UCHWAŁA NR .....

RADY GMINY DĘBNICA KASZUBSKA

z dnia ..... 2024 r.

w sprawie przyjęcia Polityki bezpieczeństwa informacji Rady Gminy Dębnica Kaszubska

Na podstawie art. 18 ust. 2 pkt 15 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 1465 i 1572; z 2023 r. poz. 1688), art. 24 ust. 1, art. 32 ust. 1 i art. 37 ust. 1 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. Urz. UE. L. z 2016 r. nr 119 poz. 1; z 2018 r. nr 127 poz. 2; z 2021 nr 74 poz. 35) uchwala się, co następuje:

§ 1. Przyjmuje się Politykę bezpieczeństwa informacji Rady Gminy Dębnica Kaszubska, stanowiącą załącznik do niniejszej uchwały.

§ 2. Wyznacza się na Inspektora Ochrony Danych Osobowych Panią Katarzynę Jakubowską.

§ 3. Wykonanie uchwały powierza się Przewodniczącemu Rady Gminy.

§ 4. Uchwała wchodzi w życie z dniem podjęcia.

Załącznik do uchwały nr .....

Rady Gminy Dębnica Kaszubska

z dnia.....2024 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI RADY GMINY DĘBNICA KASZUBSKA

Rozdział 1.
Przepisy ogólne

§ 1. 1. Polityka Bezpieczeństwa Informacji, zwana dalej „Polityką", określa podstawowe zasady zarządzania bezpieczeństwem informacji przez Radę Gminy Dębnica Kaszubska, zwaną dalej „Radą".

2. Administratorem danych osobowych przetwarzanych przez radnych Rady jest Rada.

3. Zasady zarządzania bezpieczeństwem informacji w Radzie zostały opracowane zgodnie z obowiązującymi przepisami w oparciu o wymagania standardów w obszarze bezpieczeństwa informacji, w tym w szczególności:

1) Rozporządzeniem 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. z 2016 r. nr 119 poz. 1 z późn. zm.), zwanym dalej „RODO";
2) ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781), zwaną dalej „Ustawą";
3) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 z późn. zm.);
4) rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).

§ 2. Użyte w Polityce pojęcia oznaczają:

1) aktywa (zasoby) - wszystko, co stanowi wartość dla Rady i w związku z tym wymaga ochrony, w szczególności aktywa informacyjne (informacje) rozumiane jako wiedza, dane oraz wszelkie informacje, w szczególności dane osobowe;
2) bezpieczeństwo informacji - zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieautoryzowanym dostępem lub zmianą;
3) dane osobowe - dane, o których mowa w art. 4 pkt 1 RODO;
4) dostępność - właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu;
5) incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają bezpieczeństwu informacji oraz stwarzają znaczne prawdopodobieństwo utraty aktywów lub zakłócenia realizacji zadań;
6) integralność - właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
7) naruszenie ochrony danych osobowych - naruszenie, o którym mowa w art. 4 pkt 12 RODO;
8) podatność - słabość lub wrażliwość aktywa lub grupy aktywów w zakresie funkcjonowania Rady, która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki; podatność może dotyczyć, w szczególności sposobu zarządzania lub postępowania użytkownika, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego, niedoskonałości zabezpieczeń;
9) poufność - właściwość polegająca na tym, że informacja nie jest udostępniana, ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
10) przetwarzanie - operacja lub zestaw operacji, o których mowa w art. 4 pkt 2 RODO;

11) ryzyko - potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;

12) sytuacja awaryjna - zdarzenie, którego skutki powodują utratę ciągłości działania Rady;

13) sytuacja kryzysowa - niespodziewane i niepożądane zdarzenie lub seria zdarzeń związanych z bezpieczeństwem przetwarzania informacji, w szczególności w systemach teleinformatycznych, które mogą zakłócić lub zakłócają proces realizacji zadań Rady;

14) użytkownik - radny Rady;

15) zabezpieczenie - działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów;

16) zagrożenie - zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować naruszeniem integralności, dostępności, poufności informacji albo doprowadzić do szkody lub nieosiągnięcia celów Rady.

§ 3. Celem Polityki jest ustalenie warunków bezpieczeństwa danych osobowych, zapewniających ich przetwarzanie, w szczególności reguł zdefiniowanych w rozdziale II RODO, które określają:

1) zasadę zgodności z prawem, rzetelności i przejrzystości, zwłaszcza dla osoby, której dane dotyczą z zachowaniem praw tych osób w zakresie przetwarzania;

2) zasadę ograniczenia celu przetwarzania;

3) zasadę minimalizacji;

4) zasadę prawidłowości;

5) zasadę ograniczenia przechowywania;

6) zasadę poufności i integralności;

7) zasadę rozliczalności; co oznacza, że Administrator Danych Osobowych ma każdorazowo wykazać, że realizuje zasady wymienione w pkt 1-6 poprzez zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, które dane działania wykonał;

8) zasadę dostępności, co oznacza, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.

§ 4. 1. Polityką objęte są wszystkie dane osobowe wykorzystywane przez Radę, niezależnie od formy i nośnika przetwarzania lub dystrybucji (ustne, pisemne, wizyjne, nagrania audio i wideo), utrwalone na nośnikach elektronicznych, systemach komputerowych oraz wytworzone w dokumentach.

2. Przetwarzanie danych osobowych dokonuje się w celu realizacji obowiązku prawnego nałożonego na Radę.

3. Polityka ma zastosowanie do wszystkich radnych Rady i obejmuje zakresem nie tylko obszar Urzędu Gminy Dębnica Kaszubska, ale także miejsca i sytuacje, w których informacje związane z działalnością Rady są przetwarzane poza jego siedzibą, w szczególności w kontekście zdalnej pracy Rady.

4. Do przestrzegania Polityki zobowiązane są wszystkie osoby korzystające z zasobów Rady, w szczególności radni Rady.

5. Za zapoznanie z Polityką radnych odpowiada Przewodniczący Rady Gminy, zwany dalej Przewodniczącym Rady lub Przewodniczącym.

6. Osoby, o których mowa w ust. 4, zobowiązane są do złożenia oświadczenia o zapoznaniu się z treścią Polityki, zgodnie z wzorem stanowiącym załącznik nr 1 do Polityki.

Rozdział 2.
Zasady dotyczące bezpieczeństwa informacji

§ 5. 1. Polityka realizowana jest poprzez:

1) zapewnienie odpowiedniej jakości procesów przetwarzania danych osobowych, w szczególności skuteczności i adekwatności działania zabezpieczeń (lub ich grup) i środków chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania oraz sprawności i efektywności ich wykorzystywania;

2) ochronę fizyczną, techniczną i organizacyjną aktywów przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;

3) zabezpieczenie systemów teleinformatycznych eksploatowanych przez użytkowników przed zagrożeniami;

4) zapewnienie możliwości sprawnego odtworzenia aktywów w przypadku ich zniszczenia;

5) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;

6) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem danych osobowych;

7) zapewnienie użytkownikom szkoleń i innych akcji promocyjno-edukacyjnych z zakresu bezpieczeństwa danych osobowych;

8) zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w Polityce;

9) przestrzeganie zasad bezpieczeństwa danych osobowych, o których mowa w § 6.

2. Stosowanie zabezpieczeń lub ich grup powinno uwzględniać następujące zasady:

1) zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników analiz ryzyka bezpieczeństwa informacji;

2) zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji; w doborze zabezpieczeń należy kierować się w szczególności:

a) adekwatnością,

b) uwzględnieniem wyników szacowania ryzyka;

3) świadomość użytkowników w zakresie bezpieczeństwa informacji powinna być doskonalona, w szczególności poprzez szkolenia.

§ 6. 1. Stosuje się, w szczególności, następujące zasady bezpieczeństwa danych osobowych:

1) wiedzy koniecznej (ograniczonego dostępu do informacji) - użytkownicy posiadają dostęp tylko do tych danych osobowych, które są konieczne do realizacji powierzonych im zadań; zasada ta dotyczy w szczególności informacji wrażliwych; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, w szczególności informacji dostępnych publicznie;

2) indywidualnej odpowiedzialności - za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby; zasada ta dotyczy np. wydruków lub dokumentów elektronicznych;

3) dyskrecji, ograniczonego zaufania - wszelkie dane osobowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, np. informacji dostępnych publicznie;

4) nadzorowania dokumentów - wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych.

§ 7. 1. Na potrzeby funkcjonowania Rady użycza się radnym laptopy w celu wykonywania funkcji radnego.

2. Na laptopach instaluje się oprogramowanie antywirusowe oraz dokonuje się konfiguracji, która uniemożliwia instalację dodatkowego oprogramowania.

3. Urządzenie posiada wszystkie aplikacje niezbędne do właściwego realizowania obowiązków radnego, w tym oprogramowanie pozwalające odbierać pocztę elektroniczną.

4. Logowanie do laptopa oraz aplikacji wymaga podania indywidualnego kodu PIN lub hasła.

§ 8. Obowiązki użytkownika:

1) radni, wykonując mandat radnego, są zobligowani do korzystania z użyczonych laptopów;

2) radnym udostępniana jest służbowa poczta elektroniczna wyłącznie w celach wykonywania funkcji radnego; informacja o służbowym adresie e-mail jest jawna i dostępna na stronie BIP Urzędu Gminy Dębnica Kaszubska;

3) po pierwszym zalogowaniu do aplikacji lub poczty elektronicznej radny zobowiązany jest do dokonania zmiany hasła logowania; hasło składa się co najmniej z ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny;

4) radny jest zobowiązany zapewnić bezpieczeństwo danych osobowych i informacji prawnie chronionych tajemnicą, przesyłanych służbową pocztą elektroniczną;

5) radny jest zobowiązany do wykorzystywania metod kryptografii, takich jak szyfrowanie załączników do przesyłanej za pomocą służbowej poczty elektronicznej każdej informacji, zawierającej w szczególności:

a) dane osobowe,

b) tajemnice prawnie chronione.

Hasło niezbędne do odszyfrowania wysyłanej informacji za pomocą służbowej poczty elektronicznej, radny przekazuje adresatowi informacji odrębnym kanałem komunikacji;

6) radny jest zobowiązany do przechowywania dokumentów w odpowiednio zabezpieczonych meblach;

7) na czas nieobecności radnego dostęp do laptopa jest blokowany, a po zakończeniu pracy wyłączany;

8) zachowanie prywatności kont w systemach - każdy radny zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;

9) poufność haseł - każdy radny zobowiązany jest do zachowania poufności udostępnionych mu haseł i kodów dostępu;

10) zgłaszanie incydentów bezpieczeństwa informacji - radny ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu bezpieczeństwa informacji Przewodniczącemu oraz Inspektorowi Ochrony Danych;

11) ochrona nośników danych - dane na laptopach powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania;

12) przechowywanie danych osobowych przetwarzanych w formie papierowej lub elektronicznej przed dostępem osób nieupoważnionych.

Rozdział 3.
Odpowiedzialność i uprawnienia w zakresie bezpieczeństwa informacji

§ 9. 1. Właściwe zarządzanie bezpieczeństwem informacji w Radzie zapewnia wewnętrzna struktura organizacyjna, w której skład wchodzą:

1) Przewodniczący Rady Gminy;

2) Zastępcy Przewodniczącego Rady Gminy;

3) Inspektor Ochrony Danych;

4) radni;

5) pracownik ds. obsługi Rady Gminy.

2. Odpowiedzialność za bezpieczeństwo informacji w Radzie ponoszą wszystkie osoby, o których mowa w § 9 ust. 1, w zakresie odpowiednim do nałożonych na nich obowiązków, posiadanych uprawnień.

3. Inspektor Ochrony Danych przeprowadza szkolenie dotyczące bezpieczeństwa danych osobowych dla każdego użytkownika przed przystąpieniem do przetwarzania danych osobowych.

§ 10. Użytkownicy odpowiadają w szczególności za:

1) przestrzeganie Polityki;

2) ochronę aktywów, w zakresie swojej właściwości;

3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu;

4) zabezpieczanie informacji przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą;

5) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania funkcji radnego oraz po wygaśnięciu mandatu radnego;

6) przestrzegania zasad bezpiecznego ich przetwarzania, w tym w systemach teleinformatycznych;

7) zniszczenie posiadanych danych osobowych po wygaśnięciu mandatu radnego.

Rozdział 4.
Klasyfikacja informacji i zasady postępowania z informacjami

§ 11. 1. Przyjmuje się następującą klasyfikację informacji oraz ich oznaczenie:

1) informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych;

2) informacje przekazane Radzie, radnemu przez mieszkańca, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej naruszające dobra osobiste;

3) informacje publiczne - informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej;

4) informacje prawnie chronione – np. informacje przekazane Radzie przez kontrahenta, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa).

2. W Radzie funkcjonują następujące zbiory danych osobowych:

1) Rejestr skarg i wniosków;

2) Rejestr wnoszonych spraw zawierających petycje;

3) Obywatelska inicjatywa uchwałodawcza;

4) Wnioski i postulaty mieszkańców i innych podmiotów do Rady Gminy oraz spotkania z mieszkańcami i innymi podmiotami.

3. Upoważnienie do przetwarzania danych osobowych zawartych w ww. rejestrach posiadają wszyscy radni oraz pracownik ds. obsługi Rady Gminy Dębnica Kaszubska w Urzędzie Gminy Dębnica Kaszubska. Wzór upoważnienia dla pracowników stanowi załącznik nr 2 do Polityki.

4. Upoważnienie do przetwarzania danych osobowych wygasa z dniem wygaśnięcia mandatu radnego.

5. Zasady określone w rozdziale II RODO realizuje Przewodniczący Rady i Inspektor Ochrony Danych.

6. Rejestry czynności przetwarzania danych osobowych stanowi załącznik nr 3 do Polityki.

Rozdział 5.
Szacowanie ryzyka

§ 12. 1. Identyfikacja i analiza ryzyka polega na ustaleniu występującego lub możliwego do wystąpienia zdarzenia, które stanowi lub może stanowić zagrożenie dla operacji przetwarzania danych osobowych, w szczególności naruszenia praw i wolności osób.

2. W obszarze bezpieczeństwa informacji identyfikacja i analiza ryzyka jest obligatoryjna i przeprowadza się ją cykliczne, nie rzadziej niż raz w roku.

3. Inspektor Ochrony Danych przedstawia Radzie do dnia 31 marca każdego roku ogólną ocenę bezpieczeństwa przetwarzania danych osobowych w Radzie.

§ 13. Przeprowadzając analizę ryzyka należy uwzględnić:

1) przyczyny występowania ryzyka (czynniki ryzyka);

2) prawdopodobieństwo wystąpienia ryzyka;

3) możliwe skutki wystąpienia ryzyka;

4) poziom ryzyka.

§ 14. 1. Stopień określenia prawdopodobieństwa wystąpienia ryzyka ustala się w skali punktowej za pomocą przyjętych wartości:

1) l - prawie niemożliwe - zdarzenie może zaistnieć jedynie w wyjątkowych okolicznościach, w ocenie do 20% szans zdarzenie może wystąpić raz na 5 lat, a najprawdopodobniej w ogóle nie zaistnieje, nie wystąpiło dotychczas w działalności Rady;

2) 2 - małe - w ocenie od 21% do 40% szans, zdarzenie może zaistnieć raz na 3 lata w wyniku zbiegu niezwykłych okoliczności;

3) 3 - średnie - w niektórych przypadkach, od 41% do 60% szans zdarzenie może mieć miejsce, ale dotyczy tylko niektórych spraw;

4) 4 - duże - zaistnienie zdarzenia jest bardzo prawdopodobne - w ocenie od 61% do 80%, szansa wystąpienia istnieje co najmniej raz w roku;

5) 5 - prawie pewne - przewiduje się, że w ocenie od 81% do 100% zdarzenie wystąpi regularnie co miesiąc i dotyczy wszystkich lub prawie wszystkich spraw.

2. Stopień określenia potencjalnych skutków ryzyka ustala się, biorąc pod uwagę wszystkie istniejące rozwiązania uznawane za funkcjonujące mechanizmy kontrolne w działalności Rady. Ocena następuje w skali punktowej za pomocą przyjętych wartości:

1) 1 - nieznaczny - zdarzenie ma znikomy wpływ na utratę poufności - nie wiąże się z odpowiedzialnością karną lub cywilno-prawną użytkowników odpowiedzialnych za zapewnienie ochrony danym osobowym i w efekcie nie narusza praw i wolności osób, których dane dotyczą;

2) 2 - mały - zdarzenie ma mały wpływ na utratę poufności - nie wiąże się z odpowiedzialnością karną lub cywilno-prawną użytkowników odpowiedzialnych za zapewnienie ochrony danym osobowym i w efekcie nie narusza praw i wolności osób, których dane dotyczą;

3) 3 - średni - zdarzenie ma umiarkowany wpływ na utratę poufności - nie wiąże się z odpowiedzialnością karną, ale może wiązać się z odpowiedzialnością cywilno-prawną użytkowników odpowiedzialnych za zapewnienie ochrony danym osobowym i w efekcie narusza praw i wolności osób, których dane dotyczą;

4) 4 - poważny - zdarzenie ma poważny wpływ na utratę poufności - może wiązać się z odpowiedzialnością karną lub cywilno-prawną użytkowników odpowiedzialnych za zapewnienie ochrony danym osobowym i w efekcie narusza praw i wolności osób, których dane dotyczą;

5) 5 - katastrofalne - zdarzenie ma katastrofalny wpływ w zakresie utraty poufności - wiąże się z odpowiedzialnością karną lub cywilno-prawną użytkowników odpowiedzialnych za zapewnienie ochrony danym osobowym i w efekcie narusza prawa i wolności osób, których dane dotyczą.

§ 15. 1. Na podstawie przeprowadzonej analizy prawdopodobieństwa i skutków ryzyka Przewodniczący dokonuje punktowej oceny istotności ryzyka, co oznacza zdefiniowanie poziomu ryzyka.

2. Istotność ryzyka jest iloczynem prawdopodobieństwa wystąpienia ryzyka i potencjalnych skutków ryzyka.

3. Ustalona istotność ryzyka umożliwia określenie jego poziomu wg stopni:

1) niskie - w skali od l do 6;

2) średnie - w skali od 8 do 12;

3) wysokie - w skali od 15 do 25, jak na przywołanej matrycy oceny ryzyka.

PRAWDOPODOBIEŃSTWO/ SKUTEK	PRAWIE MOŻLIWE	MAŁE	ŚREDNIE	DUŻE	PRAWIE PEWNE

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

§ 16. 1. W działalności Rady uznaje się za akceptowalne ryzyko określone na poziomie niskim, dla którego nie wymaga się planowania i wdrażania dodatkowych metod postępowania, w tym mechanizmów kontrolnych.

2. W stosunku do ryzyka określonego na poziomie średnim, Przewodniczący decyduje o przedstawieniu propozycji w sprawie wdrożenia dodatkowych mechanizmów kontrolnych, oceniając zasadność i możliwość ich wdrożenia oraz biorąc pod uwagę koszt wdrożenia działań do korzyści możliwych do uzyskania w wyniku tych działań, w taki sposób, który pozwoli zminimalizować ryzyko do poziomu niskiego lub je w ogóle wyeliminować.

3. W stosunku do ryzyka określonego na poziomie wysokim, Przewodniczący jest zobowiązany zaproponować wdrożenie dodatkowych mechanizmów kontrolnych/działań zapobiegawczych, oceniając zasadność i możliwość ich wdrożenia oraz biorąc pod uwagę koszt wdrożenia działań do korzyści możliwych do uzyskania W wyniku tych działań, W taki sposób, który pozwoli zminimalizować ryzyko do poziomu niskiego lub je w ogóle wyeliminować.

4. Karty identyfikacji, analizy i oceny ryzyka stanowią załącznik nr 4 do Polityki.

5. Przewodniczący corocznie, w pierwszym kwartale roku, dokonuje przeglądu ryzyka. W przypadku, gdy wyniki przeglądu są takie same, jak dotychczas ustalony poziom ryzyka Przewodniczący informuje o tym Radę.

6. W przypadku:

1) nieskuteczności wdrożonych mechanizmów kontrolnych (działań zapobiegawczych), które skutkowały brakiem osiągnięcia celu lub naruszeniem danych osobowych;
2) zmiany warunków, mających znaczenie dla prawdopodobieństwa i skutków wystąpienia ryzyka, Przewodniczący dokonuje ponownej identyfikacji, analizy i oceny ryzyka, a ustalenia przekazuje Radzie.

Rozdział 6.
Postanowienia końcowe

§ 17. W terminie 14 dni od dnia wejścia w życie Polityki osoby, o których mowa w § 4 ust. 4 mają obowiązek zapoznać się z jej treścią.

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji

Rady Gminy Dębnica Kaszubska

OŚWIADCZENIE O ZAPOZNANIU SIĘ Z POLITYKĄ BEZPIECZEŃSTWA INFORMACJI RADY GMINY DĘBNICA KASZUBSKA

Niniejszym oświadczam, że zapoznałam/em się z Polityką Bezpieczeństwa Informacji Rady Gminy Dębnica Kaszubska i zobowiązuję się do przestrzegania zawartych w niej zasad. Mam na uwadze zachowanie w tajemnicy informacji prawnie chronionych, do których mam lub będę miał/a dostęp w związku z wykonywaniem przeze mnie obowiązków, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji Rady Gminy Dębnica Kaszubska jest zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub cywilno-prawną na zasadach i w trybie przewidzianym w przepisach prawa.

/_____/

Data i podpis

Załącznik nr 2 do Polityki Bezpieczeństwa Informacji

Rady Gminy Dębnica Kaszubska

RADA GMINY

DĘBNICA KASZUBSKA

Dębnica Kaszubska, dnia .....r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniam Pana/Panią …….. do przetwarzania wszystkich danych osobowych zawartych w następujących zbiorach administrowanych przez Radę Gminy:

1) Rejestr skarg i wniosków;
2) Rejestr wnoszonych spraw zawierających petycje;
3) Obywatelska inicjatywa uchwałodawcza;
4) Wnioski i postulaty mieszkańców i innych podmiotów do Rady Gminy oraz spotkania z mieszkańcami i innymi podmiotami.

Jednocześnie zobowiązuję Pana/Panią do przetwarzania danych osobowych zgodnie z Polityką bezpieczeństwa informacji Rady Gminy Dębnica Kaszubska oraz powszechnie obowiązującymi przepisami prawa.

Upoważnienie jest ważne do odwołania.

Osoba upoważniona do przetwarzania danych osobowych, zobowiązana jest do zachowania ich w tajemnicy, również po ustaniu zatrudnienia jak i do zachowania w tajemnicy informacji o ich zabezpieczeniu.

/_____/

Podpis Przewodniczącego Rady Gminy

/_____/

Data i podpis osoby upoważnionej

Załącznik nr 3 do Polityki Bezpieczeństwa Informacji

Rady Gminy Dębnica Kaszubska

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Administrator Danych Osobowych: Rada Gminy Dębnica Kaszubska.

Dane kontaktowe: Urząd Gminy Dębnica Kaszubska (76-248), ul. ks. Antoniego Kani 16A, tel. 690 820 341, fax. 59 813 16 23.

Inspektor Ochrony Danych: Katarzyna Jakubowska tel. 693 064 318 e-mail: iod@debnicakaszubska.eu

<table>
<tr><td>l.</td><td>NAZWA ZBIORU DANYCH</td><td colspan="4"></td></tr>
<tr><td>2.</td><td>NAZWA INFORMACJI</td><td colspan="4">Akta sprawy:</td></tr>
<tr><td>3.</td><td>KLASA INFORMACJI
(zakres przetwarzanych danych)</td><td colspan="4">Dane osobowe zwykła:
……
W przypadku wyrażenia zgody na przetwarzanie danych – dane osobowe szczególnych kategorii:
……..</td></tr>
<tr><td>4.</td><td>OPIS KATEGORII OSÓB, KTÓRYCH DANE DOTYCZĄ</td><td colspan="4"></td></tr>
<tr><td>5.</td><td>ŹRÓDŁO POZYSKANIA INFORMACJI
(od osoby fizycznej – właściciela danych)</td><td colspan="4"></td></tr>
<tr><td rowspan="4">6.</td><td colspan="5">PODSTAWA PRZETWARZANIA DANYCH</td></tr>
<tr><td colspan="5">Zgoda osoby fizycznej (art. 6 ust. 1 lit. a)</td></tr>
<tr><td colspan="5">Realizacja obowiązku prawnego (art. 6 ust. 1 lit. c)</td></tr>
<tr><td colspan="5">Wykonanie zadania realizowanego w interesie publicznym lub sprawowania władzy publicznej powierzonej administratorowi - (art. 6 ust. 1 lit. e)</td></tr>
<tr><td>7.</td><td colspan="5">CEL</td></tr>
<tr><td rowspan="5">8.</td><td colspan="5">KATEGORIA ODBIORCÓW</td></tr>
<tr><td rowspan="2">Przewodniczący Rady Gminy</td><td colspan="2">Sposób przetwarzania (uprawnienia osób przetwarzających informacje)</td><td>Archiwizowanie</td><td>Rodzaj systemu/programu</td></tr>
<tr><td>Elektronicznie</td><td>Papierowo</td><td></td><td></td></tr>
<tr><td>Radni</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Pracownicy jednostek organizacyjnych upoważnionych do załatwienia spraw</td><td></td><td></td><td></td><td></td></tr>
<tr><td>9.</td><td>STOSOWANE SPOSOBY ZABEZPIECZENIA DOSTĘPU DO INFORMACJI
(opis technicznych i organizacyjnych środków bezpieczeństwa)</td><td colspan="4"></td></tr>
<tr><td>10.</td><td>PLANOWANY TERMIN USUNIĘCIA DANYCH</td><td colspan="4"></td></tr>
<tr><td>11.</td><td>INFORMACJE O PRZEKAZANIU DANYCH</td><td colspan="4">Dane nie są przekazywane do państwa trzeciego lub organizacji międzynarodowej</td></tr>
</table>

	(do państwa trzeciego lub organizacji międzynarodowej)	

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji

Rady Gminy Dębnica Kaszubska

KARTA IDENTYFIKACJI, ANALIZY I OCENY RYZYKA

I. ANALIZA I OCENA RYZYKA DLA PRZETWARZANIA DANYCH OSOBOWYCH	
Zbiór danych	
Cel przetwarzania danych osobowych	
Miernik	
Stosowane sposoby zabezpieczeń – mechanizmy kontrolne	
Ryzyko dla przetwarzania danych	
Przyczyny ryzyka:	
Prawdopodobieństwo wystąpienia ryzyka utraty poufności (w skali 1-5)	- pkt
Skutek ryzyka utraty poufności (w skali 1-5)	- pkt
POZIOM RYZYKA (iloraz prawdopodobieństwa i skutku utraty poufności)	- pkt

Data podpis Przewodniczącego Rady Gminy

II. PROPOZYCJA USTALENIA I WDROŻENIA DODATKOWYCH MECHANIZMÓW KONTROLNYCH DLA PRZETWARZANIA DANYCH OSOBOWYCH

Data i podpis Inspektora Ochrony Danych

III. DECYZJA PRZEWODNICZĄCEGO RADY GMINY

Data podpis Przewodniczącego Rady Gminy

IV. PONOWNA ANALIZA I OCENA RYZYKA (przeprowadzona dla przetwarzanych danych, dla których poziom ryzyka był ustalony średni lub wysoki- po wdrożeniu dodatkowych mechanizmów kontrolnych)	
Prawdopodobieństwo wystąpienia ryzyka utraty poufności (w skali 1-5)	- pkt
Skutek ryzyka utraty poufności (w skali 1-5)	- pkt
POZIOM RYZYKA (iloraz prawdopodobieństwa i skutku utraty poufności)	- pkt

Data podpis Przewodniczącego Rady Gminy

V. POTWIERDZENIE PUNKTOWEJ WERYFIKACJI – AKCEPTACJA OCENY RYZYKA I WDROŻENIA DODATKOWYCH MECHANIZMÓW KONTROLNYCH

Data i podpis Inspektora Ochrony Danych

VI. DECYZJA PRZEWODNICZĄCEGO RADY GMINY PO WERYFIKACJI

Data podpis Przewodniczącego Rady Gminy

Uzasadnienie

Zgodnie z art. 4 pkt 7 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 (ogólnego rozporządzenia o ochronie danych) (Dz. Urz. UE. L. z 2016 r. nr 119 poz. 1 z późn. zm.), zwanym dalej „RODO", administratorem danych osobowych jest „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych". Rada Gminy Dębnica Kaszubska jest administratorem danych w zakresie spraw rozstrzyganych na podstawie przepisów ustawy o samorządzie gminnym, o petycjach oraz Kodeksu postępowania administracyjnego.

W Radzie Gminy funkcjonują następujące zbiory danych osobowych:

1) Rejestr skarg i wniosków;

2) Rejestr wnoszonych spraw zawierających petycje;

3) Obywatelska inicjatywa uchwałodawcza;

4) Wnioski i postulaty mieszkańców i innych podmiotów do Rady Gminy oraz spotkania z mieszkańcami i innymi podmiotami.

Z uwagi na przetwarzanie danych osobowych przez radę oraz poszczególnych radnych Rady Gminy Dębnica Kaszubska istnieje konieczność respektowania zasad wynikających z przepisów o ochronie danych osobowych, w tym zasad określonych w art. 24 ust. 1 oraz art. 32 ust. 1 i 2 RODO. Natomiast w myśl art. 37 ust. 1 RODO administrator danych osobowych zobowiązany jest do wyznaczenia inspektora ochrony danych osobowych. Inspektor ochrony danych osobowych jest wyznaczany na podstawie kwalifikacji zawodowej, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO. Biorąc powyższe pod uwagę opracowanie Polityki bezpieczeństwa informacji Rady Gminy Dębnica Kaszubska oraz wyznaczenie Inspektora ochrony danych osobowych jest uzasadnione.

Podjęcie uchwały nie wywoła skutków finansowych.