WÓJT
GMINY MARKOWA
pow. łańcucki
woj. podkarpackie

ZARZĄDZENIE NR 127/22
WÓJTA GMINY MARKOWA
z dnia 3 października 2022 roku

w sprawie powołania zespołu do spraw dokonania analizy ryzyka dla ochrony danych osobowych w Urzędzie Gminy Markowa

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2022 r. poz. 559, poz. 1005, poz. 1079) oraz w związku z art. 35 ust. 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) (Dz. Urz. UE, L 119 z 4.05.2016r)

zarządzam, co następuje:

§ 1

Powołuję Zespół ds. przeprowadzenia analizy ryzyka dla ochrony danych osobowych w Urzędzie Gminy Markowa, zwany dalej Zespołem, w składzie:

1) Joanna Rupar – Sekretarz Gminy
2) Grzegorz Płowy – Administrator Sieci Informatycznej
3) Urszula Cwynar – Inspektor Ochrony Danych Osobowych.

§ 2

1. Zespół, o którym mowa w § 1 dokona analizy ryzyka zgodnie z „Zasadami i Trybem Przeprowadzania Analizy Ryzyka Dla Ochrony Danych Osobowych w Urzędzie Gminy Markowa".
2. Zasady, o których mowa w ust. 1 stanowi załącznik do niniejszego zarządzenia.

§ 3

Analizę ryzyka dla ochrony danych osobowych w Urzędzie Gminy Markowa należy przeprowadzić co najmniej raz w roku.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Mirosław Mac

Załącznik do Zarządzenia Nr 127/22
Wójta Gminy Markowa
z dnia 3 października 2022 roku

ZASADY I TRYB PRZEPROWADZANIA ANALIZY RYZYKA DLA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY MARKOWA

§ 1

Ilekroć w Zasadach jest mowa o:

1) **Administratorze Danych Osobowych** – należy przez to rozumieć Wójta Gminy Markowa;
2) **RODO** – należy przez to rozumieć 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) (Dz. Urz. UE L Nr 119 s. 1)
3) **Inspektorze Ochrony Danych Urzędu (IOD)** – osoba wyznaczona na podstawie art. 37 ust. 1 lit. a RODO;
4) **kierownikach** – należy przez to rozumieć kierowników wydziałów, referatów, koordynatorów oraz stanowiska samodzielne Urzędu Gminy Markowa;
5) **kontekście** – należy przez to rozumieć wszystkie informacje wiążące się z działaniem Urzędu Gminy Markowa, w tym informacje dotyczące środowiska prawnego, społecznego, finansowego czy też technologicznego, np. przepisy prawne, obowiązujące procedury wewnętrzne;
6) **aktywach** – należy przez to rozumieć wszystko to, co ma wartość dla Urzędu Gminy Markowa oraz Wójta Gminy Markowa jako administratora danych osobowych przetwarzanych w Urzędzie. Przykładowe zidentyfikowane aktywa przedstawiono w tabeli nr 1;
7) **podatności** – należy przez to rozumieć słabość aktywów, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki dla Urzędu Gminy Markowa. Przykładowe podatności przedstawiono w tabeli nr 2;
8) **zagrożeniu** – należy przez to rozumieć stan lub sytuację wywołaną przez siły natury lub przez człowieka, która powoduje, że bezpieczeństwo dla osób i rzeczy maleje bądź zupełnie zanika. Przykładowe zagrożenia przedstawiono w tabeli nr 3;
9) **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów; ryzyko jest mierzone skutkami oraz prawdopodobieństwem wystąpienia.
10) **istotności ryzyka** – należy przez to rozumieć iloczyn prawdopodobieństwa wystąpienia ryzyka oraz potencjalnego skutku jego wystąpienia.
11) **Urzędzie** – należy przez to rozumieć Urząd Gminy Markowa;
12) **Zasadach** – należy przez to rozumieć Zasady i tryb przeprowadzania analizy ryzyka przetwarzania danych osobowych w Urzędzie Gminy Markowa;
13) **Zespole** – należy przez to rozumieć pracowników wyznaczonych przez Wójta Gminy, którzy wraz z nim jako Administratorem oraz IOD przeprowadzą analizę ryzyka w Urzędzie Gminy Markowa.

§ 2

1. Celem opracowanych Zasad jest ustalenie metodyki zarządzania ryzykiem bezpieczeństwa danych osobowych przetwarzanych w Urzędzie z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą.
2. Zasady określają sposób przeprowadzania i dokumentowania procesu szacowania ryzyka.

§ 3

1. Wynikiem przeprowadzonego procesu szacowania ryzyka jest określenie adekwatnych do zagrożeń i prawdopodobieństwa ich wystąpienia, środków technicznych i organizacyjnych, niezbędnych do osiągnięcia akceptowalnego poziomu ryzyka.
2. Zarządzanie ryzykiem ma na celu działania podnoszące poziom bezpieczeństwa ochrony danych osobowych przetwarzanych w Urzędzie uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których dane dotyczą. Oznacza to między innymi, że dane osobowe przetwarzane w Urzędzie powinny być zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem. Czynności podejmowane w ramach tych działań oraz zastosowane środki techniczne i organizacyjne będą zależne od środowiska, w jakim dane są przetwarzane.
3. Pojęcie ochrony danych należy rozpatrywać pod kątem ich poufności, integralności i dostępności. Wymienione właściwości, polegają odpowiednio na:
   1) poufność – zapewnieniu, że informacja nie jest udostępniania lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
   2) integralność – zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) dostępność – zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
4. Poprzez zarządzanie ryzykiem bezpieczeństwa ochrony danych osobowych należy rozumieć działania polegające na:
   1) identyfikacji procesów;
   2) określeniu zagrożeń;
   3) szacowaniu ryzyka;
   4) postępowaniu z ryzykiem;
   5) akceptowaniu ryzyka;
   6) monitorowaniu ryzyka;
   7) informowaniu o ryzyku

w odniesieniu do zidentyfikowanego procesu przetwarzania danych osobowych.

§ 4

Monitorowanie procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w Urzędzie Gminy Markowa i dokumentowanie tych czynności jest elementem wywiązania się z ciążącego na Administratorze Danych Osobowych obowiązku zapewnienia przetwarzania zgodnego z ogólnym rozporządzeniem o ochronie danych.

§ 5

1. Wójt Gminy Markowa zapewnia warunki niezbędne do prawidłowego funkcjonowania procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w Urzędzie.
2. Cały proces szacowania ryzyka ochrony danych osobowych przetwarzanych w Urzędzie koordynuje i nadzoruje IOD.
3. Kierownicy zapewniają i odpowiadają za systematyczną identyfikację procesów i zagrożeń.

§ 6

1. Na analizę ryzyka składa się: szacowanie ryzyka, postępowanie z ryzykiem oraz akceptowanie ryzyka.
2. Szacowanie ryzyka ma na celu określenie co może się zdarzyć (kiedy, gdzie, jak i dlaczego) oraz jak dotkliwe straty mogą powstać i polega na:
   1) identyfikowaniu zagrożeń;
   2) analizie ryzyka;
   3) ocenie ryzyka.
3. W ramach identyfikacji ryzyka określany jest:
   1) kontekst;
   2) identyfikacja aktywów;
   3) identyfikacja zagrożeń dla aktywów;
   4) identyfikacja istniejących zabezpieczeń;
   5) identyfikacja podatności;
   6) identyfikacja następstw – skutków tj. np.:
      - utrata kontroli nad własnymi danymi osobowymi;
      - ograniczenie praw;
      - dyskryminacja;
      - kradzież lub sfałszowanie tożsamości;
      - strata finansowa;
      - nieuprawnione odwrócenie pseudonimizacji;
      - naruszenie dobrego imienia;
      - naruszenie poufności danych osobowych chronionych tajemnicą zawodową;
      - wszelkie inne znaczne szkody gospodarcze lub społeczne;
4. Posiadając zidentyfikowane aktywa, zagrożenia oraz zastosowane zabezpieczenia można przeprowadzić identyfikację podatności na urzeczywistnienie się określonych zagrożeń. Istotne jest, że samo istnienie podatności nie powoduje jeszcze szkody. Jej powstanie jest możliwe dopiero po zmaterializowaniu się zagrożenia, które wykorzysta daną podatność. Analiza podatności dotyczy aktywów podstawowych – przetwarzanych danych i zastosowanych do przetwarzania procesów – jak i wspierających – sprzęt, oprogramowanie, sieć komputerowa, pracownicy, siedziba, organizacja.
5. W przypadku aktywów, jakim jest zbiór danych osobowych, podatnością może być sam fakt wykorzystania danych w innym celu niż zamierzony.
6. Podczas identyfikacji następstw należy przygotować zestawienie aktywów i ich podatności, a następnie zagrożeń które mogą wykorzystać poszczególne podatności oraz przedstawić jego skutki.

7. Dokonanie analizy ryzyka polega na:
   1) oszacowaniu następstw ze szczególnym uwzględnieniem możliwości naruszenia praw lub wolności osób fizycznych;
   2) oszacowaniu prawdopodobieństwa incydentu;
   3) określeniu poziomu ryzyka.
8. Oceniając następstwa urzeczywistnienia się zagrożeń, w przypadku danych osobowych, należy uwzględnić, poza innymi czynnikami, także dotkliwe, przewidziane w RODO kary finansowe, które mogą być nakładane przez organ nadzorczy na administratora i podmioty przetwarzające w przypadku niewywiązywania się przez nie z nałożonych obowiązków właściwej ochrony danych. Szacowanie następstw dla określonych zagrożeń powinno uwzględniać zarówno materialny, jak i niematerialny charakter.
9. Przyjmuje się, że zasadniczym rodzajem reakcji na ryzyko jest działanie lub przeniesienie ryzyka. Przeniesienie oznacza przekazanie ryzyka podmiotowi zewnętrznemu, np. ubezpieczenie budynku będącego siedzibą Urzędu. Działanie może obejmować w szczególności ustanowienie nowych lub zintensyfikowanie istniejących mechanizmów kontroli, a także działania o innym charakterze (np. przeszkolenie pracowników, wprowadzenie zmian organizacyjnych, wystąpienie o dodatkowe środki finansowe, wprowadzenie dodatkowych wymogów informacyjnych, podjęcie lub nasilenie działań kontrolnych itp.).

§ 7

Proces szacowania ryzyka w sposób określony powyżej, kończy jego ocena i ustalenie planu postępowania z ryzykiem.

§ 8

Na potrzeby przeprowadzenia analizy ryzyka przyjęto następujące kryteria oceny poszczególnych jej elementów:

1) Szacowanie skutków zmaterializowania się ryzyka określono w skali pięciostopniowej, gdzie 5 oznacza bardzo wysoki skutek natomiast 1 bardzo niski. Przedmiotowe kryteria przedstawiono w tabeli nr I.
2) Szacowanie prawdopodobieństwa wystąpienia ryzyka określono w skali pięciostopniowej, gdzie 5 oznacza bardzo wysokie prawdopodobieństwo wystąpienia ryzyka natomiast 1 rzadkie prawdopodobieństwo. Przedmiotowe kryteria przedstawiono w tabeli nr II.
3) Poziom istotności ryzyka będzie obliczany według wzoru: Ryzyko (R) = skutek (S) x prawdopodobieństwo (P). Na potrzeby analizy przyjęto, że wynik od 1 – 4 oznacza poziom niski, 5 – 10 poziom średni, 12 – 16 poziom wysoki, 20 – 25 poziom krytyczny. Skalowanie poziomu ryzyka przedstawiono w tabeli nr III.
4) Przyjmuje się, że poziom ryzyka średni i powyżej nie jest akceptowalny. Kryteria akceptacji ryzyka przedstawia tabela nr IV.

§ 9

W celu przeprowadzenia i udokumentowania analizy ryzyka wykorzystana zostanie tabela, której wzór stanowi załącznik nr 1 niniejszych Zasad.

§ 10

1. Po przeprowadzonej analizie ryzyka, w razie stwierdzenia, iż istotność ryzyka przekracza poziom akceptowalny Administrator wdraża plan naprawczy, w którym określa warianty postępowania z ryzykiem oraz działania mające na celu zmniejszenie istotności ryzyka do poziomu akceptowalnego.
2. Podstawowymi wariantami postępowania z ryzykiem jest:
   1) Modyfikowanie (redukowanie, minimalizacja) ryzyka – wprowadzanie nowych rozwiązań technicznych, osobowych itp.,
   2) Akceptacja ryzyka – pozostawienie na obecnym poziomie,
   3) Unikanie ryzyka – zaprzestanie działań powodujących ryzyko,
   4) Dzielenie (przeniesienie) ryzyka – scedowanie ryzyka poprzez np. ubezpieczenie obiektów, sprzętu itp.

§ 11

Administrator na bieżąco ocenia skuteczność podejmowanych działań w celu zmniejszenia ryzyka do akceptowalnego poziomu.

§ 12

Analiza ryzyka jest przeprowadzana przynajmniej raz w roku lub w przypadku wprowadzenia zmian organizacyjnych, technicznych oraz czynności mogących mieć wpływ na pojawienie się nowych zagrożeń.

§ 13

W przypadku ujawnienia ryzyka nieakceptowanego Administrator po konsultacji z IOD podejmuje natychmiastowe działania zmierzające do przywrócenia jego akceptowalności.

WÓJT
Mirosław Mac

Tabela nr 1.

Przykładowe zidentyfikowane aktywa	
Podstawowe	**Wspierające**
• Procesy przetwarzania danych • Informacje	• Siedziba • Struktura organizacyjna • Personel • Sprzęt • Sieć • Oprogramowanie

Tabela nr 2.

Przykłady typowych podatności w zarządzaniu bezpieczeństwem informacji.
• niskie płace, • niezadowolenie z wykonywanej pracy, • wysoka rotacja pracowników, • usytuowanie budynku na terenie zalewowym, • brak procedur postępowania z urządzeniami mobilnymi, • brak polityki haseł, • brak szkoleń dla pracowników, • brak wylogowywana się podczas opuszczania stanowiska pracy, etc.

Tabela nr 3.

Przykłady typowych zagrożeń w zarządzaniu bezpieczeństwem informacji.
• pożar, zalanie, powódź; • awaria systemu klimatyzacji; • utrata dostaw prądu; • kradzież, zagubienie urządzenia; • awaria urządzenia; • błąd personelu/użytkownika; • kradzież dokumentów; • ujawnienie lub udostępnienie danych osobom nieupoważnionym; • nieautoryzowany dostęp do systemu; • nieautoryzowana modyfikacja danych (systemowo lub tradycyjnie); etc.

Tabela nr I.

Szacowanie skutków zmaterializowania się ryzyka			
Skutek	**Poziom**	**Wartość/Strata finansowa**	**Wpływ na prawa i wolności osoby fizycznej**
Bardzo wysoki	5	powyżej 500 tys. zł	Bardzo wpływa (bardzo często dochodzi do naruszeń praw i wolności)
Wysoki	4	100 – 500 tys. zł	Znacząco wpływa (często dochodzi do naruszeń praw i wolności)
Średni	3	50 – 100 tys. zł	Wpływa (sporadycznie dochodzi do naruszeń praw i wolności)
Niski	2	5 – 50 tys. zł	Częściowo wpływa (może dojść do naruszeń praw i wolności)
Bardzo niski	1	poniżej 5 tys. zł	Brak wpływu

Tabela nr II.

Szacowanie prawdopodobieństwa wystąpienia ryzyka		
Prawdopodobieństwo	**Poziom**	**Opis prawdopodobieństwa**
Bardzo wysokie	5	Występuje co najmniej raz na tydzień lub częściej
Prawdopodobne	4	Występuje co najmniej raz na miesiąc
Możliwe	3	Występuje co najmniej raz na 3 miesiące (kwartał)
Mało prawdopodobne	2	Występuje co najmniej raz na 6 miesięcy
Rzadkie	1	Występuje raz w roku lub wcale

Tabela nr III.

			SKUTEK				
	S x P = R		Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
PRAWDOPODOBIEŃSTWO	Bardzo wysokie	5	5 Ś	10 Ś	15 W	20 K	25 K
	Prawdopodobne	4	4 N	8 Ś	12 W	16 W	20 K
	Możliwe	3	3 N	6 Ś	6 Ś	12 W	15 W
	Mało prawdopodobne	2	2 N	4 N	6 Ś	8 Ś	10 Ś
	Rzadkie	1	1 N	2 N	3 N	4 N	5 Ś

Tabela nr IV.

Kryteria akceptacji ryzyka i możliwe działania		
Poziom ryzyka	**Akceptowalny ? TAK/NIE**	**Opis podejmowanych działań**
Niski (N)	TAK	Okresowe monitorowanie
Średni (Ś)	NIE	Działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Wysoki (W)	NIE	Wymaga stałego monitorowania, działanie wymagane
Krytyczny (K)	NIE	Wymaga natychmiastowego działania

Załącznik nr 1 do Zasad i trybu przeprowadzania analizy ryzyka dla ochrony danych osobowych w Urzędzie Gminy Markowa

-Wzór- ANALIZA RYZYKA
Identyfikacja ryzyka i szacowanie ryzyka

L.p.	Aktywa/obszar	Zagrożenia	Podatności	Skutki utraty poufności, integralności i dostępności w odniesieniu do aktywów	Skutek	Prawdopodobieństwo	Poziom ryzyka	Postępowanie z ryzykiem (opis)