

ZARZĄDZENIE NR OR.120.80.2023
BURMISTRZA WOŹNIK

z dnia 13 kwietnia 2023 r.

**w sprawie przyjęcia zasad przeprowadzania analizy ryzyka w obszarze ochrony danych osobowych
w Urzędzie Miejskim w Woźnikach**

Na podstawie art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

zarządzam, co następuje:

§ 1.

Wprowadza się zasady przeprowadzania analizy ryzyka w obszarze ochrony danych osobowych w Urzędzie Miejskim w Woźnikach, stanowiące załącznik nr 1 do niniejszego zarządzenia.

§ 2.

Analizę ryzyka przeprowadza się w oparciu o metodę przyjętą w załączniku nr 2 do niniejszego zarządzenia.

§ 3.

Uchyla się:

1. § 9 w Rozdziale V w Załączniku nr 1 do Zarządzenia Nr KR.120.91.2018 Burmistrza Woźnik z dnia 24.05.2018 r. w sprawie wprowadzenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Woźnikach ze zm.,

2. formularz nr 16 i 17 do Zarządzenia Nr KR.120.91.2018 Burmistrza Woźnik z dnia 24.05.2018 r. w sprawie wprowadzenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Woźnikach ze zm.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

ZASADY PRZEPROWADZANIA ANALIZY RYZYKA W OBSZARZE OCHRONY DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W WOŹNIKACH

1. Celem zarządzania ryzykiem jest zapewnienie skutecznego przestrzegania przepisów prawa, skutecznej ochrony praw i wolności osób, których dane są przetwarzane oraz skutecznej ochrony Administratora.

2. Etapy zarządzania ryzykiem.

- 1) szacowanie ryzyka:
 - a) identyfikacja zagrożeń
 - b) ocena ryzyka
- 2) reakcja na ryzyko
- 3) monitorowanie ryzyka
- 4) działania korekcyjne

3. Szacowanie ryzyka

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

4. **Identyfikacja ryzyka** ma na celu wskazanie niekorzystnych zjawisk, zdarzeń, praktyk, itp., które w konsekwencji mogą zagrozić realizacji celów i zadań oraz ochrony praw i wolności osób, których dane są przetwarzane. Zagrożenie wg PN-ISO Guide 73:2012 to źródło potencjalnej szkody. Zagrożenie może być uszczegółowione przez podanie pochodzenia (np. zagrożenie mechaniczne, zagrożenie elektryczne) albo charakteru potencjalnej szkody (np. ujawnienie poufnych danych).

5. Ocena ryzyka

Zidentyfikowane ryzyka poddawane są ocenie mającej na celu określenie prawdopodobieństwa wystąpienia ryzyka oraz jego wpływu.

Oceny ryzyka dokonywana jest różnymi metodami, w tym:

- 1) metodą ilościową - bazującą na informacjach i danych z przeszłości, które mają charakter liczbowy: ilość, częstotliwość, zmienność,
- 2) metodą jakościową - stosowaną jeśli ryzyko nie poddaje się obliczeniom lub brak jest dostępu do danych je charakteryzujących, albo gdy ich uzyskanie byłoby zbyt kosztowne; jakość oceny jest tu częściowo oparta na kompetencjach (wiedzy, doświadczeniu) osób dokonujących tych analiz, a częściowo ma charakter intuicyjny, tzw. profesjonalny osąd,
- 3) metodą ilościowo-jakościową - będącą połączeniem wskazanych wyżej dwóch technik.

6. Określenie wpływu

polega na wskazaniu stopnia zagrożenia dla realizacji zadań lub celów według poniższej skali ocen:

Wpływ	Skala	Opis
Wysoki	4	Zdarzenie uniemożliwia funkcjonowanie, koszt finansowy wysoki, znaczna utrata reputacji
Średni	3	Zdarzenie uniemożliwia realizację celów i zadań, koszt finansowy średni, średnia utrata reputacji
Niski	2	Zdarzenie utrudnia realizację celów i zadań, niski koszt finansowy, niska utrata reputacji
Znikomy	1	Zdarzenie w nieznaczny sposób wpływa na funkcjonowanie, brak kosztów finansowych oraz utraty reputacji

Określenie wpływu zdarzenia na finanse oraz wartości niematerialne, takie jak np. utrata dobrego wizerunku lub wpływ ujawnienia określonych danych na pozycję społeczną osoby, której one dotyczą

Wpływ	Skala	Opis
Wysoki	4	Wysoka wartość finansowa, wysoki wpływ na reputację
Średni	3	Średnia wartość finansowa, średni wpływ na reputację
Niski	2	Niska wartość finansowa, niski wpływ na reputację
Znikomy	1	Znikoma wartość finansowa, brak wpływu na reputację

7. Określenie prawdopodobieństwa wystąpienia

ryzyka polega na określeniu możliwości wystąpienia ryzyka, według poniższej skali ocen:

Prawdopodobieństwo	Skala	opis
Wysokie	4	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi co najmniej raz w tygodniu.
Średnie	3	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi co najmniej raz w miesiącu
Niskie	2	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi raz na pół roku
Znikome	1	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi raz w ciągu roku lub nie wystąpi w ogóle.

1) W oparciu o ocenę wpływu oraz prawdopodobieństwa ustalany jest poziom istotności ryzyka:

- a) **ryzyko bardzo poważne**, którego iloczyn prawdopodobieństwa wystąpienia oraz wpływu wynosi 12 lub 16 punktów;
- b) **ryzyko umiarkowane**, którego, którego iloczyn prawdopodobieństwa wystąpienia oraz wpływu wynosi od 6 do 9 punktów;

- c) **ryzyko niskie**, którego iloczyn prawdopodobieństwa wystąpienia oraz wpływu wynosi od 1 do 4.

8. Istotność ryzyka

1) Ustalona istotność ryzyka wpływa na poziom akceptacji dla danego ryzyka:

- Poziom ryzyka jest nieakceptowany w przypadku:
- **ryzyka bardzo poważnego**, które wymaga bezwzględnie natychmiastowej reakcji
- Poziom ryzyka jest akceptowany warunkowo w przypadku:
- **ryzyka umiarkowanego**, dla którego wskazana jest reakcja kierownictwa, która może zostać przesunięta w czasie z zastrzeżeniem bieżącego monitorowania.
- Poziom ryzyka jest akceptowany w przypadku:
- **ryzyka niskiego**, dla którego podjęcie działań uzależnia się od decyzji Kierownictwa biorąc pod uwagę ewentualne nakłady.

9. Macierz ryzyka

PRAWDOPODOBIENSTWO	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		WPLYW			

10. Reakcja na ryzyko

- W stosunku do każdego ryzyka powinno się określić rodzaj reakcji (tolerowanie, przeniesienie, unikanie, działanie).
- Należy określić działania, które należy podjąć w celu zmniejszenia danego ryzyka do akceptowanego poziomu.
- Zidentyfikowane i wyrażone wartością ryzyka poddaje się ocenie celem podjęcia odpowiednich decyzji, tj:
 - modyfikowanie (redukcja) ryzyka** – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia).
 - dzielenie (przeniesienie) ryzyka** – polega przykładowo na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub sędowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go. Zgodnie z przepisami ogólnego rozporządzenia o ochronie danych wykupienie ubezpieczenia nie wyeliminuje ryzyka niezastosowania się przez

dany podmiot do przepisów RODO. Administrator w sytuacji, kiedy zleca innym podmiotom przetwarzanie danych, to jako podmiot decydujący o zakresie i celach tego przetwarzania, ponosi pełną odpowiedzialność za zgodne z prawem przetwarzanie wskazanych danych.

- c) **zachowanie (akceptacja) ryzyka** –świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka.
- d) **unikanie ryzyka** – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków

11. Postępowanie z ryzykiem

- 1) W praktyce reakcją na ryzyko są konkretne działania, które mogą polegać m.in. na:
 - przeprowadzeniu szkolenia wewnątrz Urzędu lub skierowanie na szkolenie zewnętrzne,
 - wprowadzenie dodatkowych środków bezpieczeństwa, które umożliwią obniżenie poziomu ryzyka lub całkowite jego wyeliminowanie
 - dokonaniu zmian organizacyjnych
 - wprowadzenie nowych rozwiązań.
- 2) W przypadku, gdy na etapie dotyczącym postępowania z ryzykiem podjęta zostanie decyzja o jego modyfikacji lub całkowitej eliminacji, cały proces dotyczący szacowania ryzyka powinien być powtórzony.
- 3) Dodatkowo, kiedy na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka, zgodnie z art. 35 RODO, wymagane jest przeprowadzenie dla danego procesu przetwarzania oceny jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.
- 4) Podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy administratora, czy podmiotów przetwarzających, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.

12. Monitorowanie i przegląd ryzyka

Ustalone i wyrażone wartością ryzyka są na bieżąco monitorowane. Monitorowanie jest procesem ciągłym, wykonywanym w toku czynności bieżących, celem ewentualnej weryfikacji realizowanych działań.

13. Działania korekcyjne

W przypadku stwierdzenia odstępstwa od zaplanowanych działań podejmuje się działania korygujące, które mają na celu osiągnięcie zakładanych celów.

Arkusz analizy ryzyka									
Obszar ryzyka/ Zasób	Podatność	Zagrożenia	Naruszenie poufności	Naruszenie integralności	Naruszenie dostępności	Prawdopodobieństwo wystąpienia zagrożenia Znikome-1 Niskie-2 Średnie-3 Wysokie-4	Wpływ zagrożenia na utratę praw i wolności osób fizycznych (RODO) Znikomy-1 Niski-2 Średni-3 Wysoki-4	Ryzyko utraty praw i wolności osób których dane dotyczą 1-4 ryzyko niskie 6-9 ryzyko umiarkowane 12-16 ryzyko bardzo poważne	Reakcja na ryzyko np. Zachowanie/akceptacja ryzyka redukcja ryzyka
						0	0	0	