Zarządzenie Nr 13/18
Wójta Gminy Hanna
z dnia 24 maja 2018 r.

w sprawie wprowadzenia Procedury przeprowadzania analizy i oceny ryzyka w Urzędzie Gminy Hanna

Zarządzam, co następuje:

§ 1

Wprowadza się Procedurę przeprowadzania analizy i oceny ryzyka w Urzędzie Gminy Hanna w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się wszystkich pracowników do zapoznania i przestrzegania niniejszego zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania

WÓJT
mgr Grażyna Kowalik

Załącznik do Zarządzenie nr 13/18 Wójta Gminy Hanna z dnia 24 maja 2018 r. w sprawie wprowadzenia Procedury przeprowadzania analizy i oceny ryzyka w Urzędzie Gminy Hanna

PROCEDURY PRZEPROWADZANIA ANALIZY I OCENY RYZYKA W URZĘDZIE GMINY HANNA

§ 1.

Ilekroć w procedurze jest mowa o **Administrator Danych Osobowych** należy przez to rozumieć Urząd Gminy Hanna, reprezentowane przez Wójta Gminy Hanna.

§ 2.

Cel procedury

Analiza i ocena ryzyka ma na celu dobór odpowiednich środków technicznych i organizacyjnych służących do ochrony danych osobowych przetwarzanych przez Administratora Danych Osobowych.

§ 3.

Elementy szacowania ryzyka

Na szacowanie ryzyka składają się następujące elementy:

1) Identyfikacja kategorii danych i ich wartość;
2) Identyfikacja zagrożeń dla poszczególnych kategorii;
3) Ocena ryzyka;
4) Dobór adekwatnych zabezpieczeń do zagrożeń.

§ 4.

1. Na pierwszym etapie Administrator danych osobowych lub zespół powołany przez Administratora dokonuje klasyfikacje danych osobowych ze względu na kategorię:

1) **Dane identyfikacyjne** (imię i nazwisko, imiona rodziców, data urodzenia obywatelstwo)

2) **Dane kontaktowe** (e-mail; telefon kontaktowy, adres zameldowania, adres do korespondencji);

3) **Dane szczególnej kategorii** (dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, zdrowia, seksualności lub orientacji seksualnej, wyroków skazujących).

2. Administrator danych osobowych lub wyznaczony zespół identyfikuje istniejące zagrożenia. Przy identyfikacji ryzyka ADO bierze pod uwagę czynniki zewnętrzne i wewnętrzne mające wpływ na wystąpienie zdarzenia.

3. Każde zagrożenie jest oceniane pod względem prawdopodobieństwa jego wystąpienia:

Prawdopodobieństwo	Poziom	Opis
Duże	3	Zdarzenie może wystąpić co najmniej raz w tygodniu
Średnie	2	Zdarzenie może wystąpić co najmniej raz w miesiącu
Niskie	1	Zdarzenie może wystąpić raz w roku

4. Ocena skutków dokonywana jest w skali od 1 do 3, oceniając niżej wymienione kryteria:

Skutek	Poziom	Opis
Duży	3	Osoby, których dane zostały naruszone mogą napotkać znaczne konsekwencje, których nie mogą pokonać (trudności finansowe, takie jak czarne listy banków, dług, szkody materialne lub niemożność pracy, długoterminowe dolegliwości psychologiczne, itp.)
Średni	2	Osoby, których dane zostały naruszone mogą napotkać znaczne niedogodności, które będą w stanie pokonać pomimo kilku trudności (np. dodatkowe koszty, niemożność korzystania z usług biznesowych, strach, brak zrozumienia, stres, dolegliwości fizyczne itp.)
Mały	1	Osoby, których dane zostały naruszone nie odczują tego skutku, bądź spotkają się z nielicznymi niedogodnościami, nie stanowiącymi większego

		problemu (np. czas poświęcony na ponowne wprowadzenie danych, rozdrażnienie, irytacja)

§ 5.

Ocena ryzyka

1. Poziom ryzyka to iloczyn prawdopodobieństwa i skutku wystąpienia zdarzeń.

Prawdopodobieństwo				
	3 Duże	Ś	W	W
	2 Średnie	M	Ś	W
	1 małe	M	M	Ś
		1 Mały	2 Średni	3 Duży
		Skutek		

Poziom ryzyka określa zależność:

$$R = P \times S$$

gdzie:

R – poziom ryzyka,

P – prawdopodobieństwo wystąpienia zdarzenia,

S – skala oddziaływania w przypadku wystąpienia zdarzenia.

2. Administrator Danych Osobowych określił akceptowalny poziom ryzyka na poziomie 1 – 4. Ryzykiem nieakceptowalnym jest to ryzyko, którego poziom wynosi więcej niż 5.

3. Poziom Istotności Ryzyka:

Poziom ryzyka	Opis
Mały (M) – 1 - 2	Poziom ryzyka akceptowalny
Średni (Ś) – 3 - 4	Poziom ryzyka akceptowalny – działanie wymaga okresowego monitorowania

Wysoki (W) – 5 - 9	Poziom ryzyka nieakceptowalnego

§ 6.

1. Po oszacowaniu ryzyka Administrator Danych Osobowych określa rodzaju reakcji na ryzyko i wskazuje działania zaradcze, jakie należy podjąć w celu zmniejszenia ryzyka do poziomu akceptowalnego lub całkowite wyeliminowania danego ryzyka:

1) **Modyfikacja ryzyka** – polega na obniżeniu poziomu ryzyka np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenia skutków jego wystąpienia;

2) **Akceptacja ryzyka** – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu;

3) **Unikanie ryzyka** – polega na unikaniu działań, które powodują powstanie określonych typów zagrożenia;

4) **Przeniesienie ryzyka** – dotyczyć to będzie kategorii ryzyka w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz.

2. Po zastosowaniu działań profilaktycznych mających na celu wyeliminowanie lub zmniejszenie ryzyka Administrator danych osobowych dokonuje ponownej oceny.

§ 7.

Administrator Danych Osobowych po przeprowadzonej analizie dostosowuje środki bezpieczeństwa, zarówno techniczne, jak i organizacyjne, do wyników uzyskanych z przeprowadzonej analizy.

§ 8.

Analiza i ocena ryzyka dokonywana jest raz w roku oraz po każdej zmianie, która może mieć wpływ na bezpieczeństwo danych osobowych przetwarzanych przez Administratora Danych Osobowych.