

Urząd Gminy Czernice Borowe

**SPRAWOZDANIE Z ZADANIA
ZAPEWNIĄCEGO**

P.n. „Ochrona danych osobowych”

Temat zadania	„Ochrona danych osobowych”					
Numer zadania	1720.2.2024					
Nazwa i adres jednostki audytowanej	Urząd Gminy Czernice Borowe ul. Dolna 2, 06-415 Czernice Borowe					
Imię i nazwisko Audytora Wewnętrznego	Mariusz Repelewicz					
Cele przeprowadzenia zadania	Celem zadania jest przedstawienie Wójtowi racjonalnego zapewnienia o realizacji zadań, w tym kontroli zarządczej.					
Zakres podmiotowy zadania	Urząd Gminy Czernice Borowe ul. Dolna 2, 06-415 Czernice Borowe (dalej Urząd Gminy)					
Zakres przedmiotowy zadania	Zakres przedmiotowy zadania obejmował wprowadzone procedury w zakresie ochrony danych osobowych. Ryzyko: 1. Działania niezgodne z przyjętymi i obowiązującymi procedurami w zakresie bezpieczeństwa informacji i ochrony danych osobowych 2. Utraty danych, w tym danych osobowych Obiekty audytu: 1. Kontrola dostępu 2. Bezpieczeństwo informacji Oczekiwane mechanizmy kontroli: Pracownicy realizują procedury zgodnie z obowiązującymi przepisami oraz przyjętymi wewnętrznymi procedurami. zgodnie z zakresem czynności i odpowiedzialności. Zakres czasowy badania 01.01.2024 r do 30.11.2024 r.					
Kryteria oceny	1. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 1557 z późn.zm.)					

2. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206 z późn. zm.) 3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781 z późn. zm.) 4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247 tj. z późn. zm. Uchylone z dniem 23 maja 2024 r.) 5. Rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz. U. z 2019 r. poz. 1041 z późn. zm.) 6. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773 z późn. zm.) 7. Zarządzenie nr 71/2024 Wójta Gminy Czernice Borowe z dnia 7 czerwca 2024 r. w sprawie ogłoszenia jednolitego tekstu Regulaminu Organizacyjnego Urzędu Gminy Czernice Borowe 8. Zarządzenie Nr 79a/2018 Wójta Gminy Czernice Borowe z dnia 31 sierpnia 2018 r. w sprawie powołania Inspektora Ochrony Danych Osobowych 9. Zarządzenie Nr 146/2022 Wójta Gminy Czernice Borowe z dnia 30.12.2022 r. w sprawie utworzenia	
--	--

Centrum Monitoringu Wizyjnego Gminy Czernice Borowe 10. Zarządzenie Nr 5/2020 Wójta Gminy Czernice Borowe z dnia 27 stycznia 2020 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Czernice Borowe	Data rozpoczęcia zadania	16 września 2024 r.
	Data sporządzenia sprawozdania	3 grudnia 2024 r.
Kierownictwo oraz osoby udzielające informacji i udostępniające dokumenty		Pani Monika Łukasiak – Sekretarz pełniła funkcję Inspektor Ochrony Danych Osobowych (dalej IODO)

A. Ustalenia audytu.

1. Ustalenia stanu faktycznego wraz ze sklasyfikowanymi wynikami ich oceny według przyjętych kryteriów

1.1. Do zadań komórki organizacyjnej (IODO) w zakresie audytu należy w szczególności:
1.1.1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie;

1.1.2. Monitorowanie przestrzegania przepisów oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

1.1.3. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z ochroną danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art.36 RODO oraz stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach

1.1.4. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art.35 RODO;

1.1.5. Współpraca z organem nadzorczym;

- 1.2. Analizie poddano następujące dokumenty:
 - 1.2.1. Zawiadomienie o wyznaczeniu nowego IOD z podpisem Wójta z dnia 31.08.2018 r.
 - 1.2.2. Zgłoszenie osób kontaktowych do CSIRT NASK Pana Sylwestra Kienig Informatyka jako osobę odpowiedzialną za cyberbezpieczeństwa oraz Panią Monikę Łukasziak Inspektora ds. organizacyjnych i kadry z dnia 20.05.2020 r.
 - 1.2.3. Pismo nr KN-PRGNG.0132.2.2024 wpłynęło z dnia 27.11.2024 r. Głównego Urzędu Geodezji i Kartografii dotyczące zgłoszenia naruszenia ochrony danych osobowych
 - 1.2.4. Pismo nr CG-R-III.042.1.1.2022.JL z dnia 05.12.2022 r. Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie dotyczącego informacji o incydencie bezpieczeństwa w infrastrukturze, polegającego na zaszyfrowaniu serwerów i braku dostępu do systemów informatycznych wdrażanych w realizowanych projektach.
 - 1.2.5. Pismo nr CG-R-II.433.35.2017.BR z dnia 07.12.2022 r. Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie dotyczące incydentu, w związku z którym obecnie nie mogą określić terminu usunięcia awarii.
 - 1.2.6. Rejestr czynności przetwarzania danych osobowych w Urzędzie Gminy Czernice Borowe zgodnie z Polityką Bezpieczeństwa Danych Osobowych oraz Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Gminy
 - 1.2.7. Przeglądnięto również: „Rejestr umów powierzenia przetwarzania danych osobowych” (nie było wpisanej umowy z audytorem wewnętrznym)
 - 1.2.8. Przeglądnięto również: „Rejestr osób upoważnionych do przetwarzania danych w Urzędzie Gminy Czernice Borowe”
 - 1.2.9. Analizie poddano również:
 - 1.2.9.1. Analizę ryzyka – Incydent GUGiK z dnia 02.12.2024 r.
 - 1.2.9.2. Analizę ryzyka – Incydent ransomware w Węzle Regionalnym UMM z dnia 03.02.2023 r.
 - 1.2.9.3. Analiza ryzyka bezpieczeństwa informacji z dnia 10.01.2022 r.
 - 1.2.9.4. Analiza ryzyka bezpieczeństwa informacji z dnia 20.02.2021 r.
- 1.3. W zakresie kontroli dostępu – celem zapewnienia dostępu autoryzowanym użytkownikom.

1.3.1. W Urzędzie Gminy obowiązuje formalny proces rejestracji użytkownika systemu informatycznego

1.3.2. Użytkownik systemu informatycznego otrzymując dostęp do odpowiednich zasobów otrzymuje pisemne potwierdzenie nadania uprawnień

1.3.3. W przypadku gdy pracownik zmienił stanowisko lub odszedł z pracy niezwłocznie odbierane są prawa dostępu i dokonywane są odpowiednie adnotacje w rejestrze użytkowników systemu

1.3.4. Użytkownicy systemu informatycznego mają przydzielany unikalny identyfikator użytkownika

1.3.5. Uzyskując dostęp do urządzeń komputerowych lub systemów informatycznych oprócz identyfikatora konieczne jest podanie osobistego hasła

1.3.6. System wymusza zmianę początkowego hasła oraz cykliczną zmianę użytkowanego hasła – tylko system główny Windows, oprogramowanie nie wymusza

1.3.7. Pracownicy przeszkoleni zostali w zakresie tworzenia i zabezpieczenia hasła osobistego

1.3.8. Część pracowników Urzędu Gminy ma zdalny dostęp (np. za pomocą Internetu) do zasobów informacyjnych, zgromadzonych w systemach komputerowych (w tym także do serwerów pocztowych). Zdalny dostęp pracowników do zasobów w Urzędzie Gminy jest zabezpieczony poprzez szyfrowanie połączenia oraz proces autoryzacji.

1.4. W zakresie bezpieczeństwa informacji – celem zapewnienie odpowiedniego poziomu bezpieczeństwa

1.4.1. Zabezpieczenie pomieszczeń serwerowych przed zalaniem

1.4.2. Utrzymanie sprzętu i dokumentów powyżej poziomu podłogi

1.4.3. Kopie zapasowe przechowywane w innej lokalizacji

1.4.4. Instalacja czujników dymu, gąsienic i systemu alarmowego

1.4.5. Przechowywanie wrażliwych dokumentów w zamkniętych szafach ognioodpornych

1.4.6. Według uzyskanych informacji, serwer pocztowy zapewnia:

1.4.6.1. Rozliczalność - odpowiedzialność podmiotu za jego akcje i decyzje

1.4.6.2. Niezaprzeczalność - zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że dany podmiot, je wywołał,

- w celu rozstrzygnięcia sporu w zakresie wystąpienia lub niewystąpienia tego zdarzenia lub tej akcji oraz zaangażowania podmiotów w to zdarzenie
- 1.4.6.3. Niezawodność - właściwość oznaczająca spójne, zamierzone zachowanie i skutki
- 1.4.7. Informacje zawarte w „likwidowanym” koncie poczty są usuwane
- 1.4.8. Użytkownik poczty elektronicznej ma uprawnienia do zmiany hasła poczty elektronicznej, jak również odpowiada za zachowanie jego bezpieczeństwa
- 1.4.9. Jednym z zabezpieczeń jest oprogramowanie antyspamowe przetwarzające listy przychodzące do systemu pocztowego w celu klasyfikacji listów na spam i nie spam
- 1.4.10. Zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji
- 1.4.11. Ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych
- 1.4.12. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
- 1.4.12.1. Dbłości o aktualizację oprogramowania,
- 1.4.12.2. Minimalizowaniu ryzyka utraty informacji w wyniku awarii,
- 1.4.12.3. Ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
- 1.4.12.4. Zapewnieniu bezpieczeństwa plików systemowych,
- 1.4.12.5. Niezwłocznym podejmowaniu działań po dostarczeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- 1.4.12.6. Kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa
- 1.4.12.7. Polityka innych haseł
- 1.4.13. Bezwzględne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących

2. Zalecenia w sprawie wyeliminowania słabości kontroli zarządczej
- 1.1. W związku z realizacją zadań w zgodzie z przyjętą Polityką Bezpieczeństwa zalecenia nie zostały sformułowane.

1.2. Należy pamiętać aby po wprowadzeniu „zaktualizowanych procedur”:

1.2.1. Stosować przyjęte regulacje.

1.2.2. Dokonywać ich najlepiej corocznego przeglądu

1.2.3. Aktualizować i dostosowywać do bieżących potrzeb

1.2.4. Przeprowadzać co roku audyt bezpieczeństwa informacji

B. **Opinia audytora wewnętrznego w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem**

Audyt wewnętrzny, wykonując zadanie audytowe dokonał oceny najistotniejszych dla procesu obszarów, w ramach realizacji przedmiotu zadania. System zarządzania, obejmujący kompletną zasadę realizacji zadań z badanego zakresu, uwzględnia specyfikę jednostki, w tym wymogi prawne. Zarządzanie ryzykiem odbywa się na odpowiednich poziomach zarządzania według zasad akceptacji ryzyka, dlatego pozytywnie ocenia system kontroli zarządczej, tym samym wydaje racjonalne zapewnienie o adekwatności, skuteczności i efektywności kontroli w badanym obszarze.

Mariusz Repelwicz
Audyt wewnętrzny