Analiza Ryzyka transmisji obrad Rady Gminy Augustów w Urzędzie Gminy Augustów	Data wydania 02.01.2020r.

URZĄD GMINY AUGUSTÓW
ul. Mazurska 1 C
16-300 Augustów

Analiza Ryzyka transmisji obrad Rady Gminy Augustów

w

Urzędzie Gminy Augustów

		Imię i nazwisko	Data	Podpis
Opracował	Inspektor Ochrony Danych	Elżbieta Pszczoła	02.01.2020	
Zatwierdził	Administrator Danych Osobowych	Zbigniew Buksiński	02.01.2020	WÓJT mgr inż. Zbigniew Buksiński

1. PODSTAWA PRAWNA

- 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, RODO).

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

2. PODEJŚCIE OPARTE NA RYZYKU

Zasada podejścia opartego na ryzyku jest ważną, perspektywiczną koncepcją, stanowiącą trzon ogólnego rozporządzenia o ochronie danych.

Zasada ta uzależnia sposób realizacji obowiązków nałożonych na administratora od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów administratora

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko [motyw 76 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 - RODO)].

3. CEL

Celem Analizy Ryzyka jest zapewnienie, że:

1. proces szacowania ryzyka jest kompletny oraz daje szczegółowe, porównywalne i odtwarzalne rezultaty,
2. kryteria oceny ryzyka są ustanowione i spójne z rzeczywistym stanem bezpieczeństwa danych osobowych w Organizacji oraz dostarczają rzetelnych wyników na temat faktycznego poziomu ryzyka,
3. zidentyfikowano potencjalne ryzyko, opisano w kategoriach ilościowych i zarządza się nim świadomie,
4. dokumentacja szacowania ryzyka jest poddawana cyklicznym przeglądom.

Celem Analizy jest ustalenie metodyki oceny ryzyka bezpieczeństwa danych osobowych oraz skutecznego pomiaru wyselekcjonowanych zabezpieczeń i grup zabezpieczeń poprzez mierniki oceny skuteczności. Na proces oceny ryzyka składa się:

1. przeprowadzenie szczegółowej oceny ryzyka w kontekście utraty integralności, poufności i/lub dostępności danego aktywa,
2. opracowanie planu postępowania z ryzykiem w oparciu o przyjęte kryteria akceptacji ryzyka z uwzględnieniem powtórnej analizy, w ramach wdrożonych działań zawartych w Planie postępowania z ryzykiem, zidentyfikowanych nowych podatności i zagrożeń oraz dokonanych incydentów dotyczących naruszenia bezpieczeństwa informacji.

3. TERMINOLOGIA I SKRÓTY

Ryzyko naruszenia praw i wolności osób fizycznych na gruncie RODO uwzględnia:

- prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem, oraz
- powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w poniodniesieniu do osoby, której dane dotyczą.

Aktywa – wszystko, co posiada wartość dla organizacji z punktu widzenia bezpieczeństwa danych osobowych.

Dostępność - możliwość uzyskania i wykorzystania na żądanie przez uprawnioną jednostkę.

Poufność - cecha informacji, która nie jest udostępniana ani ujawniana nieupoważnionym osobom, jednostkom lub procesom.

Integralność - dokładność i kompletność zasobów.

Bezpieczeństwo danych osobowych - ochrona poufności, integralności i dostępności informacji; mogą tu także należeć inne właściwości, takie jak autentyczność, odpowiedzialność, brak odrzucenia i niezawodność.

Incydent związany z ochroną danych osobowych - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, stwarzających znaczne prawdopodobieństwo zakłócenia lub zatrzymania działań biznesowych i zagrażających bezpieczeństwu danych osobowych w odniesieniu do poufności, integralności i dostępności,

Zdarzenie związane z ochroną danych osobowych - zwane też zdarzeniem bezpieczeństwa — jest to określony stan systemu, usługi lub sieci, który wskazuje na niezgodność, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem (może wpływać na bezpieczeństwo) i może być przyczyną incydentu lub słabością systemu,

Słabość systemu lub zabezpieczenia, aktywu — stan, sytuacja lub właściwość która, może spowodować wystąpienia incydentu lub zdarzenia związanego z ochroną danych osobowych,

Podatność — słabość aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie.

4. SZACOWANIE RYZYKA

TRYB POSTĘPOWANIA

- Ocena ryzyka

Istotą procesu oceny ryzyka jest określenie znaczenia ryzyka na podstawie porównania wyznaczonych wartości ryzyk dla zidentyfikowanych aktywów z kryteriami akceptowania ryzyka w kontekście celów strategicznych i biznesowych organizacji oraz spełnienia przepisów prawa. Ocena ryzyka powinna być prowadzona na właściwym stopniu szczegółowości z uwzględnieniem strat finansowych, wizerunkowych i informacyjnych których organizacja doświadczyła bądź może doświadczyć w przyszłości. Polega to na przypisywaniu wartości liczbowej prawdopodobieństwu wystąpienia podatności oraz skutkom zdarzeń.

Ponowną ocenę ryzyka przeprowadza się raz w roku lub w przypadku wystąpienia zmian w organizacji mogących mieć wpływ na ocenę ryzyka.

- Identyfikowanie potencjalnych zagrożeń i podatności

Ocena ryzyka przeprowadzana jest dla każdego zidentyfikowanego aktywa i rozpatruje dwa obszary:

1. prawdopodobieństwo wystąpienia zagrożenia,
2. siła oddziaływania - skutków potencjalnych zagrożeń, biorąc pod uwagę następstwa naruszenia lub utraty:
   - [redacted] poufności,
   - [redacted] integralności,
   - [redacted] dostępności,

   które mogą nastąpić w wyniku działań:
   - [redacted] umyślnych,
   - [redacted] przypadkowych,
   - [redacted] naturalnych.

Analiza Ryzyka transmisji obrad Rady Gminy Augustów w Urzędzie Gminy Augustów	Data wydania 02.01.2020r.

- Metodyka Oceny Ryzyka

Metodyka Oceny Ryzyka w Organizacji, została ustanowiona w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w organizacji oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka. Ocena ryzyka przeprowadzana jest w Arkuszu Oceny Ryzyka w programie EXCEL. Za dane wejściowe do procesu oceny uważa się wszelkie informacje przedstawione w analizie ryzyka, a także wiedzę pracowników na temat stosowanych zabezpieczeń, w szczególności miejsce przetwarzania, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywa.

Szacowanie prawdopodobieństwa

Badane kryterium	Ryzyko	Wartość
(P) Prawdopodobieństwo (możliwość wystąpienia)	niskie, odległe, mało realne szanse na zdarzenie	1
	może się zdarzyć lub zdarza się sporadycznie	2
	bardzo realne szanse wystąpienia	3

Powaga zdarzenia

Badane kryterium	Ryzyko	Wartość
(S) Skutek (wpływ na organizację i/lub proces)	utrata danych nie spowoduje utrudnień w pracy Urzędu lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu	1
	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku Urzędu, odtworzenie danych jest możliwe ale pracochłonne	2
	utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne; odtworzenie danych i reputacji będzie trudne i kosztowne.	3

- Kategoria Ryzyka

Analiza Ryzyka transmisji obrad Rady Gminy Augustów w Urzędzie Gminy Augustów	Data wydania 02.01.2020r.

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:

$$R = P \times S$$

gdzie:

P - Prawdopodobieństwo

S – Skutek (powaga zdarzenia)

Wynik z działania zgodnie z poniższą tabelą, należy przypisać ustanowionym kategoriom ryzyka, a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego w ramach Planu postępowania z ryzykiem.

Wytyczne do postępowania z ryzykiem

Klasa Kategorii	Kategoria Ryzyka	Wartość Ryzyka	Akceptacja Ryzyka Tak / Nie	Działania zapobiegawcze
1	Małe	1 - 3	TAK	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące.
2	Średnie	4	TAK	Należy rozważyć konieczność zredukowania ryzyka do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne.
3	Duże	6 - 9	NIE	Ocena skutków. Należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc aktywa w bezpieczniejsze miejsce.

- Plan postępowania z ryzykiem

Inspektor Ochrony Danych dla aktywów gdzie ryzyko było nieakceptowalne, ocenia skutki i formułuje Plan Postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu bezpiecznego — akceptowalnego.

Ostatecznie zatwierdzone i wdrożone zabezpieczenia należy wpisać w dokument oceny ryzyka, w kolumnie działań zapobiegawczych i/lub korygujących w celu przeprowadzenia ponownej oceny ryzyka.

5. **Tabela szacowania ryzyka wg RODO dotycząca transmisji obrad Rady Gminy Augustów w Urzędzie Gminy Augustów. Wnioski z przeprowadzonej Analizy Ryzyka (załącznik).**

6. **Wnioski.**

W celu prawidłowego nadzoru nad obowiązkiem transmisji obrad kolegialnych organów jednostek samorządu terytorialnego należy zastosować istniejące mechanizmy kontroli oraz propozycje reakcji na ryzyko w szczególności należy:

- Zapewnić aby dane przetwarzane w związku z transmisją obrad kolegialnych organów jednostek samorządowych spełniały wymogi 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, RODO) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781),
- Wdrożona została Procedura udostępniania danych w Biuletynie Informacji Publicznej,
- Pracownicy/osoby przetwarzające dane osobowy posiadały wiedzę w zakresie bezpieczeństwa danych osobowych,
- Analiza ryzyka wykonywana była okresowo.

WÓJT

mgr inż. Zbigniew Buksiński