ANALIZA – SZACOWANIE RYZYKA

PRZY PRZETWARZANIU DANYCH OSOBOWYCH

W URZĘDZIE GMINY W KAŹMIERZU

**SPIS TREŚCI: STRONA**

Definicje …………………………………………………………………………………………………………………………… 3-4

Kontekst organizacji……………………………………………………………………………………………………………. 5

Wykaz zbiorów przetwarzania przez UG……………………………………………………………………………… 5-7

Wykaz pomieszczeń……………………………………………………………………………………………………………. 7-9

Aktywa ……………………………………………………………………………………………………………………………….. 9-10

Ewentualne koszty związane z utratą aktywów ………………………………………………………………….. 11

Zagrożenia dla systemu informatycznego …………………………………………………………………………… 11-13

Analiza zagrożeń i ryzyka …………………………………………………………………………………………………… 14

Pojęcie i cele ryzyka …………………………………………………………………………………………………………… 15

Identyfikacja ryzyka (zagrożeń i podatności) ………………………………………………………………………. 15

Sposób szacowania ryzyka………………………………………………………………………………………………….. 16-17

Pomiar i analiza ryzyka ………………………………………………………………………………………………………..17-41

Wyniki analizy……………………………………………………………………………………………………………………… 42-47

Ocena skutków …………………………………………………………………………………………………………………… 48

Wykaz rodzajów operacji przetwarzania danych osobowych……………………………………………… 49-56

Wpływ na prywatność………………………………………………………………………………………………………… 56-57

**DEFINICJE:**

**Ryzyko** – możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia”. W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.

**Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011)

**Identyfikacja ryzyka** - jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

**Kryteria akceptacji ryzyka** – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-2.

**Kryteria oceny ryzyka** - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.

**Podatność** - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

**Zabezpieczenie** - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

**Zagrożenie** - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

**Proces przetwarzania danych osobowych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

**Operacja przetwarzania danych osobowych** - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

**Anonimizacja –** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.

**Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

**Grupa Robocza Art. 29 -** Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej, i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.

**RODO** - 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), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.

**INTEGRALNOŚĆ** - właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany – pożar, katastrofa budowlana, błąd ludzki przy przetwarzaniu danych osobowych, zniszczenie płyty zawierającej jedyną kopię danych osobowych.

**KONTEKST ORGANIZACJI**

**URZĄD GMINY W KAŹMIERZU** :Urząd Gminy jest organem pomocniczym Wójta. Wójt jest kierownikiem urzędu i on nadaje jego Regulamin. W skład Urzędu Gminy w Kaźmierzu wchodzą poszczególne wydziały : Wydział Organizacyjno – Gospodarczy, Wydział Promocji, Informacji i Komunikacji Społecznej, Wydział Spraw Obywatelskich i USC, Wydział Rolnictwa i Ochrony Środowiska, Wydział Nieruchomości i Inwestycji, Wydział Planowania Przestrzennego i Przetwarzania Danych, Wydział Księgowości i Opłat, Gminny Zespół Oświatowy, jako CUW.

**PODSTAWY PRAWNE FUNKCJONOWANIA URZĘDU GMINY W KAŹMIERZU** : Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym ( Dz.U. z 2019 r. poz.506 ), Statut Gminy Kaźmierz, Regulamin Organizacyjny, Kodeks Etyki, Schemat Organizacyjny, Regulamin Pracy.

**ZAKRES WŁADCTWA ORAZ ORGANY GMINY KAŹMIERZ**: Wójt Gminy Kaźmierz i Rada Gminy Kaźmierz. Wójt wykonuje uchwały rady gminy i zadania gminy określone przepisami prawa. Do właściwości Rady Gminy należą wszystkie sprawy pozostające w zakresie działania gminy, o ile ustawy nie stanowią inaczej.

**JEDNOSTKI, DLA KTÓRYCH UG JEST ORGANEM PROWADZĄCYM** : Biblioteka Publiczna i Centrum Kultury w Kaźmierzu, Gminny Ośrodek Pomocy Społecznej w Kaźmierzu, Gminny Zespół Oświatowy w Kaźmierzu, Przedszkole Samorządowe w Kaźmierzu, Zespół Szkolno – Przedszkolny w Bytyniu, Szkoła Podstawowa w Kaźmierzu, Zakład Usług Komunalnych w Kaźmierzu.

 **WYKAZ ZBIORÓW PRZETWARZANYCH PRZEZ URZĄD GMINY W KAŹMIERZU (WYCIĄG Z RCP):**

1. Prowadzenie rejestru umów Urzędu Gminy - Wydział Organizacyjno - Gospodarczy - ORG
2. Prowadzenie dokumentacji dot. dofinansowania kosztów kształcenia Młodocianych Pracowników Wydział Organizacyjno - Gospodarczy - ORG
3. Skargi i wnioski załatwiane bezpośrednio - wpływające do Wójta - Wydział Organizacyjno - Gospodarczy - ORG
4. Prowadzenie rejestru cen najmu lokali mieszkalnych nienależących do publicznego zasobu mieszkaniowego - Wydział Organizacyjno - Gospodarczy - ORG
5. Prowadzenie rejestru kontroli zewnętrznych w podmiotach - Wydział Organizacyjno - Gospodarczy - ORG
6. Prowadzenie rejestru wydawanych upoważnień i pełnomocnictw - Wydział Organizacyjno - Gospodarczy - ORG
7. Prowadzenie Rejestru Faktur - Wydział Organizacyjno - Gospodarczy - ORG
8. Zbiór pracowników korzystających z samochodów prywatnych do celów służbowych - Wydział Organizacyjno - Gospodarczy - ORG
9. Realizacja zadań dotyczących dowodu osobistego - Wydział Spraw Obywatelskich i USC
10. Realizacja zadań z zakresu CEIDG - Wydział Spraw Obywatelskich i USC
11. Realizacja zadań z zakresu powszechnego obowiązku obrony RP - Wydział Spraw Obywatelskich i USC
12. Ustalanie uprawnień do najmu lokali z mieszkaniowego zasobu gminy- Wydział Spraw Obywatelskich i USC
13. Świadczenie wychowawcze 500 PLUS - Wydział Spraw Obywatelskich i USC
14. Zbiór danych osobowych dotyczących ustalenia prawa do świadczenia dobry start- program 300 PLUS Wydział Spraw Obywatelskich i USC
15. Ewidencja ludności - Wydział Spraw Obywatelskich i USC
16. Zgromadzenia publiczne - Wydział Spraw Obywatelskich i USC
17. Wybory - Rejestr Wyborców - Wydział Spraw Obywatelskich i USC
18. Profil zaufany - Wydział Spraw Obywatelskich i USC
19. Rejestr aktów notarialnych - wydział Podatków i Opłat
20. Podatki i opłaty lokalne - wydział Podatków i Opłat
21. Rejestr zobowiązanych do zapłaty należności cywilno-prawnych oraz innych opłat - wydział Podatków i Opłat
22. Prowadzenie czynności związanych z ustaleniem wpływu realizacji inwestycji na środowisko - Wydział Nieruchomości i Inwestycji - NI
23. Prowadzenie czynności związanych z ochroną zabytków i opieką nad zabytkami - Wydział Nieruchomości i Inwestycji - NI
24. Sprawy osobowe radnych - Wydział Organizacyjno - Gospodarczy - ORG
25. Oświadczenia majątkowe radnych - Wydział Organizacyjno - Gospodarczy - ORG
26. Zakładowy Fundusz Świadczeń Socjalnych - Wydział Organizacyjno - Gospodarczy - ORG
27. Ewidencja zgłoszeń zamiaru usunięcia drzew i wniosków o zezwolenie na usunięcie drzew i krzewów Wydział Rolnictwa i Ochrony Środowiska
28. Ochrona ppoż - ewidencja szkoleń, badań lekarskich, uprawnień kierowców, zgłoszenia do konkursów i turniejów - Wydział Rolnictwa i Ochrony Środowiska
29. Ewidencja wyrobów zawierających azbest i miejsc ich występowania - Wydział Rolnictwa i Ochrony Środowiska
30. Ewidencja pozwoleń na uprawę maku i konopii - Wydział Rolnictwa i Ochrony Środowiska
31. Kontrola przestrzegania "uchwał antysmogowych" - Wydział Rolnictwa i Ochrony Środowiska
32. Zarządzanie kryzysowe Wydział Rolnictwa i Ochrony Środowiska, Gminny Zespół Zarządzania Kryzysowego
33. Ochrona zwierząt: ewidencja zezwoleń na utrzymywanie psów ras agresywnych, ewidencja decyzji o odbiorze zwierząt, Roczny Program opieki nad zwierzętami bezdomnymi i zapobiegania bezdomności zwierząt - Wydział Rolnictwa i Ochrony Środowiska
34. Wnioski interesantów i korespondencja - Poznański Związek Spółek Wodnych - Wydział Rolnictwa i Ochrony Środowiska
35. Pozwolenia wodnoprawne - Wydział Rolnictwa i Ochrony Środowiska
36. Ewidencja zbiorników bezodpływowych i przydomowych oczyszczalni ścieków - Wydział Rolnictwa i Ochrony Środowiska
37. Rejestr decyzji ustalającej opłatę od wzrostu wartości nieruchomości w związku z uchwaleniem mpzp Wydział Nieruchomości i Inwestycji - NI
38. Zbiór postępowań o opłaty z tytułu wzrostu wartości nieruchomości w wyniku podziału Wydział Nieruchomości i Inwestycji - NI
39. Zbiór użytkowników wieczystych - Wydział Nieruchomości i Inwestycji - NI
40. Zbiór dzierżawców - Wydział Nieruchomości i Inwestycji - NI
41. Rejestr umów użyczenia - Wydział Nieruchomości i Inwestycji - NI
42. Rejestr odszkodowań za nieruchomości przejęte pod drogi publiczne - Wydział Nieruchomości i Inwestycji - NI
43. Rejestr kupna nieruchomości - Wydział Nieruchomości i Inwestycji - NI
44. Rejestr sprzedaży nieruchomości - Wydział Nieruchomości i Inwestycji - NI
45. Rejestr zaświadczeń z miejscowego planu zagospodarowania przestrzennego i oraz wypisy i wyrysy z MPZP - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
46. Rejestr wniosków o zmianę studium uwarunkowań i kierunków zagospodarowania przestrzennego - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
47. Rejestr wniosków o opracowanie/ zmianę miejscowego planu zagospodarowania przestrzennego - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
48. Ustalenia sporządzanych/ zmienianych studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
49. Ustalenia planów miejscowych zagospodarowania przestrzennego - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
50. Rejestr wydanych decyzji o warunkach zabudowy - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
51. Zbiór postępowań podziałowych - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
52. Zbiór postępowań w sprawie rozgraniczenia nieruchomości, scalenie nieruchomości - Wydział Planowania Przestrzennego i Przetwarzania Danych - PPPD
53. Numeracja porządkowa nieruchomości - Wydział Nieruchomości i Inwestycji
54. Decyzje o ustaleniu lokalizacji inwestycji celu publicznego - Wydział Nieruchomości i Inwestycji
55. Zezwolenie na lokalizację zjazdu - Wydział Nieruchomości i Inwestycji
56. Zezwolenie na lokalizowanie w pasie drogowym obiektów budowlanych lub urządzeń niezwiązanych z potrzebami zarządzania drogami lub potrzebami ruchu drogowego - Wydział Nieruchomości i Inwestycji
57. Zezwolenie na zajęcie pasa drogowego w celu prowadzenia robót - Wydział Nieruchomości i Inwestycji
58. Zezwolenie na zajęcie pasa drogowego i ustalenie opłaty za umieszczenie urządzenia infrastruktury technicznej niezwiązanej z potrzebami zarządzania drogami lub potrzebami ruchu drogowego - Wydział Nieruchomości i Inwestycji
59. Zezwolenie na zajęcie pasa drogowego w celu umieszczenia reklamy - Wydział Nieruchomości i Inwestycji
60. Umowy zlecenia - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
61. Wnioskodawcy pism o udzielenie informacji publicznej - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
62. Oświadczenia majątkowe lub inne oświadczenia o osobach zatrudnionych i członkach ich rodzin Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
63. Ewidencja skazanych odbywających karę pracy na cele społeczne w ZUK Kaźmierz - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
64. Akta i sprawy osobowe pracowników - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
65. Staże, praktyki, wolontariat - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
66. Petycje wpływające do Wójta - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
67. Zapotrzebowanie i nabór kandydatów do pracy - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK
68. Konkursy dla NGO - Wydział Promocji, Informacji i Komunikacji Społecznej - PIK

**WYKAZ POMIESZCZEŃ ZE STOSOWANYMI ZABEZPIECZENIAMI TECHNICZNYMI.**

|  |
| --- |
| **Budynek A****Urząd Gminy w Kaźmierzu, ul. Szamotulska 20, 64 – 530 Kaźmierz** |
| **L.P.** | **Nr pomieszczenia** | **Nazwa stanowiska** | **Miejsce, położenie** | **Uwagi** |
| 1. | 23 | Wójt Gminy Kaźmierz | piętro |  |
| 2. | 24 | Zastępca Wójta Gminy Kaźmierz | piętro |  |
| 3. | 22 | Sekretarz Gminy Kaźmierz | piętro |  |
| 4. | 25 | Zastępca Dyrektora Gminnego Zespołu Oświatowego | piętro |  |
| 5. | 26 | Kierownik Wydziału PIK, Samodzielny Referent Wydziału PIK | piętro |  |
| 6. | 28 | Kierownik Wydziału NI | piętro |  |
| 7. | 27 | Inspektor Wydziału NI  | piętro |  |
| 8. | 29 | Inspektor Wydziału NI | piętro |  |
| 9. | 21 | Sekretariat Wójta | piętro |  |
| 10. | 12 | Kierownik Wydziału ORG | parter |  |
| 11. | 11 | Kancelaria – Specjalista, Referent | parter |  |
| 12. | 17 | Kierownik Wydziału SO i USC | parter |  |
| 13. | 16 | Zastępca Kierownika USC | parter |  |
| 14. | 18 | Główny Specjalista Wydziału SO | parter |  |
| 15. | 19 | Referent Wydziału SO | parter |  |
| 16. | 13 | p.o. Kierownik Wydziału ROŚ, Główny Specjalista Wydziału ROŚ | parter |  |
| 17. | 15 | Skarbnik Gminy Kaźmierz | parter |  |
| 18. | 14 | Inspektor Wydziału OP, Specjalista Wydziału OP, Referent Wydziału OP | parter |  |
| 19. |  | archiwum | parter |  |
| 20. |  | Pomieszczenie przetwarzania danych niejawnych | parter |  |
| 21. |  | Składnica akt GZO | parter |  |

|  |
| --- |
| **Budynek B****Urząd Gminy w Kaźmierzu, ul. Szamotulska 20, 64 – 530 Kaźmierz** |
| **L.P.** | **Nr pomieszczenia** | **Nazwa stanowiska** | **Miejsce, położenie** | **Uwagi** |
| 1. | 1 | Referent Wydziału Księgowości  | piętro |  |
| 2. | 2 | Główny Księgowy | piętro |  |
| 3. | 3 | Księgowość Gminnego Zespołu Oświatowego | piętro |  |

**Budynek Urzędu Gminy w Kaźmierzu jest objęty monitoringiem wizyjnym. Wszystkie pomieszczenia wewnątrz budynku są zamykane na klucz.**

**OGÓLNE WYMOGI BEZPIECZEŃSTWA**

Przetwarzanie danych osobowych w Urzędzie Gminy w Kaźmierzu odbywa się w postaci:

* elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera),
* papierowej (wydruki).

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

* środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem,
* środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy).

**AKTYWA**

**Wśród aktywów będących w posiadaniu Urzędu Gminy w Kaźmierzu należy wyróżnić:**

* **posiadaną wiedzę,**
* **personel,**
* **sprzęt,**
* **oprogramowanie,**
* **pozostałe środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych**

**Aktywa podzielone zostały na podstawowe i wspierające, co przedstawia poniższy schemat:**

**EWENTUALNE KOSZTY ZWIĄZANE Z UTRATĄ AKTYWÓW**

1. Koszty związane z odtworzeniem aktywów,
2. Koszty utraty zaufania do administratora danych osobowych,
3. Koszty związane z utratą:

- poufności,

- integralności,

- dostępności danych ,

1. Możliwość nałożenia kary przez organ nadzorczy,
2. Koszty związane z możliwością nakazania przez organ nadzorczy całkowitego zaprzestania lub czasowego zaprzestania przetwarzania danych osobowych , np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

**ZAGROŻENIA DLA SYSTEMU INFORMATYCZNEGO**

Podstawowe zagrożenia dla systemu informatycznego, przeznaczonego do przetwarzania danych osobowych:

1. utrata poufności (pozyskanie danych przez osoby nieupoważnione):
	* nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki)
	* nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu),
	* nieuprawnione skopiowanie danych osobowych na inny nośnik,
	* zgubienie nośnika zawierającego dane osobowe,
	* niedostateczne zniszczenie wydruku zawierającego dane osobowe,
	* klęska żywiołowa powodująca utratę poufności danych.
2. utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione):
	* nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej),
	* błędy ludzkie,
	* działania wirusów (brak programów antywirusowych i firewalli),
	* awarie oprogramowania komputerów,
3. utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań) :
	* brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze,
	* brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne.

Do głównych źródeł zagrożeń dla stanowisk komputerowych, na których przetwarzane są dane osobowe przedstawia poniższa tabela:

|  |
| --- |
| **ŹRÓDŁO ZAGROŻENIA** |
| Siły wyższe – naturalne -niezależne od jednostki ludzkiej | * pożar np.: będący skutkiem uderzenia pioruna,
* starzenie się sprzętu,
* powódź,
* katastrofa budowlana,
* wilgoć, kurz,
 |
| Działalność człowieka | * błędy użytkowników,
* zgubienie nośnika informacji,
* niewłaściwe usunięcie danych z nośnika informacji,
* terroryzm,
* utrata prądu,
* szpiegostwo,
* utrata dostępu do nośnika z danymi,
* kradzież komputera ( dysku twardego,
* wandalizm,
* celowe działania pracownika na szkodę organizacji ( sabotaż ),
* obserwacja bezpośrednia ( w tym filmowanie, fotografowanie )
* podglądanie zawartości ekranu monitora przez osoby nieuprawnione,
* włamanie do systemu informatycznego,
* wyłudzenie haseł dostępu,
* nieuprawnione instalowanie urządzeń,
* nieuprawniona modyfikacja używanego oprogramowania,
* kopiowanie danych,
* korzystanie z nielicencjonowanego oprogramowania,
* nieuprawniony dostęp do pomieszczeń,
* włamanie do pomieszczeń,
* utrata danych podczas napraw sprzętu,
* odczytanie informacji z nośników przeznaczonych do naprawy,
* uszkodzenia sprzętu komputerowego,
* uszkodzenie fizyczne nośnika danych,
* awaria systemu operacyjnego,
* awaria zasilania.
 |

**ZAGROŻENIA DLA ZASOBÓW PAPIEROWYCH**

|  |
| --- |
| **ŹRÓDŁO ZAGROŻENIA** |
| Siły wyższe – naturalne -niezależne od jednostki ludzkiej | * pożar np.: będący skutkiem uderzenia pioruna,
* powódź,
 |
| Działalność człowieka | * kradzież dokumentów,
* zgubienie dokumentów,
* celowe działania pracownika na szkodę organizacji ( sabotaż ),
* wgląd do danych przez osobę nieupoważnioną do przetwarzania ( w tym obserwacja, filmowanie, fotografowanie ),
* podgląd dokumentów przetwarzanych przez innego użytkownika,
* nieuprawniony dostęp do pomieszczeń,
* włamanie do pomieszczeń,
* wykorzystywanie zużytych wydruków ( zamiast zniszczenia),
* błędy w obiegu dokumentów
 |

**ANALIZA ZAGROŻEŃ I RYZYKA**

Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.

Zagrożenia i ryzyka w zakresie ochrony danych osobowych:

* Niedostateczne kwalifikacje Inspektora (w tym brak podnoszenia kwalifikacji),
* Brak procedur ochrony danych osobowych,
* Niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych,
* Brak lub wady upoważnień do przetwarzania danych osobowych,
* Brak lub wady ewidencji wydanych upoważnień,
* Brak lub wady szkoleń z zakresu ochrony danych osobowych,
* Wady nadzoru nad przetwarzaniem i ochroną danych osobowych,
* Brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych.

**POJĘCIE I CELE RYZYKA**

Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia”. Rozporządzenie
w Artykule 32 definiuje cele w zakresie bezpieczeństwa przetwarzania i są to:

* pseudonimizacja i szyfrowanie danych osobowych,
* zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
* zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich
w razie incydentu fizycznego lub technicznego,
* regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych
i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W związku z powyższym ryzyko w przetwarzaniu danych jest związane z potencjalną sytuacją,
w której określone zagrożenie wykorzysta podatność (np. niezabezpieczony hasłem sprzęt komputerowy), powodując w ten sposób szkodę dla jednostki organizacyjnej (np. kradzież lub upublicznienie informacji).

**IDENTYFIKACJA RYZYKA (ZAGROŻEŃ I PODATNOŚCI)**

Zgodnie z zapisem 75 punktu preambuły Rozporządzenia, wyszczególnione zostały zagrożenia związane z przetwarzaniem danych z wyszczególnieniem prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

* jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
* jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw
i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
* jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
* jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
* lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
* jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

**SPOSÓB SZACOWANIA RYZYKA**

Ryzyko szacowane jest na podstawie wzoru:

**R = P x S**

**R** - ryzyko

**P** - prawdopodobieństwo wykorzystania podatności przez zagrożenie - szacując prawdopodobieństwo wykorzystania podatności przez zagrożenie bierzemy pod uwagę trzy elementy:

- prawdopodobieństwo zaistnienia zagrożenia w rzeczywistości danej organizacji – ocenione na podstawie informacji na temat czynników sprzyjających zmaterializowaniu się zagrożenia mających swoje źródło zarówno wewnątrz jak i na zewnątrz organizacji;

- podatność zasobów danych osobowych na zaistniałe już zagrożenie;

- stosowane techniczne i organizacyjne środki zabezpieczeń zmniejszające prawdopodobieństwo wystąpienia zagrożenia i wykorzystania podatności przez zagrożenia.

**S** - skala skutku - skalę skutku określa się poprzez zaokrąglenie w górę do pełnej liczy średniej wartości liczbowej skutków zmaterializowania się zagrożenia dla poufności, dostępności
i integralności danych. Wartość skutku każdego rodzaju uwzględnia dwa elementy:

- konsekwencje zmaterializowania się zagrożenia dla odpowiednio poufności, dostępności
i integralności danych;

- stosowane techniczne i organizacyjne środki zmniejszające skalę skutku zmaterializowania się zagrożenia dla odpowiednio poufności, dostępności i integralności danych.

Poziom ryzyka określa się na podstawie poniższej macierzy ryzyka:

|  |
| --- |
| **SKUTEK** |
|  | Bardzo niski | Niski | Średni | Wysoki | Bardzo wysoki |
| 1 | 2 | 3 | 4 | 5 |
| **Prawdopodobieństwo** | Prawie pewne | 5 | **Ś** | **W** | **K** | **K** | **K** |
| Prawdopodobne | 4 | **Ś** | **W** | **W** | **K** | **K** |
| Możliwe | 3 | **N** | **Ś** | **W** | **W** | **K** |
| Mało prawdopodobne | 2 | **N** | **Ś** | **Ś** | **W** | **W** |
| Rzadkie | 1 | **N** | **N** | **Ś** | **W** | **W** |

|  |  |  |
| --- | --- | --- |
|  | **Poziom ryzyka**  | **Opis działania** |
|  | Niski **( N )** | Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów |
|  | Średni **( Ś )** | Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania |
|  | Wysoki **( W )** | Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania |
|  | Krytyczny **( K )** | Poziom ryzyka nietolerowany – wymaga natychmiastowego działania |

**POMIAR I ANALIZA RYZYKA**

**Wydział organizacyjno-gospodarczy** **(ORG) – czynności przetwarzania - forma papierowa:**

- prowadzenie rejestru umów UG,

- dokumentacja dot. dofinansowania kosztów kształcenia Młodocianych Pracowników,

- Skargi i Wnioski załatwiane bezpośrednio – wpływające do Wójta,

- Prowadzenie rejestru cen najmu lokali mieszkalnych nienależących do publicznego zasobu mieszkaniowego,

- Prowadzenie rejestru kontroli zewnętrznej w podmiotach,

- Prowadzenie rejestru wydawanych upoważnień i pełnomocnictw,

- Zbiór pracowników korzystających z samochodów prywatnych do celów służbowych.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **ORG** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 3 | 3 | 2 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kradzież dokumentów** |  | 1 | 3 | 3 | 3 | 3 | 3 | **3** |
| **Zgubienie dokumentów** |  | 2 | 1 | 2 | 2 | 1,67 | 2 | **4** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 2 | 2 | 2 | 2 | 2 | 2 | **4** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 1 | 1  | 2 | 1 | 1,33 | 2 | **2** |

**Analiza ryzyka – zasoby w postaci elektronicznej ORG**

- Prowadzenie rejestru umów UG,

- Dokumentacja dot. dofinansowania kosztów kształcenia Młodocianych Pracowników,

- Skargi i Wnioski załatwiane bezpośrednio – wpływające do Wójta,

- Prowadzenie rejestru cen najmu lokali mieszkalnych nienależących do publicznego zasobu mieszkaniowego,

- Prowadzenie rejestru kontroli zewnętrznej w podmiotach,

- Prowadzenie rejestru wydawanych upoważnień i pełnomocnictw,

- Zbiór pracowników korzystających z samochodów prywatnych do celów służbowych,

- Prowadzenie rejestru faktur.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **CORG** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 1 | 1 | 2,33 | 3 | **9** |
| **Utrata dostępu do nośnika z danymi** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 2 | 2 | 2 | 2 | 2 | **4** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Włamanie do systemu informatycznego** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kopiowanie danych** |  | 2 | 2 | 0 | 0 | 0,67 | 1 | **2** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 1 | 1 | 2 | 2 | 1,67 | 2 | **2** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Uszkodzenie fizyczne nośnika danych** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |
| **Awaria systemu operacyjnego** |  | 3 | 0 | 1 | 1 | 0,67 | 1 | **3** |
| **Awaria zasilania** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |

**Analiza Ryzyka -**  **czynności przetwarzania - forma papierowa:**

**Wydział Nieruchomości i Inwestycji - NI**

- rejestr decyzji ustalającej opłatę od wzrostu wartości nieruchomości w związku z uchwaleniem mpzp

- zbiór postępowań o opłaty z tytułu wzrostu wartości nieruchomości w wyniku podziału

- zbiór użytkowników wieczystych

- Zbiór dzierżawców

- rejestr umów użyczenia

- rejestr odszkodowań za nieruchomości przejęte pod drogi publiczne

- rejestr kupna nieruchomości

- rejestr sprzedaży nieruchomości

- Numeracja porządkowa nieruchomości

- decyzje o ustaleniu lokalizacji inwestycji celu publicznego

- zezwolenie na lokalizację zjazdu

- Zezwolenie na lokalizowanie w pasie drogowym obiektów budowlanych lub urządzeń niezwiązanych z potrzebami zarządzania drogami lub potrzebami ruchu drogowego

- zezwolenie na zajęcie pasa drogowego w celu prowadzenia robót

- zezwolenie na zajęcie pasa drogowego i ustalenie opłaty za umieszczenie urządzenia infrastruktury technicznej niezwiązanej z potrzebami zarządzania drogami lub potrzebami ruchu drogowego

- zezwolenie na zajęcie pasa drogowego w celu umieszczenia reklamy

- Prowadzenie czynności związanych z ustaleniem wpływu realizacji inwestycji na środowisko

- Prowadzenie czynności związanych z ochroną zabytków i opieką nad zabytkami

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **NI** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 5 | 5 | 3,33 | 4 | **8** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 3 | 2 | 1,67 | 2 | **2** |
| **Kradzież dokumentów** |  | 1 | 4 | 5 | 3 | 4 | 4 | **4** |
| **Zgubienie dokumentów** |  | 2 | 4 | 4 | 3 | 3,67 | 4 | **8** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 1 | 4 | 4 | 2 | 3,33 | 4 | **4** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 2 | 3 | 0 | 0 | 1 | 1 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 3 | 2 | 0 | 0 | 0,67 | 1 | **3** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 0 | 1 | 0,67 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 0 | 1 | 0,67 | 1 | **1** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 2 | 1  | 2 | 2 | 1,67 | 2 | **4** |

**Analiza ryzyka – zasoby w postaci elektronicznej**

**Wydział Nieruchomości i Inwestycji - NI**

- rejestr decyzji ustalającej opłatę od wzrostu wartości nieruchomości w związku z uchwaleniem mpzp

- zbiór postępowań o opłaty z tytułu wzrostu wartości nieruchomości w wyniku podziału

- zbiór użytkowników wieczystych

- zbiór dzierżawców

- rejestr umów użyczenia

- rejestr odszkodowań za nieruchomości przejęte pod drogi publiczne

- rejestr kupna nieruchomości

- rejestr sprzedaży nieruchomości

- numeracja porządkowa nieruchomości

- decyzje o ustaleniu lokalizacji inwestycji celu publicznego

- zezwolenie na lokalizację zjazdu

- zezwolenie na lokalizowanie w pasie drogowym obiektów budowlanych lub urządzeń niezwiązanych z potrzebami zarządzania drogami lub potrzebami ruchu drogowego

- zezwolenie na zajęcie pasa drogowego w celu prowadzenia robót

- zezwolenie na zajęcie pasa drogowego i ustalenie opłaty za umieszczenie urządzenia infrastruktury technicznej niezwiązanej z potrzebami zarządzania drogami lub potrzebami ruchu drogowego

- zezwolenie na zajęcie pasa drogowego w celu umieszczenia reklamy

- prowadzenie czynności związanych z ustaleniem wpływu realizacji inwestycji na środowisko

- prowadzenie czynności związanych z ochroną zabytków i opieką nad zabytkami

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **CNI** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 5 | 5 | 3,33 | 4 | **8** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 3 | 2 | 1,67 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 5 | 5 | 5 | 5 | **15** |
| **Utrata dostępu do nośnika z danymi** |  | 3 | 1 | 1 | 1 | 1 | 1 | **3** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 4 | 2 | 2 | 2,67 | 3 | **6** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 1 | 2 | 0 | 0 | 0,67 | 1 | **1** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 0 | 0 | 0,67 | 1 | **1** |
| **Włamanie do systemu informatycznego** |  | 2 | 4 | 1 | 1 | 2 | 2 | **4** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 1 | 3 | 3 | 2,33 | 3 | **3** |
| **Kopiowanie danych** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 2 | 1 | 2 | 2 | 1,67 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 0 | 1 | 0,67 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 0 | 1 | 0,67 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 4 | 4 | 3 | 3 | **3** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Uszkodzenie fizyczne nośnika danych** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Awaria systemu operacyjnego** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Awaria zasilania** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |

**Analiza Ryzyka -**  **czynności przetwarzania - forma papierowa:**

**Wydział Promocji, informacji i komunikacji społecznej**

- umowy zlecenia

- wnioski o udzielenie informacji publicznej

-Oświadczenia majątkowe i inne oświadczenia o osobach zatrudnionych i członkach ich rodzin

- Ewidencja skazanych odbywających karę pracy na cele społeczne

- Akta i sprawy osobowe pracowników

- Staże, praktyki, wolontariat

- Petycje wpływające do Wójta

**-** Zapotrzebowanie i nabór kandydatów do pracy

- Konkursy dla NGO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **PIK** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 3 | 3 | 2 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kradzież dokumentów** |  | 1 | 3 | 3 | 3 | 3 | 3 | **3** |
| **Zgubienie dokumentów** |  | 2 | 1 | 2 | 2 | 1,67 | 2 | **4** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 2 | 2 | 2 | 2 | 2 | 2 | **4** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 1 | 1  | 2 | 1 | 1,33 | 2 | **2** |

**Analiza ryzyka – zasoby w postaci elektronicznej**

**Wydział Promocji, informacji i komunikacji społecznej**

- umowy zlecenia

- Wnioski o udzielenie informacji publicznej

-Oświadczenia majątkowe i inne oświadczenia o osobach zatrudnionych i członkach ich rodzin

- Ewidencja skazanych odbywających karę pracy na cele społeczne

- Akta i sprawy osobowe pracowników

- Staże, praktyki, wolontariat

- Petycje wpływające do Wójta

**-** Zapotrzebowanie i nabór kandydatów do pracy

- Konkursy dla NGO

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **CPIK** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 1 | 1 | 2,33 | 3 | **9** |
| **Utrata dostępu do nośnika z danymi** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 2 | 2 | 2 | 2 | 2 | **4** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Włamanie do systemu informatycznego** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kopiowanie danych** |  | 2 | 2 | 0 | 0 | 0,67 | 1 | **2** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 1 | 1 | 2 | 2 | 1,67 | 2 | **2** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Uszkodzenie fizyczne nośnika danych** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |
| **Awaria systemu operacyjnego** |  | 3 | 0 | 1 | 1 | 0,67 | 1 | **3** |
| **Awaria zasilania** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |

**Analiza Ryzyka -**  **czynności przetwarzania - forma papierowa:**

**Wydział Rolnictwa i Ochrony Środowiska**

- prowadzenie ewidencji zbiorników bezodpływowych i przydomowych oczyszczalni ścieków

- ewidencja zgłoszeń zamiaru usunięcia drzew oraz wniosków o zezwolenie na usunięcie drzew i krzewów

- ochrona p-poż - ewidencja szkoleń, badań lekarskich, uprawnień kierowców, konkursy i turnieje

- ewidencja wyrobów zawierających azbest i miejsc ich występowania

- ewidencja pozwoleń na uprawę maku i konopi

- kontrola przestrzegania "uchwał antysmogowych"

- zarządzanie kryzysowe

- ochrona zwierząt: ewidencja zezwoleń na utrzymywanie psów ras agresywnych, ewidencja decyzji o odbiorze zwierząt, Roczny Program opieki nad zwierzętami bezdomnymi i zapobiegania bezdomności

- wnioski interesantów i korespondencja - Poznański Związek Spółek Wodnych

- pozwolenia wodnoprawne – udział w postępowaniu, opiniowanie

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **ROŚ** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 3 | 3 | 2 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 3 | 1,67 | 2 | **2** |
| **Kradzież dokumentów** |  | 2 | 3 | 3 | 4 | 3,33 | 4 | **8** |
| **Zgubienie dokumentów** |  | 2 | 3 | 2 | 4 | 3 | 3 | **6** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 1 | 3 | 2 | 3 | 2,67 | 3 | **3** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 1 | 3 | 1 | 1 | 1,67 | 2 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 3 | 1 | 1 | 1,67 | 2 | **2** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 2 | 1  | 2 | 1 | 1,33 | 2 | **4** |

**Analiza ryzyka – zasoby w postaci elektronicznej**

**Wydział Rolnictwa i Ochrony Środowiska**

- prowadzenie ewidencji zbiorników bezodpływowych i przydomowych oczyszczalni ścieków

- ewidencja zgłoszeń zamiaru usunięcia drzew i wniosków o zezwolenie na usunięcie drzew i krzewów

- ochrona p-poż - ewidencja szkoleń, badań lekarskich, uprawnień kierowców, konkursy i turnieje

- ewidencja wyrobów zawierających azbest i miejsc ich występowania

- ewidencja pozwoleń na uprawę maku i konopi

- kontrola przestrzegania "uchwał antysmogowych"

- zarządzanie kryzysowe

- ochrona zwierząt: ewidencja zezwoleń na utrzymywanie psów ras agresywnych, ewidencja decyzji o odbiorze zwierząt, Roczny Program opieki nad zwierzętami bezdomnymi i zapobiegania bezdomności

- wnioski interesantów i korespondencja - Poznański Związek Spółek Wodnych

- pozwolenia wodnoprawne – udział w postępowaniu, opiniowanie

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **CROŚ** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 1 | 1 | 2,33 | 3 | **9** |
| **Utrata dostępu do nośnika z danymi** |  | 3 | 1 | 1 | 1 | 1 | 1 | **3** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 2 | 2 | 2 | 2 | 2 | **4** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Włamanie do systemu informatycznego** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kopiowanie danych** |  | 2 | 2 | 0 | 0 | 0,67 | 1 | **2** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 1 | 1 | 2 | 2 | 1,67 | 2 | **2** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Uszkodzenie fizyczne nośnika danych** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |
| **Awaria systemu operacyjnego** |  | 3 | 0 | 1 | 1 | 0,67 | 1 | **3** |
| **Awaria zasilania** |  | 2 | 0 | 1 | 2 | 1 | 1 | **2** |

**Analiza Ryzyka -**  **czynności przetwarzania - forma papierowa:**

**Wydział Spraw Obywatelskich i USC**

* Ewidencja ludności,
* zgromadzenia publiczne,
* wybory - Rejestr Wyborców,
* profil zaufany,
* realizacja zadań dotyczących dowodu osobistego,
* realizacja zadań z zakresu CEIDG,
* realizacja zadań z zakresu powszechnego obowiązku obrony RP,
* ustalanie uprawnień do najmu lokali z mieszkaniowego zasobu gminy,
* dane osobowe świadczeniobiorców 300+ i ich rodzin,
* dane osobowe świadczeniobiorców 500+ i ich rodzin,
* Urząd Stanu Cywilnego,
* archiwum zakładowe,
* Karta Dużej Rodziny,
* realizacja zadań powiązanych z zezwoleniami na sprzedaż napojów alkoholowych,
* testamenty.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **SO** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 5 | 5 | 3,33 | 4 | **8** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 3 | 2 | 1,67 | 2 | **2** |
| **Kradzież dokumentów** |  | 1 | 4 | 5 | 3 | 4 | 4 | **4** |
| **Zgubienie dokumentów** |  | 2 | 4 | 4 | 3 | 3,67 | 4 | **8** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 1 | 4 | 4 | 2 | 3,33 | 4 | **4** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 2 | 3 | 0 | 0 | 1 | 1 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 0 | 1 | 0,67 | 1 | **1** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 2 | 1  | 2 | 2 | 1,67 | 2 | **4** |

**Analiza ryzyka – zasoby w postaci elektronicznej**

**Wydział Spraw Obywatelskich i USC**

* Ewidencja ludności,
* zgromadzenia publiczne,
* wybory - Rejestr Wyborców,
* profil zaufany,
* realizacja zadań dotyczących dowodu osobistego,
* realizacja zadań z zakresu CEIDG,
* realizacja zadań z zakresu powszechnego obowiązku obrony RP,
* ustalanie uprawnień do najmu lokali z mieszkaniowego zasobu gminy,
* dane osobowe świadczeniobiorców 300+ i ich rodzin,
* dane osobowe świadczeniobiorców 500+ i ich rodzin,
* Urząd Stanu Cywilnego,
* archiwum zakładowe,
* Karta Dużej Rodziny,
* realizacja zadań powiązanych z zezwoleniami na sprzedaż napojów alkoholowych,
* testamenty.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **CSO** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 5 | 5 | 3,33 | 4 | **8** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 3 | 2 | 1,67 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 5 | 5 | 5 | 5 | **15** |
| **Utrata dostępu do nośnika z danymi** |  | 3 | 1 | 1 | 1 | 1 | 1 | **3** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 4 | 2 | 2 | 2,67 | 3 | **6** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 1 | 2 | 0 | 0 | 0,67 | 1 | **1** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 0 | 0 | 0,67 | 1 | **1** |
| **Włamanie do systemu informatycznego** |  | 2 | 4 | 1 | 1 | 2 | 2 | **4** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 1 | 3 | 3 | 2,33 | 3 | **3** |
| **Kopiowanie danych** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 2 | 1 | 2 | 2 | 1,67 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 0 | 1 | 0,67 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 0 | 1 | 0,67 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 4 | 4 | 3 | 3 | **3** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Uszkodzenie fizyczne nośnika danych** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Awaria systemu operacyjnego** |  | 3 | 0 | 4 | 4 | 2,67 | 3 | **9** |
| **Awaria zasilania** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |

**Analiza Ryzyka -**  **czynności przetwarzania - forma papierowa:**

**Wydział Planowania Przestrzennego i Przetwarzania Danych – PPPD**

-Rejestr zaświadczeń z miejscowego planu zagospodarowania przestrzennego oraz wypisy i wyrysy z MPZP

- Rejestr wniosków o zmianę studium uwarunkowań i kierunków zagospodarowania przestrzennego

- Rejestr wniosków o opracowanie/ zmianę miejscowego planu zagospodarowania przestrzennego

- Ustalenia sporządzanych/ zmienianych studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy

- Ustalenia planów miejscowych zagospodarowania przestrzennego

- Rejestr wydanych decyzji o warunkach zabudowy

- Zbiór postępowań podziałowych

- Zbiór postępowań w sprawie rozgraniczenia nieruchomości, scalenie nieruchomości

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **PPPD** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 5 | 5 | 3,33 | 4 | **8** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 3 | 2 | 1,67 | 2 | **2** |
| **Kradzież dokumentów** |  | 1 | 4 | 5 | 3 | 4 | 4 | **4** |
| **Zgubienie dokumentów** |  | 2 | 4 | 4 | 3 | 3,67 | 4 | **8** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 1 | 4 | 4 | 2 | 3,33 | 4 | **4** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 2 | 3 | 0 | 0 | 1 | 1 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 3 | 2 | 0 | 0 | 0,67 | 1 | **3** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 0 | 1 | 0,67 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 0 | 1 | 0,67 | 1 | **1** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 2 | 1  | 2 | 2 | 1,67 | 2 | **4** |

**Analiza ryzyka – zasoby w postaci elektronicznej**

**Wydział Planowania Przestrzennego i Przetwarzania Danych – PPPD**

- Rejestr zaświadczeń z miejscowego planu zagospodarowania przestrzennego oraz wypisy i wyrysy z MPZP

- Rejestr wniosków o zmianę studium uwarunkowań i kierunków zagospodarowania przestrzennego

- Rejestr wniosków o opracowanie/ zmianę miejscowego planu zagospodarowania przestrzennego

- Ustalenia sporządzanych/ zmienianych studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy

- Ustalenia planów miejscowych zagospodarowania przestrzennego

- Rejestr wydanych decyzji o warunkach zabudowy

- Zbiór postępowań podziałowych

- Zbiór postępowań w sprawie rozgraniczenia nieruchomości, scalenie nieruchomości

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **C****PPPD** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 5 | 5 | 3,33 | 4 | **8** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 3 | 2 | 1,67 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 5 | 5 | 5 | 5 | **15** |
| **Utrata dostępu do nośnika z danymi** |  | 3 | 1 | 1 | 1 | 1 | 1 | **3** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 4 | 2 | 2 | 2,67 | 3 | **6** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 1 | 2 | 0 | 0 | 0,67 | 1 | **1** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 0 | 0 | 0,67 | 1 | **1** |
| **Włamanie do systemu informatycznego** |  | 2 | 4 | 1 | 1 | 2 | 2 | **4** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 1 | 3 | 3 | 2,33 | 3 | **3** |
| **Kopiowanie danych** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 2 | 1 | 2 | 2 | 1,67 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 0 | 1 | 0,67 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 0 | 1 | 0,67 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 4 | 4 | 3 | 3 | **3** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Uszkodzenie fizyczne nośnika danych** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Awaria systemu operacyjnego** |  | 2 | 0 | 4 | 4 | 2,67 | 3 | **6** |
| **Awaria zasilania** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |

**Analiza Ryzyka -**  **czynności przetwarzania - forma papierowa:**

**Wydział Podatków i Opłat – OP**

- Rejestr aktów notarialnych

- Podatki i opłaty lokalne

- Rejestr zobowiązanych do zapłaty należności cywilno-prawnych oraz innych opłat

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|   | **OP** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 3 | 3 | 2 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 3 | 1,67 | 2 | **2** |
| **Kradzież dokumentów** |  | 2 | 3 | 3 | 4 | 3,33 | 4 | **8** |
| **Zgubienie dokumentów** |  | 2 | 3 | 2 | 4 | 3 | 3 | **6** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** |  | 1 | 3 | 2 | 3 | 2,67 | 3 | **3** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 1 | 3 | 1 | 1 | 1,67 | 2 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 3 | 1 | 1 | 1,67 | 2 | **2** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Błędy w obiegu dokumentów** |  | 2 | 1  | 2 | 1 | 1,33 | 2 | **4** |

**Analiza ryzyka – zasoby w postaci elektronicznej**

**Wydział Podatków i Opłat - OP**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **COP** | **Prawdopodobieństwo****(P)** | **Skutek dla:**1. **Poufności**
2. **Dostępności**
3. **Integralności**
 | **Średnia** | **Skutek****(S)** | **Ryzyko****(R=P\*S)** |
| **Pożar** |  | 2 | 0 | 2 | 2 | 1,33 | 2 | **4** |
| **Zalanie pomieszczenia** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kradzież komputera (dysku twardego)** |  | 3 | 5 | 1 | 1 | 2,33 | 3 | **9** |
| **Utrata dostępu do nośnika z danymi** |  | 3 | 1 | 1 | 1 | 1 | 1 | **3** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** |  | 2 | 2 | 2 | 2 | 2 | 2 | **4** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** |  | 2 | 2 | 1 | 1 | 1,33 | 2 | **4** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** |  | 1 | 2 | 1 | 1 | 1,33 | 2 | **2** |
| **Włamanie do systemu informatycznego** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Wyłudzenie haseł dostępu** |  | 1 | 2 | 2 | 2 | 2 | 2 | **2** |
| **Nieuprawnione instalowanie urządzeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Nieuprawniona modyfikacja używanego oprogramowania** |  | 1 | 0 | 2 | 2 | 1,33 | 2 | **2** |
| **Kopiowanie danych** |  | 2 | 2 | 0 | 0 | 0,67 | 1 | **2** |
| **Korzystanie z nielicencjonowanego oprogramowania** |  | 1 | 1 | 2 | 2 | 1,67 | 2 | **2** |
| **Nieuprawniony dostęp do pomieszczeń** |  | 2 | 1 | 1 | 1 | 1 | 1 | **2** |
| **Włamanie do pomieszczeń** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Utrata danych podczas napraw sprzętu** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** |  | 1 | 1 | 1 | 1 | 1 | 1 | **1** |
| **Uszkodzenia sprzętu komputerowego** |  | 2 | 0 | 1 | 1 | 0,67 | 1 | **2** |
| **Uszkodzenie fizyczne nośnika danych** |  | 1 | 0 | 1 | 1 | 0,67 | 1 | **1** |
| **Awaria systemu operacyjnego** |  | 3 | 0 | 1 | 1 | 0,67 | 1 | **3** |
| **Awaria zasilania** |  | 2 | 0 | 1 | 2 | 1 | 1 | **2** |

Ponadto dla skutecznej realizacji zadań związanych z minimalizacją ryzyka należy zwracać szczególną uwagę na:

1. **SPRZĘT**
* Nieuprawnione kopiowanie danych z dysku twardego,
* Korzystanie z oprogramowań nie posiadających licencji,
* Uszkodzenie sprzętu komputerowego (drukarka, karta sieciowa, jednostka centralna, klawiatura, mysz itp.) oraz łączy transmisyjnych,
* Uszkodzenie fizyczne nośników danych,
* Starzenie się nośników,
* Wejście do systemu operacyjnego z wykorzystaniem obcego identyfikatora.

**Nieuprawniony dostęp do procesu przetwarzania danych :**

* Włamanie do pomieszczeń po godzinach pracy.
1. **LUDZIE**
* Kradzież dokumentów papierowych lub elektronicznych przechowywanych na stanowiskach pracy,
* Kradzież dysku twardego komputera,
* Zagubienie dokumentów lub utrata w czasie awarii , pożaru, zalania itp.,
* Zagubienie dokumentów lub utrata przetwarzanych danych osobowych,
* Stosowanie korupcji , szantażu w celu wydobycia określonych informacji od pracowników jednostki,
* Infiltracja środowiska przez wyszukiwanie osób uważających się za pokrzywdzonych przez pracodawcę, zwalnianych lub poszukujących zatrudnienia w innej komórce,
* Podglądanie zawartości danych znajdujących się na ekranie monitora,
* Włamanie do systemu – podszycie się pod uprawnionego użytkownika,
* Wyłudzenie , fałszowanie dokumentów, kart dostępu , haseł dostępu itp.,
* Nieuprawniona świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
* Skorzystanie z cudzego identyfikatora i hasła,
* Błędy popełniane przez użytkowników,
* Wejście osoby nieupoważnionej do strefy przetwarzania danych osobowych,
* Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych , konserwacji sprzętu ,
* Odczytanie danych z nośników przewidzianych do naprawy,
* Podgląd danych przetwarzanych przez poprzedniego użytkownika,
* Zapisywanie danych na prywatne nośniki użytkownika,
* Nieuprawnione kopiowanie danych,
* Przeglądanie (przeszukiwanie) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji,
* Pozostawienie przez pracownika dokumentów , nośników informacji na biurku po godzinach pracy,
* Utrata kluczowych pracowników,
* Brak możliwości rozliczania działań użytkowników – brak kontroli nad dostępem do przetwarzanych danych osobowych,
* Dostęp do informacji przez osoby nieuprawnione podczas ponownego wykorzystania używanych nośników danych,
* Obserwacja bezpośrednia poprze filmowanie, fotografowanie, nagrywanie .
1. **APLIKACJE**
* Nieuprawnione instalowanie urządzeń służących do naruszenia poufności przetwarzanych informacji,
* Nieuprawniona , świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
* Korzystanie z nielicencjonowanego oprogramowania,
* Przypadkowa zmiana ustawień konfiguracyjnych ,
* Stosowanie niewłaściwego systemu plików,
* Wykorzystanie przechowywanych dokumentów na dysku twardym,
1. **POMIESZCZENIA**
* Katastrofy budowlane,
* Ekstremalne czynniki środowiskowe (temperatura, wilgotność, zapylenie),
* Awaria klimatyzacji ,
* Pożar w pomieszczeniach, w których są przetwarzane dane osobowe,
* Zalanie pomieszczeń , w których są przetwarzane dane osobowe,
* Zamach terrorystyczny,
1. **DODATKOWE INNE NIEBEZPIECZEŃSTWA**
* Celowe lub przypadkowe zniszczenie zbiorów i programów zewnętrznym impulsem elektromagnetycznym,
* Podsłuch emisji akustycznych na zewnątrz budynku z obszaru przetwarzania danych osobowych,
* Awaria zasilania,
* Awaria systemu operacyjnego lub ujawnienie wady oprogramowania aplikacyjnego,
* Zbieranie się ładunków elektrostatycznych,
* Nierzetelna kontrola rejestrowanych zdarzeń systemowych,
* Wykorzystanie błędów w obiegu dokumentów,
* Ponowne wykorzystywanie nośników , które powinny być wcześniej skutecznie zniszczone ,
* Nieprawidłowości w przypadku kserowania , powielania – brak nadzoru lub uprawnień,
* Niepełny , niedokładny opis procedur w instrukcjach bezpiecznej eksploatacji.

**Wyniki analizy ryzyka – zasoby w formie papierowej**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ZAGROŻENIA** | **ORG** | **NI** | **PIK** | **ROŚ** | **SO** | **PPPD** | **OP** | **ŚREDNIA** | **RANKING** |
| **Zgubienie dokumentów** | **4** | **8** | **4** | **6** | **8** | **8** | **6** | **6,29** | **1** |
| **Pożar** | **4** | **8** | **4** | **4** | **8** | **8** | **4** | **5,71** | **2** |
| **Kradzież dokumentów** | **3** | **4** | **3** | **8** | **4** | **4** | **8** | **4,86** | **3** |
| **Wykorzystywanie zużytych wydruków (zamiast zniszczenia)** | **4** | **4** | **4** | **4** | **4** | **4** | **4** | **4** | **4** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż)** | **4** | **4** | **4** | **3** | **4** | **4** | **3** | **3,71** | **5** |
| **Podgląd dokumentów przetwarzanych przez innego użytkownika** | **4** | **3** | **4** | **4** | **4** | **3** | **4** | **3,71** | **5** |
| **Błędy w obiegu dokumentów** | **2** | **4** | **2** | **4** | **4** | **4** | **4** | **3,43** | **6** |
| **Zalanie pomieszczenia** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **7** |
| **Wgląd do danych przez osobę nieupoważnioną do przetwarzania (w tym obserwacja, filmowanie, fotografowanie)** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **7** |
| **Nieuprawniony dostęp do pomieszczeń** | **1** | **2** | **1** | **2** | **1** | **2** | **2** | **1,57** | **8** |
| **Włamanie do pomieszczeń** | **1** | **1** | **1** | **2** | **1** | **1** | **2** | **1,28** | **9** |

W przypadku danych osobowych przetwarzanych w formie papierowej poziom wysoki ryzyka osiągnięto dla następujących zagrożeń:

1. Zgubienie dokumentów (**NI, SO, PPPD**)

2. Pożar (**NI, SO, PPPD**)

3. Kradzież dokumentów (**ROŚ, OP**)

**1. Zgubienie dokumentów**

 W przypadku Wydziału **NI** wysoki poziom ryzyka w sytuacji zgubienia dokumentów wynika z tego, że istnieje ryzyko pozostawienia dokumentacji projektowej np. na budowie czy
w Starostwie Powiatowym. Jednak kopie zapasowe dokumentacji są na komputerach
i serwerach.

W przypadku Wydziału **SO** wysoki poziom zagrożenia dla dokumentów w sytuacji zgubienia dokumentów wynika z tego, że obecnie podczas epidemii COVID -19 został utworzony osobny punkt obsługi interesanta, który mieści się w drugim budynku Urzędu Gminy. Dokumenty spraw obywatelskich i USC są przenoszone do tego punktu, co niesie ze sobą ryzyko zgubienia dokumentów. Sytuacja wróci do normy po ustaniu epidemii.

W przypadku Wydziału **PPPD** wysoki poziom zagrożenia dla dokumentów w sytuacji zgubienia dokumentów wynika z tego, że istnieje ryzyko pozostawienia dokumentacji projektowej np. w Urzędzie Wojewódzkim . Jednak kopie zapasowe dokumentacji są na komputerach i serwerach.

**2. Pożar**

Wysoki poziom zagrożenia dla dokumentów **NI** w sytuacji wybuchu pożaru wynika
z tego, że gdyby doszło do spalenia całej dokumentacji papierowej, nie wszystkie dokumenty posiadają kopie na serwerach np. mapy projektowe. ( alternatywą na odzyskanie map jest geodeta ).

 Wysoki poziom zagrożenia dla dokumentów w sytuacji wybuchu pożaru wynika z tego, że gdyby doszło do spalenia wszystkich dokumentów **SO** i USC j kopie zapasowe znajdują się na serwerach zakładając, że pożar nie zajmie piętra urzędu, na którym znajduje się Serwerownia.

 Wysoki poziom zagrożenia dla dokumentów **PPPD** w sytuacji wybuchu pożaru wynika
z tego, że gdyby doszło do spalenia całej dokumentacji papierowej, nie wszystkie dokumenty posiadają kopie na serwerach np. mapy projektowe (alternatywą na odzyskanie map jest projektant urbanista).

**W przypadku spalenia się Serwerowni istnieje szansa na odzyskanie bazy danych, ponieważ trzy razy w tygodniu dokonywana jest kopia danych naprzemiennie na dwa dyski zewnętrzne. Dyski przechowywane są w osobnej metalowej szafie w osobnym pomieszczeniu.**

**3. Kradzież dokumentów**

W przypadku Wydziału **ROŚ** wysoki poziom zagrożenia dla dokumentacji w sytuacji kradzieży dokumentów wynika z tego, że w elektronicznym systemie obiegu dokumentów skanowane są tylko pierwsze strony bez załączników. Jednak dodatkowe zabezpieczenia
w postaci monitoringu urzędu, biuro i szafy zamykane na klucz zmniejszają to ryzyko.

W przypadku Wydziału **OP** wysoki poziom zagrożenia dla dokumentów w sytuacji kradzieży dokumentów wynika z tego, że jeden raz taka sytuacja miała miejsce. Doszło do kradzieży laptopa, który był w dyspozycji pracownika poza Urzędem. Od tego czasu laptopy pozostają tylko w budynku urzędu.

**Wyniki analizy ryzyka – zasoby w formie elektronicznej**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ZAGROŻENIA** | **CORG** | **CNI** | **CPIK** | **CROŚ** | **CSO** | **CPPPD** | **COP** | **ŚREDNIA** | **RANKING** |
| **Kradzież komputera (dysku twardego)** | **9** | **15** | **9** | **9** | **15** | **15** | **9** | **11,57** | **1** |
| **Pożar** | **4** | **8** | **4** | **4** | **8** | **8** | **4** | **5,71** | **2** |
| **Celowe działania pracownika na szkodę organizacji (sabotaż, man in the middle)** | **4** | **6** | **4** | **4** | **6** | **6** | **4** | **4,86** | **3** |
| **Awaria systemu operacyjnego** | **3** | **6** | **3** | **3** | **9** | **6** | **3** | **4,71** | **4** |
| **Utrata danych podczas napraw sprzętu** | **2** | **6** | **2** | **2** | **6** | **6** | **2** | **3,71** | **5** |
| **Uszkodzenia sprzętu komputerowego** | **2** | **6** | **2** | **2** | **6** | **6** | **2** | **3,71** | **5** |
| **Włamanie do systemu informatycznego** | **2** | **4** | **2** | **2** | **4** | **4** | **2** | **2,86** | **6** |
| **Kopiowanie danych** | **2** | **4** | **2** | **2** | **4** | **4** | **2** | **2,86** | **6** |
| **Korzystanie z nielicencjonowanego oprogramowania** | **2** | **4** | **2** | **2** | **4** | **4** | **2** | **2,86** | **6** |
| **Obserwacja bezpośrednia (w tym filmowanie, fotografowanie)** | **4** | **1** | **4** | **4** | **1** | **1** | **4** | **2,71** | **7** |
| **Utrata dostępu do nośnika z danymi** | **2** | **3** | **2** | **3** | **3** | **3** | **3** | **2,71** | **7** |
| **Nieuprawniona modyfikacja używanego oprogramowania** | **2** | **3** | **2** | **2** | **3** | **3** | **2** | **2,43** | **8** |
| **Uszkodzenie fizyczne nośnika danych** | **1** | **4** | **1** | **1** | **4** | **4** | **1** | **2,29** | **9** |
| **Nieuprawniony dostęp do pomieszczeń** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **10** |
| **Zalanie pomieszczenia** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **10** |
| **Wyłudzenie haseł dostępu** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **10** |
| **Nieuprawnione instalowanie urządzeń** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **10** |
| **Odczytanie informacji z nośników przeznaczonych do naprawy** | **1** | **3** | **1** | **1** | **3** | **3** | **1** | **1,86** | **11** |
| **Podglądanie zawartości ekranu monitora przez osoby nieuprawnione** | **2** | **1** | **2** | **2** | **1** | **1** | **2** | **1,57** | **12** |
| **Awaria zasilania** | **2** | **1** | **2** | **2** | **1** | **1** | **2** | **1,57** | **12** |
| **Włamanie do pomieszczeń** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **13** |

1. W przypadku danych osobowych przetwarzanych w formie elektronicznej poziom krytyczny ryzyka osiągnięto dla następujących zagrożeń:

 1. Kradzież komputera - dysku twardego ( **NI, SO, PPPD**)

1. W przypadku danych osobowych przetwarzanych w formie elektronicznej poziom wysoki ryzyka osiągnięto dla następujących zagrożeń:

 1. Kradzież komputera- dysku twardego **( ORG, PIK,ROŚ,OP )**

 2. Pożar **( SO, PPPD )**

1. Awaria systemu operacyjnego **( SO )**
2. **Poziom krytyczny**
3. **Kradzież komputera - dysku twardego**

 W przypadku Wydziału **NI** krytyczny poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że gdyby doszło do takiej sytuacji istnieje duże ryzyko wycieku danych związanych z czynnościami wydziału Nieruchomości i Inwestycji.

Komputery są zabezpieczone hasłem i pomieszczenia zamykane są na klucz.

 W przypadku Wydziału **SO** krytyczny poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że gdyby doszło do takiej sytuacji istnieje duże ryzyko wycieku danych wrażliwych mieszkańców, które są przetwarzane w wydziale Spraw Obywatelskich i Urzędu Stanu Cywilnego.

Komputery są zabezpieczone hasłem i pomieszczenia zamykane są na klucz.

W przypadku Wydziału **PPPD** krytyczny poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że gdyby doszło do takiej sytuacji istnieje duże ryzyko wycieku danych związanych z czynnościami wydziału Planowania Przestrzennego i Przetwarzania Danych.

Komputery są zabezpieczone hasłem i pomieszczenia zamykane są na klucz.

**II Poziom wysoki**

1. **Kradzież komputera- dysku twardego**

 W przypadku Wydziału **ORG** wysoki poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że istnieje ryzyko kradzieży laptopa podczas Sesji Rady Gminy, która odbywa się poza budynkiem urzędu. Często w Sesji biorą udział różne osoby z zewnątrz.

 W przypadku Wydziału **PIK** wysoki poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że istnieje ryzyko kradzieży laptopa podczas Sesji Rady Gminy, która odbywa się poza budynkiem urzędu.

 W przypadku Wydziału **ROŚ** wysoki poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że w elektronicznym systemie obiegu dokumentów skanowane są tylko pierwsze strony bez załączników. W przypadku kradzieży nie ma dostępu do pełnej dokumentacji. Ryzyko jednak maleje, ponieważ w urzędzie jest monitoring, w ostatnim czasie zamontowano dodatkowe odgrodzenie od części budynku urzędu. Interesanci są przyjmowani wyłącznie w holu głównym. Biuro jest zamykane na klucz.

 W sytuacji gdyby doszło do kradzieży laptopa – ryzyko istnieje, ponieważ pracownik odpowiedzialny za Zarządzanie Kryzysowe ma laptopa przy sobie, wówczas kopie zapasowe dokumentów są na serwerach.

 W przypadku Wydziału **OP** wysoki poziom zagrożenia dla dokumentów w sytuacji kradzieży komputera wynika z tego, że jeden raz taka sytuacja miała miejsce. Doszło do kradzieży laptopa, który był w dyspozycji pracownika poza Urzędem. Od tego czasu laptopy wydziału Podatków i Opłat pozostają tylko w budynku urzędu.

1. **Pożar**

 Wysoki poziom zagrożenia dla dokumentów w sytuacji wybuchu pożaru wynika z tego, że gdyby doszło do spalenia wszystkich dokumentów **SO** **i USC** jedyne kopie zapasowe znajdują się na serwerach zakładając, że pożar nie zajmie piętra urzędu, na którym znajduje się Serwerownia.
W przypadku spalenia się Serwerowni istnieje szansa na odzyskanie bazy danych, ponieważ trzy razy w tygodniu dokonywana jest kopia danych na dwa dyski zewnętrzne. Dyski przechowywane są
w osobnej metalowej szafie w osobnym pomieszczeniu.

 Wysoki poziom zagrożenia dla dokumentów **PPPD** w sytuacji wybuchu pożaru wynika
z tego, że gdyby doszło do spalenia całej dokumentacji papierowej, nie wszystkie dokumenty posiadają kopie na serwerach np. mapy projektowe (alternatywą na odzyskanie map jest projektant urbanista).

1. **Awaria systemu operacyjnego**

W przypadku Wydziału **SO** wysoki poziom zagrożenia dla dokumentów w sytuacji awarii systemu operacyjnego wynika z tego, że gdy dojdzie do awarii systemu to w danym momencie nie można zrobić nic, dotyczy to np. programu IZYDA do obsługi wniosków na świadczenia 500+. Pozostałe programy komputerowe spraw obywatelskich i USC zabezpiecza minister.

**OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH**

Warszawa, dnia 8 lipca 2019 r.

Poz. 666

**KOMUNIKAT**

**PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH**

z dnia 17 czerwca 2019 r.

**w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony**

 Na podstawie art. 54 ust. 1 pkt 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669oraz z 2019 r. poz. 730) w związku z art. 35 ust. 4 i 6 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 119 z 04.05.2016, str. 1 oraz L 127 z 23.05.2018, str. 2) ogłasza się, co następuje:

1) ogłasza się wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 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) – wykaz określa załącznik do komunikatu;

2) wykaz, o którym mowa w pkt 1, uchyla zawarty w komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. poz. 827), wykaz nieobejmujący czynności przetwarzania związanych z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach

członkowskich Unii Europejskiej.

 Prezes Urzędu Ochrony Danych Osobowych: *J. Nowak*

**WYKAZ RODZAJÓW OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH WYMAGAJĄCYCH PRZEPROWADZENIA OCENY SKUTKÓW PRZETWARZANIA DLA ICH OCHRONY**

Poniższy wykaz zawiera rodzaje operacji przetwarzania, które w opinii Urzędu Ochrony Danych Osobowych wymagają oceny skutków dla ochrony danych. Wykaz ten został opracowany
w ramach realizacji obowiązku nałożonego na Urząd Ochrony Danych Osobowych na podstawie art. 35 ust. 4 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) jako polski organ nadzorczy.

Wykaz ten nie zwalnia administratora z obowiązku przeanalizowania wszelkich operacji przetwarzania danych w oparciu o pełną ocenę skutków dla ochrony danych na podstawie art. 35 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). Wykaz został opracowany w oparciu o wytyczne Grupy Roboczej Artykułu 29 (WP 248) „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie «może powodować wysokie ryzyko» do celów rozporządzenia 2016/679. Wykaz ten uzupełnia i konkretyzuje powyższe wytyczne.

|  |  |  |
| --- | --- | --- |
| **I. Rodzaje/kryteria dla****operacji przetwarzania, dla****których wymagane jest przeprowadzenie oceny** | **II. Potencjalne obszary wystąpienia/ istniejące obszary występowań** | **III. Przykłady operacji/zakresu****danych/okoliczności, w których może wystąpić****wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania** |
| **1. Ewaluacja lub ocena,****w tym profilowanie****i przewidywanie (analiza****behawioralna) w celach****wywołujących negatywne****skutki prawne, fizyczne,****finansowe lub inne****niedogodności dla osób fizycznych** | Media społecznościowe, firmy marketingowe,firmy headhunterskieBanki, inne instytucje finansowe upoważnionedo udzielania kredytów, instytucje pożyczkowew procesie oceny zdolności kredytowejFirmy ubezpieczeniowe – oferowanie zniżekzwiązanych ze stylem życia (papierosy, alkohol, sporty ekstremalne, styl jazdy samochodem)Firmy ubezpieczeniowe – np. korzystniejsze oferty ubezpieczeniowe lub kredytowe dla pracowników określonych grup, np. administracji | Profilowanie użytkowników portalispołecznościowych i innych aplikacji w celu wysyłania informacji handlowejOcena zdolności kredytowej, przy użyciualgorytmów sztucznej inteligencji, objętaobowiązkiem zachowania tajemnicy i żądanieujawnienia danych niemających bezpośredniegozwiązku z oceną zdolności kredytowejOcena stylu życia, odżywiania się, jazdy, sposobuspędzania czasu itp. osób fizycznych w celu np.podwyższenia im ceny składki ubezpieczeniowej,na podstawie tej oceny, nazywana ogólnieoptymalizacją składki ubezpieczeniowejProfilowanie pośrednie (ocena osoby na podstawieprzynależności do określonej grupy) |
| **2. Zautomatyzowane****podejmowanie decyzji****wywołujących skutki****prawne, finansowe lub podobne istotne skutki** | Drogi objęte odcinkowym pomiarem prędkości(system gromadzi informacje nie tylko o pojazdach naruszających przepisy, aleo wszystkich pojazdach pojawiających sięw kontrolowanym obszarze), odcinki drógwyposażone w system elektronicznego poboru opłat viaTOLLSklepy internetowe oferujące ceny promocyjnedla określonych grup klientów.Firmy obsługujące programy lojalnościowe(wspólnoty zakupowe)Programy marketingowe zawierające elementyprofilowania osób | Systemy monitoringu wykorzystywanedo zarządzania ruchem, umożliwiające szczegółowynadzór nad kierowcą oraz jego zachowaniem nadrodze, w szczególności systemy pozwalające naautomatyczną identyfikację pojazdówSystemy automatycznego pobierania opłat za wjazdSystemy profilowania klientów pod kątemzidentyfikowania preferencji zakupowych,automatycznego ustalania cen promocyjnychw oparciu o profilMonitorowanie zakupów i preferencji zakupowych(np. alkohol, słodycze) |
| **3. Systematyczne****monitorowanie na dużą****skalę miejsc dostępnych****publicznie wykorzystujące****elementy rozpoznawania****cech lub właściwości****obiektów, które znajdą się****w monitorowanej****przestrzeni. Do tej grupy****systemów nie są zaliczane****systemy monitoringu****wizyjnego, w których obraz****jest nagrywany****i wykorzystywany tylko****w przypadku potrzeby****analizy incydentów****naruszenia prawa** | Środki komunikacji miejskiej, miasta oferującesystemy wypożyczania rowerów, samochodóworaz wyznaczające strefy płatnego parkowaniaZakłady pracy (monitoring systemów informatycznych poczty elektronicznej,używanego oprogramowania, kart dostępowychitp.)Przetwarzanie informacji pozyskiwanych przezInternet rzeczy (opaski medyczne, smartwatcheitp.) oraz ich przesyłanie w sieci przy użyciu urządzeń mobilnych typu smartfon czy tabletSystemy komunikujące się typu maszyna – maszyna, w których samochód informujeotoczenie o swoim zachowaniu (ruchu) i w przypadku pojawiającego się zagrożeniaotrzymuje od tego otoczenia (infrastruktura drogowa, inne samochody) komunikatyostrzegawczeOpinia Europejskiego Komitetu Ekonomiczno- Społecznego w sprawie identyfikacji radiowej (RFID) (2007/C 256/13)Szpitale/Organizacje prowadzące badaniakliniczne.Kluby fitness/ podmioty/ organizacje pobierającemateriał genetyczny do badań | Monitorowanie osób korzystających z usługw przestrzeni publicznej, przy wykorzystaniudanych wykraczających poza dane niezbędnedo świadczenia tych usługSystemy monitorowania czasu pracy pracownikóworaz przepływu informacji w wykorzystywanychprzez nich narzędziach (poczty elektronicznej,Internetu)Kryterium: systematyczne monitorowanie (*vide* WP2491) + wrażliwe podmioty danychGromadzenie i wykorzystywanie danych przezaplikacje instalowane w urządzeniach mobilnych,w tym w urządzeniach zintegrowanychz mundurem, kaskiem lub w inny sposóbpołączonych z osobą pozyskującą daneSystemy monitoringu pojazdów nawiązujące połączenia z otoczeniem, w tym z innymipojazdamiSystemy wykorzystujące RFID w przypadku, gdy znaczniki/etykiety są lub mogą być przypisane osobom fizycznymDane dotyczące zdrowia pacjentów |
| **4. Przetwarzanie****szczególnych kategorii****danych osobowych****i dotyczących wyroków****skazujących i czynów****zabronionych (danych wrażliwych wg opinii WP 29)** | Partie polityczne, komitety wyborcze, komitetyreferendalne i inicjatywy ustawodawcze,organizacje społeczne, kampanie wyborcze Operatorzy telekomunikacyjni ; dostawcy mediów (prąd, gaz, woda) w zakresie inteligentnego opomiarowania – Zalecenie 2012/148/UE Komisji Europejskiej z marca2012 r. w sprawie przygotowańdo rozpowszechniania inteligentnych systemówpomiarowychUsługi poczty elektronicznej; systemymonitoringu osiągnięć sportowychwspółpracujące z opaskami typu fitnesswykorzystujące chmurę obliczeniową; aplikacjedostarczane przez producentów czytnikówelektronicznych do zakupu książek, gazetelektronicznych z funkcjami robienia notatek itp. | Przetwarzanie przez organy państwowe lubpodmioty prywatne danych osobowych dotyczących przynależności partyjnej i/lub preferencji wyborczychRegularne przetwarzanie danych pomiarowychumożliwiające obserwację stylu życia, przemieszczania się w terenie, intensywnościkorzystania z mediów, energii itp. (np. danych geolokalizacyjnych, danych z inteligentnych liczników pomiarowych o zużywanej energii, danych bilingowych dotyczących komunikacji elektronicznej itp.)Serwisy internetowe i inne systemy informatyczneoferowane osobom fizycznym do przetwarzaniainformacji obejmujących działania o charakterzeczysto osobistym lub domowym (jak np. usługiprzetwarzania w chmurze do zarządzaniadokumentami osobistymi, usługi pocztyelektronicznej, kalendarze, e-czytniki wyposażonew funkcje robienia notatek oraz różne aplikacjetypu „life-logging”, które mogą zawieraćinformacje o bardzo osobistym charakterze),których ujawnienie lub przetwarzanie do celówinnych niż czynności ocharakterze domowymmoże być uznane za bardzo ingerujące w prywatność |
| **5. Przetwarzanie danych****biometrycznych wyłącznie****w celu identyfikacji osoby****fizycznej bądź w celu kontroli****dostępu****6. Przetwarzanie danych****genetycznych** | Systemy rozpoznawania twarzy, weryfikacja tożsamości w miejscu pracy w celu kontrolidostępu, weryfikacja tożsamości w urządzeniach/ aplikacjach (wliczającrozpoznawanie głosu, odcisków palców, twarzy); systemy monitoringu wejść do określonych pomieszczeń; klubów fitness, hoteli itp.Laboratoria/Firmy/Szpitale oferującediagnostykę genetyczną | Wejścia do określonych obszarów, pomieszczeń lubuzyskanie dostępu do określonego kontaw systemie informatycznym w celu np. wykonania zlecenia transakcji w systemie teleinformatycznymlub wypłaty gotówki przy użyciu bankomatu itp.Testy DNA, Badania medyczne, badania medyczne |
| **7. Dane przetwarzane na****dużą skalę, gdzie pojęcie****dużej skali dotyczy:****• liczby osób, których dane****są przetwarzane,****• zakresu przetwarzania,****• okresu przechowywania****danych oraz****• geograficznego zakresu****przetwarzania** | Centralny system:– informacji oświatowej;– informacji w szkolnictwie wyższym;– obsługi ubezpieczeń komunikacyjnych;– kwalifikacji zawodowych itp.Portale społecznościowe, przeglądarkiinternetowe, dostawcy usług telewizji kablowej,serwisy subskrypcyjne z filmami i programamitelewizyjnymi dostępne na urządzeniachz dostępem do Internetu | Centralne zbiory danych wspomagające zarządzanie określoną grupą osób w celachzwiązanych z realizacją zadań publicznych, z których dane udostępniane są w różnym zakresie w zależności od ich roli i zadań związanych z realizacją tych obowiązkówZbieranie szerokiego zakresu danycho przeglądanych stronach internetowych,realizowanych zakupach/ historii zakupów,oglądanych programach telewizyjnych lubradiowych |
| **8. Przeprowadzanie****porównań, ocena lub****wnioskowanie na podstawie****analizy danych pozyskanych****z różnych źródeł** | Firmy marketingowe pobierające dane z różnychźródeł, gdzie występują dane osoboweo klientach, w celach przeprowadzaniaukierunkowanych na określone grupy klientówakcji marketingowychFirmy marketingowe w celach doskonalenia i rozszerzania profili potencjalnych klientów oraz doskonalenia usług reklamy ukierunkowanej na określone grupy społeczne;firmy obsługujące programy lojalnościowe (wspólnoty zakupowe) | Łączenie danych z różnych rejestrów państwowychi/lub publicznychTworzenie profili osób ze zbiorów danych pochodzących z różnych źródeł (łączenie zbiorów) |
|  | Portale społecznościowe, sieci handlowe, firmy marketingowe, banki i instytucje finansowe | Zbieranie danych o przeglądanych stronach,wykonywanych operacjach bankowych, zakupachw sklepach internetowych, a następnie ich analiza w celu tworzenia profilu osoby |
| **9. Przetwarzanie danych****dotyczących osób, których****ocena i świadczone im usługi****są uzależnione od****podmiotów lub osób, które****dysponują uprawnieniami****nadzorczymi i/lub ocennymi** | Serwisy oferujące pracę, które dokonują dopasowania ofert do określonych preferencjipracodawcówSystemy służące do zgłaszania nieprawidłowości(whistleblowing) | Przetwarzanie danych, w których dokonuje sięklasyfikacji lub ocen osób, których dane dotyczą,pod względem np. wieku, płci, a następnie klasyfikacje te wykorzystuje się do przedstawienia ofert lub innych działań, które mogą mieć wpływ na prawa lub wolność osób, których dane sąprzetwarzaneSystemy służące do zgłaszania nieprawidłowości(związanych np. z korupcją, mobbingiem) –w szczególności gdy przetwarzane są w nim dane pracowników |
| **10. Innowacyjne****wykorzystanie lub****zastosowanie rozwiązań****technologicznych lub****organizacyjnych** | Sprzedawcy i dystrybutorzy mediów(prąd, gaz, woda, usługi telekomunikacyjne)wdrażający inteligentne licznikiSerwisy internetowe przetwarzające danez urządzeń typu Internet rzeczy, np. aparatówfotograficznych wyposażonych w funkcjelokalizacyjne (GPS)Zastosowanie komunikacji między urządzeniami(Internet rzeczy – np. beacony, drony) w przestrzeni publicznej i w miejscach użyteczności publicznejAplikacje z funkcjami komunikowania sięi oprogramowaniem umożliwiającym wymianęinformacji z najbliższym otoczeniem oraz zdalniepoprzez sieć telekomunikacyjnąZabawki interaktywneSpecjalistyczne porady i konsultacjemedyczne, badania kliniczne o zasięgu międzynarodowym | Systemy zdalnego opomiarowania, które, biorącpod uwagę zakres i częstość zbierania danych,umożliwiają profilowanie osób lub grupy osóbSystemy analizy i przetwarzania danychznajdujących się w metadanych, np. zdjęciaopatrzone danymi geolokalizacyjnymiSystemy stosowane do analizy i przekazywaniadanych dostawcom usługi przy użyciu aplikacjimobilnych z urządzeń przenośnych typu:smartwatch, inteligentne opaski, beacony itp.analizujące i przekazujące dane dostawcom przyużyciu aplikacji mobilnychStosowanie urządzeń wyposażonych w różnegorodzaju interfejsy (głośnik, mikrofon, kamera) orazoprogramowanie i system łączności umożliwiająceprzekazywanie danych poprzez sieci telekomunikacyjneUsługi i zabawki dedykowane dzieciomKonsultacje telemedyczne z ośrodkami spoza UE,przekazywanie osobowych danych medycznych o zasięgu międzynarodowym |
| **11. Gdy przetwarzanie samo****w sobie uniemożliwia****osobom, których dane****dotyczą, wykonywanie****prawa lub korzystanie****z usługi lub umowy** | Podmioty udzielające pożyczek i kredytów oraz oferujące sprzedaż ratalnąSklepy internetowe oraz dostawcy innych usług typu gry, muzyka, loterie itp. | Podejmowanie decyzji kredytowej w stosunku dopotencjalnych klientów na podstawie informacjizawartych w bazach zawierających informacjeo dłużnikach lub podobnych bazach danychUzależnianie możliwości korzystania z usługi odinformacji w zakresie dochodów, kwoty wydatkówmiesięcznych i innych wartości zebranych w wyniku profilowania |
| **12. Przetwarzanie danych****lokalizacyjnych** | Urządzenia, aplikacje i platformy wykorzystująceInternet rzeczy.Przetwarzanie danych w kontekście pracyw domu i pracy wykonywanej zdalnie.Przetwarzanie danych lokalizacyjnych pracowników | Przetwarzanie wykorzystujące śledzenie lokalizacjiosoby fizycznej (wliczając sieci komunikacyjne i usługi komunikacyjne, wskazujące geograficzną pozycję telekomunikacyjnych terminali urządzeń użytkownika publicznie dostępnej usługi telekomunikacyjnej |

Przykład:

**Skutek prawny**

* wystąpienie zagrożenia nie doprowadzi do naruszenia przepisów prawa,
* wystąpienie zagrożenia doprowadzi do naruszenia przepisów prawa z wyłączeniem przepisów karnych; lub w przypadku nie podjęcia odpowiednich działań naprawczych naruszenie prawa zostanie uniknione,
* bezpośrednią konsekwencją wystąpienia zagrożenia jest naruszenie przepisów karnych.

**Skutek finansowy**

* wystąpienie zagrożenia nie powoduje strat finansowych lub powoduje znikome straty finansowe ,
* wystąpienie zagrożenia spowoduje straty finansowe ,

**Skutek wizerunkowy**

* wystąpienie zagrożenia nie ma wpływu na wizerunek organizacji lub ten wpływ jest znikomy, nie wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku,
* wystąpienie zagrożenia ma mało znaczący negatywny wpływ na wizerunek organizacji lub krótkoterminową utratę wizerunku, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku ,
* wystąpienie zagrożenia powoduje istotny lub duży negatywny wpływ na wizerunek organizacji, wiąże się z zaangażowaniem środków organizacyjno-finansowych w celu odbudowania wizerunku ,

**WAŻNE:**

Jeżeli ocena skutków dla ochrony danych wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym.

**WPŁYW NA PRYWATNOŚĆ**

Wpływ na prywatność oznacza wszystko, co może powodować zagrożenie lub negatywny wpływ na prywatność osób, np. nieuprawnione gromadzenie, dostęp, wykorzystanie, zachowanie lub ujawnianie danych osobowych, w tym kradzież tożsamości i inne formy nadużyć, kwestie bezpieczeństwa fizycznego, takie jak: prześladowanie, straty finansowe, negatywny wpływ na zatrudnienie lub naruszenie dobrego imienia.

Negatywny wpływ na prywatność osób fizycznych może również mieć istotne skutki dla funkcjonowania jednostki i jej postrzegania na rynku. Może poważnie wpłynąć na jej renomę
i spowodować utratę zaufania u dotychczasowych lub potencjalnych klientów. Zakłócenia operacyjne mogą wpłynąć na ciągłość i jakość świadczonych usług, nie wspominając o ryzyku prawnym, np.
z powodu niezgodności z RODO.

**PRZYKŁADY WPŁYWU RYZYKA NA PRYWATNOŚĆ**:

* Brak podstawy prawnej do zbierania, wykorzystywania lub ujawniania danych osobowych.
* Przetwarzanie niekompletnych lub nieaktualnych danych.
* Nieuzasadnione użycie lub ujawnienie danych, np. gdy pseudonimizowane lub anonimowe dane są wystarczające, aby osiągnąć cel.
* Zbyt szeroki zakres przetwarzanych danych.
* Przetwarzanie danych niezgodnie z pierwotnym celem.
* Przetwarzanie danych po wygaśnięciu celu ich przetwarzania.
* Ujawnienie danych nieuprawnionym podmiotom.
* Wykorzystanie danych w sposób nieetyczny lub w sposób, którego osoby, których dane dotyczą, się nie spodziewały.
* Brak stosowania odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa wynikający z analizy ryzyka.
* Brak możliwości wypełniania praw podmiotów danych w zgodzie z RODO.

Po przeprowadzeniu analizy ryzyka, nie stwierdzono, żeby którykolwiek proces przetwarzania danych osobowych odbywający się w Urzędzie Gminy w Kaźmierzu wymagał przeprowadzenia oceny skutków dla ochrony danych.

Wobec opisanych zagrożeń oraz ryzyk zostaną podjęte kroki naprawcze realizujące następujące warianty działania:

1. **Akceptacja –** zgoda na wystąpienie incydentu, jego skutki są akceptowalne, a koszt wdrożenia zabezpieczeń przewyższa wartość ewentualnych strat.
2. **Minimalizacja** - wdrożenie rozwiązań zmniejszających poziom ryzyka (techniczne lub organizacyjne środki zaradcze).
3. **Unikanie** - unikanie i eliminacja działań powodujących występowanie ryzyka.
4. **Przeniesienie**- przekazanie ryzyka innemu podmiotowi (np. ubezpieczyciel).

Analizę ryzyka przeprowadziła oraz raport sporządziła Marta Andraszak, Inspektor Ochrony Danych
w Urzędzie Gminy w Kaźmierzu, dnia: 15.10.2022 roku .