycznymi: • Opracowanie lub uaktualnienie. • Zweryfikowanie istniejących dokumentów pod kątem zgodności z przepisami (podstawowych wymagań zawartych w przepisach).	ABI, ASI
5	Analiza zagrożeń w systemach informatycznych: • Analiza istniejących systemów informatycznych. • Analiza zgodności systemów z przepisami prawa. • Kontrola osób przetwarzających dane w systemach. • Kontrola zabezpieczeń systemów informatycznych.	ABI, ASI
6	Kontrola użytkowników: • Ustalenie zakresu kontroli ABI i ASI. • Opracowanie harmonogramu kontroli użytkowników przez ABI i ASI. • Prowadzenie kontroli przez ABI nad ASI w zakresie zabezpieczenia systemów informatycznych, analiz zagrożeń. • Prowadzenie kontroli przez ADO nad ABI w zakresie przetwarzania danych, wypracowanych dokumentów (Polityka bezpieczeństwa danych osobowych, Instrukcja zarządzania systemami informatycznymi). • Prowadzenie kontroli nad zgodnością systemów z przepisami prawa przez ABI. • Kontrola zagrożeń w systemach informatycznych sprawowana przez ABI.	ABI, ASI

Źródło: opracowanie własne.

Precyzyjne wskazanie zadań i przydzielenie ich konkretnym osobom do realizacji w analizowanym obszarze ma na celu zapewnienie zabezpieczenia procesu.

Podsumowanie

O znaczeniu zarzadzania ryzykiem przy ochronie przetwarzania danych osobowych nie trzeba przekonywać. W publikacji przeanalizowano etapy realizacji tego procesu z uwzględnieniem zmian wprowadzonych od 1 stycznia 2015 roku, dotyczących nowej roli administratora bezpieczeństwa informacji, któremu powierzono większy zakres obowiązków. ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych. Administrator danych zapewnia środki i organizacyjną odrębność ABI niezbędną do niezależnego wykonywania przez niego zadań. Do jego zadań ponadto należą: przestrzeganie zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO; nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych; zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych; prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez ADO.

Jest to szereg bardzo istotnych funkcji o kluczowym znaczeniu dla procesu zarzadzania ryzykiem. Szczególnie że zmiana roli administratora bezpieczeństwa informacji wpływa na funkcjonowanie mechanizmów kontrolnych w procesie zarządzania ryzykiem w przetwarzaniu danych osobowych w systemach informatycznych.

Literatura

1. Ustawa z dnia z dnia 26 czerwca 2014 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych w internetowym systemie aktów prawnych na stronie Sejmu Rzeczypospolitej Polskiej (DzU z 2014 r., poz. 1182).
2. Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych w internetowym systemie aktów prawnych na stronie Sejmu Rzeczypospolitej Polskiej (DzU z 2004 r. nr 33, poz. 285).
3. Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych w internetowym systemie aktów prawnych na stronie Sejmu Rzeczypospolitej Polskiej (DzU z 2001 r. nr 100, poz. 1087).
4. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w internetowym systemie aktów prawnych na stronie Sejmu Rzeczypospolitej Polskiej (DzU z 1997 r. nr 133, poz. 883).
5. www.uke.gov.pl (2013).
6. file:///C:/Users/user/Downloads/sprawozdanie-GIODO-za-rok-2008.pdf.

THE RISK MANAGEMENT IN PERSONAL DETAILS PROCESSING IN IT SYSTEMS

Summary

The risk management was presented in the area of personal details processing and control mechanisms in the department of public finances were presented in this paper. In terms of control mechanisms the changes in the Personal Data Protection Act which is effective on 1 January 2015 was considered. The changes concern new role of an administrator of information safety.

Keywords: risk management, identification and risk analysis, personal details, personal data processing, IT systems.

Translated by Ewa Kulińska