OCENA RYZYKA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH ZWIĄZANA Z MINITORINGIEM WIZYJNYM W URZĘDZIE GMINY AUGUSTÓW

1. Aby poprawić przestrzeganie *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),* gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

2. Poniżej została przedstawiona ocena ryzyka skutków dla danych osobowych związana z monitoringiem wizyjnym w Urzędzie Gminy Augustów.

Lp	Opis ryzyka	Prawdopodobieństwo wystąpienia ryzyka (skala 1 - 3)	Skutek - powaga zdarzenia (skala 1 -3)	Ocena ryzyka – wynik (dopuszczalność)	Istniejące mechanizmy kontroli	Propozycje reakcji na ryzyko
Obsługa programu VULCAN						
1	Udostepnienie obrazu z monitoringu osobom nieupoważnionym	1	3	3	Dostęp do monitoringu posiada jedynie Administrator, inne osoby nie posiadają dostępu. Opracowano i wdrożono załącznik do Regulaminu pracy, regulujący zasady funkcjonowania monitoringu.	
2	Przetwarzanie z naruszeniem przepisów	1	3	3	Monitoring służy tylko i wyłącznie do zapewnienia bezpieczeństwa, a także ochrony mienia. Nie służy do innych celów. Operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów. Opracowano klauzulę informacyjną związaną z monitoringiem wizyjnym. Osoby objęte monitoringiem zapoznają się z ww. klauzulą.	
3	Zmiana lub uszkodzenie nagrań	1	2	2	Dostęp do zapisów z monitoringu posiada tylko i wyłącznie Administrator. Osoby postronne i nieupoważnione nie posiadają dostępu. Opracowano i wdrożono załącznik do Regulaminu pracy,	

					regulujący zasady funkcjonowania monitoringu.	
4	Utrata danych osobowych w związku z atakiem złosliwego oprogramowania	1	3	3	Opracowano i wdrożono Instrukcja Zarządzania Systemem Informatycznym.	
5	Klęska żywiołowa, pożar, powódź, wypadek, zdarzenie, w wyniku których utracono poufność danych osobowych	1	3	3	Brak	
6	Nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego lub urządzenia mobilnego	1	3	1	Instrukcja Zarządzania Systemem Informatycznym	

3. **Wnioski z przeprowadzonej oceny ryzyka:**
    - Należy przestrzegać zapisów załącznika do Regulaminu pracy, regulującego zasady funkcjonowania monitoringu.
    - Należy przestrzegać zapisów Instrukcji Zarządzania Systemem Informatycznym.

4. 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 przedsiębiorstwa lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu	1
	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku przedsiębiorstwa, 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

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.