URZĄD GMINY I MIASTA
59-623 LUBOMIERZ
Pl. Wolności 1
tel. (075) 78 33 166, 78 33 151
fax (075) 78 33 167 NIP 616-14-47-152

Polityka Ochrony Danych Osobowych w Urzędzie Gminy i Miasta Lubomierz z siedzibą Pl. Wolności 1, 59-623 Lubomierz

I. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora Danych, którym jest Burmistrz Gminy i Miasta Lubomierz, wykonujący swoje zadania przy pomocy Urzędu Gminy i Miasta Lubomierz, w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

II. Inwentaryzacja danych

1. Dane osobowe wymagające ochrony administrator danych opracował w postaci papierowej, stanowiącej załącznik nr 1 do Polityki Ochrony Danych jako wykaz zbiorów.
2. Wykaz obejmuje nazwę zbioru, zakres przetwarzania danych, system danych tradycyjny lub informatyczny, zabezpieczenia i lokalizację.
3. W Urzędzie została opracowana Polityka Zarządzaniem ryzykiem w przetwarzaniu Danych Osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia.
4. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował analizę oceny ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

III. Zapewnienie o przetwarzania danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:

   1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;
   2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;

3) Administrator przechowuje dane osobowe przez konkretnie określony czas, z uwzględnieniem zasad określonych w przepisach prawa i w czasie określonym przepisami prawa;
4) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12, 13, 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym";
5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji Inspektora Ochrony Danych i przekazano im dane kontaktowe;
6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

2. Potwierdzenie przetwarzania danych osobowych zgodnie z prawem znajduje się w **załączniku nr 1** – Wykaz Zbiorów Danych Osobowych.

3. Wzór klauzuli informacyjnej znajduje się w **załączniku nr 2** – Klauzula Informacyjna.

IV. Polecenie-Upoważnienie

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.

2. Każda osoba upoważniona może przetwarzać dane wyłącznie na Polecenie Administratora lub na podstawie przepisu prawa (art. 29 RODO).

3. Upoważnienia nadawane są do zbiorów przez Burmistrza lub upoważnionego pracownika jako reprezentanta Administratora Danych. Polecenia-Upoważnienia określają zakres operacji na danych.

4. Upoważnienia nadawane są w formie Polecenie-Upoważnienie, wg wzoru **załącznik nr 4.**

5. Administrator Danych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych, **załącznik nr 3** - Ewidencja osób upoważnionych.

V. Procedura analizy ryzyka i ocena skutków

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zdarzenia, skutku, reakcji, działania i właścicielu ryzyka (stanowiska pracy).
3. W Urzędzie Gminy i Miasta Lubomierz stosuje się procedurę zarządzania ryzykiem zalecaną przez metodologię PRINCE 2, która wykorzystuje procedurę M_o_R (Management of Risk) obejmującą pięć następujących kroków:

   1) Identyfikuj
   2) Oceniaj
   3) Planuj
   4) Wdrażaj
   5) Komunikuj

VI. Instrukcja postępowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, szafek, biurek).

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator Danych lub Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
2) proponuje ewentualne działania dyscyplinarne;
3) proponuje działania na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – **załącznik nr 5** – Raport naruszeń oraz **załącznik nr 6** Formularz rejestracji incydentu.

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

VII. Regulamin Ochrony Danych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania - **załącznik nr 7** – Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – **załącznik nr 8** Oświadczenie.

VIII. Procedura przywracania dostępności danych osobowych

Zgodnie z art. 32 RODO, Administrator Danych powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator Danych wdrożył odpowiednie procedury w celu zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich, za które odpowiada Informatyk.

IX. Wykaz zabezpieczeń

1. Administrator w wykazie zbiorów wprowadza wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych .

2. W wykazie wskazano stosowane zabezpieczenia fizyczne jako środki organizacyjne oraz zabezpieczenia informatyczne jako środki techniczne.

X. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO oraz innymi przepisami związanymi z ochroną danych osobowych w tym przepisami i procedurami wewnętrznymi.

2. Za przeprowadzenie szkolenia odpowiada Administrator Danych.

3. Szkolenie prowadzi Inspektor Ochrony Danych lub podmiot zewnętrzny specjalizujący się w ochronie danych osobowych.

4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

5. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

BURMISTRZ
Gminy i Miasta Lubomierz
Wiesław Ziółkowski

Polityka Zarządzania Ryzykiem w procesie przetwarzania danych osobowych w Urzędzie Gminy i Miasta Lubomierz

---

Rozdział 1
Postanowienia ogólne

§ 1.1. Ilekroć w dokumencie jest mowa o:

1) **administratorze danych** – należy przez to rozumieć Burmistrza Gminy i Miasta Lubomierz, wykonującego swoje zadania przy pomocy Urzędu Gminy i Miasta Lubomierz;

2) **aktywach** – należy przez to rozumieć środki materialne i niematerialne mające wpływ na przetwarzanie danych;

3) **procesie przetwarzania danych** – należy przez to rozumieć zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych w celu określonego celu przetwarzania;

4) **operacji przetwarzania danych** – należy przez to rozumieć każdą czynność wykonywaną na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawniane poprzez wysłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

5) **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;

6) **zarządzaniu ryzykiem** – należy przez to rozumieć realizowany przez administratora danych osobowych proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki;

7) **mapie ryzyka** – jest to tabela (macierz) odzwierciedlająca ocenę siły oddziaływania i prawdopodobieństwo wystąpienia zidentyfikowanego ryzyka w Urzędzie;

8) **ocenie ryzyka** – należy przez to rozumieć czynność polegającą na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie projektowania systemu bezpieczeństwa danych;

9) **kryteriach akceptacji ryzyka** – są to kryteria, które określają dopuszczalność ryzyka, zdefiniowane poprzez wartość progową. Istotność ryzyka określamy jako iloczyn danego prawdopodobieństwa i danego wpływu, co w konsekwencji określa nam poziom ryzyka czy też poziom zagrożenia.

10) **rejestrze ryzyk** – należy przez to rozumieć dokument odzwierciedlający przeprowadzoną identyfikację i analizę ryzyk, a także przyjętą reakcję na ryzyko;

11) **bezpieczeństwie informacji** – należy przez to rozumieć zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

12) **zdarzeniu związanym z bezpieczeństwem danych** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych;

13) **incydencie** związanym z bezpieczeństwem danych – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne zakłócenia zadań i zagrażają bezpieczeństwu danych;

14) **zagrożeniu** – są to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

15) **podatności** – jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki;

16) **dostępności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

17) **integralności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

18) **poufności** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

19) **informatycznym nośniku danych** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

20) **zasobach systemu teleinformatycznego** - należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

§ 2. Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych, zwana dalej „polityką zarządzania ryzykiem", obejmuje:

1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
2) zasady i tryb identyfikacji ryzyka;
3) zasady i tryb dokonywania analizy ryzyka;
4) zasady określania właściwej reakcji na ryzyko.

§ 3. Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich stanowisk pracy w Urzędzie.

§ 4. Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych w § 2.

§ 5. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:

1) rozpoznanie – czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością placówki w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;

2) ocenę ryzyka i jego istotności, przy pomocy skali określonej w § 8;

3) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;

4) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

Rozdział 2
Zakresy zadań i obowiązków

§ 6.1. Za realizację polityki zarządzania ryzykiem odpowiada kierownik Urzędu - Burmistrz poprzez:

1) kształtowanie i wdrażanie polityki zarządzania ryzykiem;
2) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
3) wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
4) podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

2. Pracownicy na kierowniczych i samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:

1) identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych;
2) wskazywanie właścicieli zidentyfikowanych ryzyk;
3) przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z IOD;

4) proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;

5) wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.

3. Pracownicy wymienieni w ust. 2 są zobowiązani do współpracy z Administratorem Danych oraz IOD.

Rozdział 3
Identyfikacja ryzyka

§ 7.1. Identyfikacja ryzyk prowadzona jest dla wszystkich zbiorów danych na poziomie całego Urzędu jak i na poziomie poszczególnych stanowisk pracy.

2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia. Ze względu na ich źródło ryzyka dzielą się na:

1) Zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne;

2) Wewnętrzne – ryzyko to obejmuje działania wewnętrzne w Urzędzie i może być zarządzane wewnątrz jednostki.

3. Dla każdego zidentyfikowanego ryzyka ustala się reakcje na ryzyko oraz podjęte działanie w celu unikania ryzyka.

4. Dla każdego zidentyfikowanego ryzyka ustala się jego właściciela.

5. Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań w zakresie ochrony danych osobowych.

Rozdział 4
Analiza ryzyka

§ 8.1. Każde ryzyko w zakresie ochrony danych osobowych podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków. Załącznik nr 1 do Polityki Zarządzania Ryzykiem.

2. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

3. W celu dokonania oceny ryzyka wykorzystuje się Mapę Ryzyka, którą stanowi macierz „prawdopodobieństwo – skutek".

4. Mapa ryzyka definiuje ryzyka na:

1) bardzo niskie o wartości do 3;
2) niskie o wartości powyżej 3 do 8
3) średnie o wartości od 9 do 12;
4) wysokie – o wartości powyżej 12 do 16.
5) bardzo wysokie/katastrofalne – o wartości 20 i powyżej.

5. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;

1) 1 – oznacza skutek bardzo mały;
2) 2 – oznacza skutek mały;
3) 3 – oznacza skutek średni;
4) 4 – oznacza skutek duży;
5) 5 – oznacza skutek bardzo duży.

6. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie:

1) 1 – oznacza prawdopodobieństwo bardzo niskie (0-10 %);
2) 2 – oznacza prawdopodobieństwo niskie (11 - 30%);
3) 3 – oznacza prawdopodobieństwo średnie (31 - 50 %);
4) 4 – oznacza prawdopodobieństwo wysokie (51 - 70 %);
5) 5 – oznacza prawdopodobieństwo prawie pewne (71 -100 %).

Rozdział 5
Reakcja na ryzyko

§ 9. Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1) unikanie

2) redukowanie

3) plan rezerwowy

4) nadzór

5) kontrola

Rozdział 6
Postanowienia końcowe.

§ 10. 1. Polityka zarządzania ryzykiem obowiązuje od 25 maja 2018 roku.

2. Pracownicy Urzędu Gminy i Miasta Lubomierz obowiązani są do systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich Burmistrzowi lub zastępującemu pracownikowi.

BURMISTRZ
Gminy i Miasta Lubomierz
Wiesław Zrółkowski
/Burmistrz/

Załącznik nr 1
do Polityki Zarządzania Ryzykiem
w procesie przetwarzania danych osobowych

ANALIZA ZAGROŻEŃ I RYZYKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

w URZĘDZIE GMINY i MIASTA

LUBOMIERZ

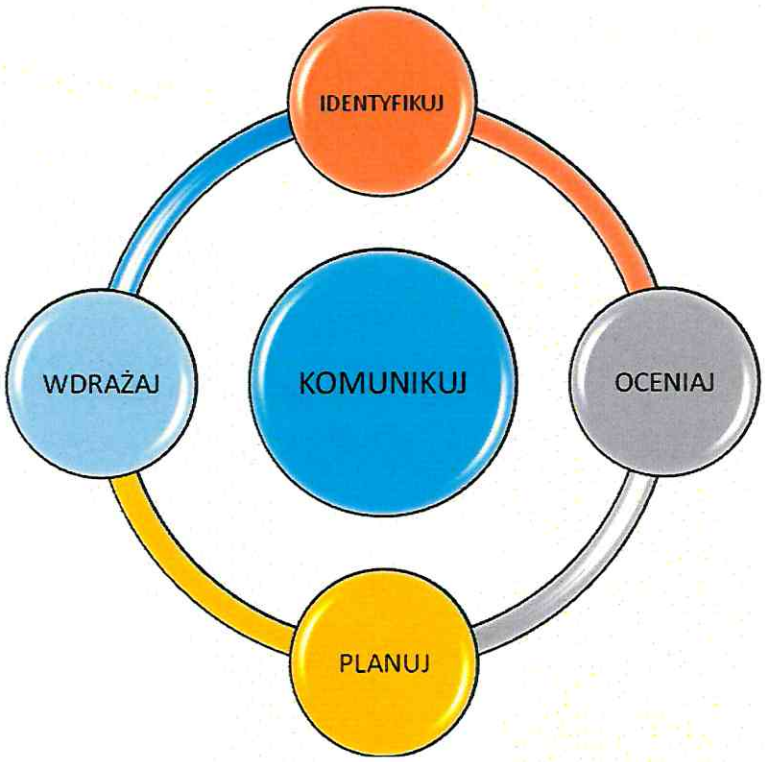
Opracował:
Inspektor Ochrony Danych
mgr Adam Skrzydłowski

Zatwierdził:
BURMISTRZ
Gminy i Miasta Lubomierz
.....
Wiesław Ziółkowski

Ryzyko to prawdopodobieństwo wystąpienia niepożądanych zdarzeń związanych z wykonywaną pracą z danymi osobowymi, powodujących ich udostępnienie w sposób naruszający ustawę o ochronie danych osobowych. W szczególności chodzi o zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Zarządzanie ryzykiem odnosi się do systematycznego stosowania procedur dotyczących zadań identyfikowania i oceniania ryzyka, a następnie planowania i wdrażania reakcji na nie.

W Urzędzie Gminy i Miasta Lubomierz stosuje się procedurę zarządzania ryzykiem zalecaną przez metodologię PRINCE 2, która wykorzystuje procedurę M_o_R (Management of Risk) obejmującą pięć następujących kroków:

1. Identyfikuj
2. Oceniaj
3. Planuj
4. Wdrażaj
5. Komunikuj



1. **Identyfikowanie ryzyka** polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji. W tym celu przyjęto jako podstawową technikę mieszaną, będącą połączeniem technik „przeglądu doświadczeń" oraz „burzy mózgów". Przegląd doświadczeń opiera się na wiedzy eksperckiej oraz analizie wcześniejszych incydentów związanych z naruszeniem informacji. Burza mózgów opiera się na myśleniu grupowym, które może być bardziej produktywne niż indywidualne oraz umożliwia zrozumienie poglądów innych interesariuszy na temat zidentyfikowanych ryzyk.
2. **Ocenianie** polega na oszacowaniu zagrożeń oraz możliwości ich zmaterializowania w przypadku nie podjęcia odpowiednich działań. Do tego celu wykorzystano „macierz prawdopodobieństwo/wpływ". Zawiera ona wartości niezbędne do sklasyfikowania zagrożeń w ujęciu jakościowym. Skale prawdopodobieństwa są miarami pochodzącymi z wartości procentowych, natomiast skale wpływu są wybrane w celu określenia miary oddziaływania na Urząd.

3. **Planowanie** polega na przygotowaniu określonych reakcji zarządczych w celu usunięcia lub zmniejszenia zagrożeń wynikających ze zmaterializowania się określonego ryzyka. Wprowadza się następujące możliwe reakcje na ryzyko:
   1) Unikanie (prewencja) – jeżeli to możliwe podjęcie stosownych reakcji zarządczych tak aby zagrożenie (przypisane do danego ryzyka) nie mogło wpłynąć na bezpieczeństwo informacji lub nie mogło zaistnieć.
   2) Redukowanie – działania podjęte w celu zmniejszenia prawdopodobieństwa wystąpienia zdarzenia lub ograniczenia jego wpływu (redukcja jednego lub dwóch parametrów z macierzy prawdopodobieństwo/wpływ).
   3) Plan rezerwowy – opracowanie działań, które zostaną podjęte w celu zredukowania skutków zagrożenia dla ryzyka, które się zmaterializowało.
4. **Wdrażanie** polega na zapewnieniu, aby planowane reakcje na ryzyko zostały zrealizowane oraz aby podjęte zostały działania korygujące w przypadku gdyby reakcje te nie spełniły związanych z nim oczekiwań. Jest to istotnym elementem ról i obowiązków w zarządzaniu ryzykiem. Wprowadza się następujące role:
   1) Właściciele ryzyka – wskazane stanowisko lub osoba odpowiedzialna zarządzanie, monitorowanie i kontrolowanie wszystkich aspektów przypisanych jej ryzyka łącznie z wdrożeniem wybranych reakcji na zagrożenie.
   2) Wykonawca reakcji na ryzyko – stanowisko lub osoba wyznaczona do wykonywania działań związanych z reakcją na konkretne ryzyko. Wykonawca reakcji wspiera właściciela ryzyka i otrzymuje od niego polecenia.
5. **Komunikacja** polega na zapewnieniu, aby wszystkie informacje o zagrożeniach docierały do wszystkich zainteresowanych. Jako podstawową formę

komunikacji wprowadza się w Urzędzie drogę elektroniczną poprzez pocztę e-mail oraz tradycyjnie.

Analiza ryzyka

Identyfikowanie ryzyka

W Urzędzie Gminy i Miasta Lubomierz zanalizowano możliwe do wystąpienia następujące ryzyka w danych przetwarzanych w sposób tradycyjny:

- oszustwo;
- kradzież;
- sabotaż;
- zdarzenia losowe (powódź, pożar);
- zaniedbania pracowników (niedyskrecja, udostępnienie danych osobie nieupoważnionej);
- niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;
- pokonanie zabezpieczeń fizycznych;
- podsłuchy, podglądy;
- ataki terrorystyczne;
- brak rejestrowania udostępniania danych;
- niewłaściwe miejsce i sposób przechowywania dokumentacji.

Stosowane środki ochrony przetwarzania danych w sposób tradycyjny to:

- przechowywanie danych w pomieszczeniach zamykanych na zamki;
- przechowywanie danych osobowych w szafach zamykanych lub/i zamykanych na klucz;
- przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ADO;
- zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania.

W Urzędzie Gminy i Miasta Lubomierz zidentyfikowano następujące ryzyka w systemach informatycznych (I) oraz tradycyjnych (T):

Identyfikator	Ryzyko	system
1	Włamanie do sieci z zewnątrz	I
2	Włamanie do sieci wewnątrz	I
3	Błędy przesyłania, adresowania danych	I, T
4	Zawodność infrastruktury technicznej	I
5	Podsłuch, programy szpiegujące	I, T
6	Błędy w oprogramowaniu	I
7	Pogorszenie jakości sprzętu i oprogramowania	I
8	Niepożądany ruch w sieci	I
9	Kopiowanie, podmiana lub niszczenie plików	I, T
10	Nieświadome udostępnienie informacji	I, T
11	Świadome udostępnienie informacji	I, T
12	Klęski żywiołowe	I, T

MAPA RYZYKA

PRAWDOPODOBIEŃSTWO							
	5	Bardzo wysokie 71-100%	5	10	15	20	25
	4	Wysokie 51-70%	4	8	12	16	20
	3	Średnie 31-50%	3	6	9 **ID: 10**	12 **ID: 7**	15
	2	Niskie 11-30%	2	4 **ID: 6**	6 **ID: 3**	8	10 **ID: 1,4,12**
	1	Bardzo niskie <10%	1	2 **ID: 5, 11**	3 **ID: 8,9**	4	5 **ID:2**
			Bardzo mały	Mały	Średni	Duży	Bardzo duży
			1	2	3	4	5
			WPŁYW				

Istotność ryzyka określamy jako iloczyn danego **prawdopodobieństwa** i danego **wpływu**, co w konsekwencji określa nam poziom ryzyka czy też poziom zagrożenia.

I = P x W

Mapa Ryzyka definiuje ryzyka na:

1. bardzo niskie o wartości do 3;
2. niskie o wartości powyżej 3 do 8
3. średnie o wartości od 9 do 12;
4. wysokie – o wartości powyżej 12 do 16.
5. bardzo wysokie/katastrofalne – o wartości 20 i powyżej.

Kolorem bordowym oznaczono ryzyko na poziomie nieakceptowalnym, wymagające ciągłego monitorowania sytemu zabezpieczeń oraz uprawnień, sprawdzania przestrzegania procedur oraz odpowiedzialności pracowników.

Kolorem czerwonym oznaczono ryzyko na poziomie nieakceptowalnym, wymagające monitorowania zagrożeń, szkolenia oraz podnoszenie świadomości pracowników w zakresie zagrożenia i odpowiedzialności.

Kolorem pomarańczowym oznaczono obszar o średnim zagrożeniu wymagające monitorowania, szkolenia pracowników oraz podnoszenie świadomości pracowników.

Kolorem fioletowym i różowym oznaczono zdarzenia mało prawdopodobne o niskim wpływie na Urząd, wymagające samokontroli i przestrzegania procedur.

Rejestr ryzyk

ID	Zdarzenie	Skutek	P	W	Reakcja	Działanie	Właściciel ryzyka
1	Nieuprawniony dostęp z zewnątrz. Włamanie do sieci z zewnątrz.	Utrata integralności, poufności, dostęp do informacji.	2	5	Unikanie.	Zabezpieczenie systemów IT przez informatyków , szkolenia pracowników, podniesienie świadomości pracowników.	Każde stanowisko /pracownik z dostępem do sieci zewnętrznej, informatyk.
2	Nieuprawniony dostęp wewnątrz. Włamanie do sieci wewnątrz.	Utrata integralności, poufności, dostęp do informacji.	1	5	Redukowanie.	Zabezpieczenie stanowisk komputerowych, określenie odpowiedzialności pracowników, przestrzeganie procedur oraz instrukcji dotyczących ochrony danych.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
3	Błędne przesyłanie, adresowanie danych.	Możliwy dostęp do informacji osób nieuprawnionych.	2	3	Redukowanie.	Podniesienie świadomości pracowników.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
4	Zawodność infrastruktury technicznej. Możliwość brak ciągłej pracy systemów IT.	Utrudnienia pracy Urzędu i obsługi zainteresowanych.	2	5	Redukowanie, Plan rezerwowy.	Zapewnienie odpowiednich środków finansowych, prowadzenie systematycznych przeglądów infrastruktury technicznej.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk
5	Nieuprawniony dostęp do informacji. Podsłuch, programy szpiegujące.	Utrata poufności informacji.	1	2	Unikanie, nadzór , kontrola.	Powiadomienie właściwych służb o możliwym zaistnieniu zdarzenia.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
6	Błędy w oprogramowaniu. Możliwy brak ciągłości pracy systemów IT.	Utrudnienia pracy Urzędu i obsługi Zainteresowanych.	2	2	Redukowanie.	Zapewnienie środków finansowych na umowy serwisowe, asysty techniczne, zabezpieczenia, oprogramowanie.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
7	Pogorszenia jakości sprzętu i oprogramowania. Możliwy brak ciągłości pracy	Utrudnienia pracy Urzędu i obsługi Zainteresowanych.	3	4	Unikanie.	Zapewnienie środków finansowych na zakup nowego sprzętu i oprogramowania.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.

	systemów IT.						
8	Niepożądany ruch w sieci. Możliwe wprowadzenie do sieci potencjalnie niebezpiecznych kodów lub aplikacji.	Utrata, zniszczenie lub udostępnienie informacji w całości lub części. Niewłaściwa praca systemów.	1	3	Redukowanie.	Monitorowanie ruchu sieciowego.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
9	Nieuprawnione udostępnienie lub zniszczenie informacji. Kopiowanie, podmiana, niszczenie plików.	Utrata, zniszczenie lub udostępnienie informacji w całości lub części.	1	3	Redukowanie.	Podnoszenie świadomości pracowników.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
10	Nieświadome, przypadkowe udostępnienie informacji.	Nieuprawniony dostęp do informacji.	3	3	Redukowanie.	Podnoszenie świadomości pracowników.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
11	Celowe, świadome udostępnienie informacji.	Nieuprawniony dostęp do informacji.	1	2	Kontrola, nadzór.	Podnoszenie świadomości pracowników.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.
12	Klęski żywiołowe lub zdarzenia noszące znamiona klęski. Pożar, powódź, uderzenie pioruna.	Zniszczenie infrastruktury, utraty informacji.	2	5	Redukowanie, Plan rezerwowy.	Opracowanie procedur reagowania, oraz zabezpieczenie budynku placówki oraz jego aktywów.	Każde stanowisko/ pracownik z dostępem do sieci wewnętrznej oraz bez dostępu, informatyk.

Podsumowanie

Macierz prawdopodobieństwo/wpływ ilustruje obszary różnego poziomu zagrożenia. Z punktu widzenia Urzędu najbardziej istotne są wyrazy (będące iloczynem prawdopodobieństwa i wpływu) o największej wartości, które oznaczone zostały kolorem bordowym, jako ryzyko bardzo duże, oraz czerwonym, jako ryzyko duże, które obejmuje ryzyko dotyczące katastrofalnych następstw. W Urzędzie Gminy i Miasta Lubomierz, obecnie nie ma ryzyk o wartości dużej i bardzo dużej. Ryzyka te są na poziomie nieakceptowalnym i wymagają ciągłej kontroli wewnętrznej oraz należytej świadomości pracowników.

Kolor pomarańczowy obejmuje ryzyko o średniej istotności tj. :

1. Włamanie do sieci z zewnątrz (ID 1).
2. Zawodność infrastruktury technicznej (ID 4).
3. Pogorszenie się jakości sprzętu i oprogramowania (ID 7).
4. Nieświadome, przypadkowe udostępnienie informacji (ID 10).
5. Klęski żywiołowe, pożary (ID 12).

Należy stwierdzić, że ryzyka, o których mowa wyżej znajdują się na poziomie średnim, w związku z powyższym są one traktowane w sposób doraźnej kontroli samych pracowników oraz ciągle monitorowane. Zmaterializowanie się ich może zagrażać funkcjonowaniu jednostki i jej aktywów.

Kolorem fioletowym oznaczono obszar o małym ryzyku. W jego skład wchodzą następujące ryzyka:

1. Błędy przesyłania, adresowania danych (ID 3).
2. Włamanie do sieci wewnątrz (ID 2).
3. Błędy w oprogramowaniu. Możliwy brak ciągłości pracy systemów IT (ID 6).

Kolor różowy oznacza obszar ryzyk, w którym zmaterializowanie się zdarzeń jest mało prawdopodobne lub ich wpływ na Urząd jest niewielki.

1. Podsłuch. Nieuprawniony dostęp (ID 5).
2. Niepożądany ruch w sieci. Możliwe wprowadzenie do sieci potencjalnie niebezpiecznych kodów lub aplikacji (ID 8).

3. Nieuprawnione udostępnienie lub zniszczenie informacji. Kopiowanie, podmiana, niszczenie plików (ID 9).

4. Celowe udostępnienie informacji (ID 11).

W Urzędzie Gminy i Miasta Lubomierz podejmowane są działania zgodne z procedurą zarządzania ryzykiem. Istotnym ich elementem jest zabezpieczanie środków finansowych niezbędnych do redukowania zagrożeń polegających na zmniejszeniu wystąpienia prawdopodobieństwa zdarzenia oraz w przypadku jego wystąpienia ograniczeniu wpływu na Urząd. Dotyczy to wszystkich obszarów i zidentyfikowanych ryzyk.

BURMISTRZ
Gminy i Miasta Lubomierz
Wiesław Ziółkowski