ZARZĄDZENIE Nr 39/2026
Wójta Gminy Szczytniki
z dnia 7 września 2026r.

w sprawie: wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji, w tym polityki bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Gminy w Szczytnikach.

Na podstawie art. 31 i art. 33 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2026 r., poz. 662 ze zm.), art. 24 ust. 2 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. U. UE. L. z 2016 r., Nr 119, str. 1) oraz art. 8 ust. 3 i art. 10 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20), **zarządzam, co następuje:**

§1. 1. Na użytek niniejszego zarządzenia:

1) **„RODO”** oznacza 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1);
2) **„UoKSC”** oznacza ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
3) **„Urząd”** oznacza Urząd Gminy w Szczytnikach;
4) **„Administrator Danych Osobowych”** oznacza Wójta Gminy Szczytniki z siedzibą 62-865 Szczytniki 139;
5) **„Zarządzenie ODO/KSC”** oznacza niniejsze zarządzenie Wójta Gminy Szczytniki;
6) Zastosowano definicje pojęć zgodnie z definicjami w art. 4 RODO;
7) **„Kierownicy komórek organizacyjnych Urzędu”** oznaczają odpowiednio kierowników referatów oraz samodzielne stanowiska pracy.
8) **„System Informatyczny Urzędu Gminy w Szczytnikach”** oznacza system informatyczny funkcjonujący w Urzędzie, na który składają się: systemy operacyjne, oprogramowanie, sprzęt komputerowy oraz teleinformatyczny (w tym sieciowy), wszelkie nośniki cyfrowe, systemy poczty elektronicznej, strony internetowe (w tym Biuletyn Informacji Publicznej), przetwarzane dane oraz procedury i polityki bezpieczeństwa dotyczące ich funkcjonowania.

§2. 1. Wszyscy pracownicy Urzędu zobligowani są do stosowania zasad bezpieczeństwa informacji i ochrony danych osobowych zgodnie z obowiązującym prawem Unii Europejskiej, prawem krajowym oraz przepisami wewnętrznymi określonymi w zarządzeniach Wójta Gminy Szczytniki.

2. Zgodnie z art. 29 oraz art. 32 ust. 4 RODO każdy pracownik Urzędu musi posiadać upoważnienie do przetwarzania danych osobowych. Natomiast zgodnie z UoKSC Urząd zapewnia dopuszczenie do informacji wyłącznie osób posiadających stosowne uprawnienia do systemów informacyjnych (w tym systemów operacyjnych, usług sieciowych i aplikacji) oraz zapewnienie środków uniemożliwiających nieautoryzowany dostęp do tych systemów;

3. Wzór upoważnienia, o którym mowa w ust. 2 stanowi **załącznik nr 1** do Zarządzenia ODO/KSC/KSC.

4. Kierownicy komórek organizacyjnych Urzędu odpowiadają za terminowe przygotowanie oraz przedłożenie do podpisu projektów upoważnień do przetwarzania danych osobowych dla podległych pracowników.

5. Sekretarz Gminy odpowiada za terminowe przygotowanie oraz przedłożenie do podpisu projektów upoważnień do przetwarzania danych osobowych dla Kierowników komórek organizacyjnych Urzędu.

6. Osoby, które zostały upoważnione do przetwarzania danych osobowych są obowiązane zachować je w tajemnicy, a także sposoby ich zabezpieczania, w trakcie oraz po ustaniu zatrudnienia.

7. Urząd jest zobowiązany do stosowania zasad przyznania minimalnych uprawnień niezbędnych dla realizacji zadań.

8. Urząd zapewnia bezzwłoczne cofanie przyznanych uprawnień w przypadku stwierdzenia braku podstawy dostępu do informacji na stałe lub zawieszanie uprawnień w przypadku **niewykonywania obowiązków co najmniej przez jeden miesiąc**.

9. Urząd zapewnia modyfikację zakresu przyznanych uprawnień, jeżeli jest to zasadne z uwagi na zmianę charakteru wykonywanych zadań i zakresu dostępu do informacji.

10. Kierownicy komórek organizacyjnych Urzędu określają, w indywidualnych zakresach czynności pracowników, zakres odpowiedzialności za ochronę danych osobowych znajdujących się w zbiorze danych, przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem danych.

§3. 1. Administrator powołuje Inspektora ochrony danych osobowych zarządzeniem w sprawie wyznaczenia Inspektora ochrony danych, który jest odpowiedzialny za nadzór nad stosowaniem środków organizacyjnych i technicznych, zapewniających ochronę przetwarzanych danych, w szczególności przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, kradzieżą, uszkodzeniem lub zniszczeniem. Status i obowiązki Inspektora określa załącznik nr 2 do Zarządzenia ODO/KSC.

2. Inspektor Ochrony Danych powinien:
   1) posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,
   2) posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO, ustawie i aktach prawa wewnętrznego,
   3) wykonywać zadania niezależnie i bez konfliktu interesów,
   4) mieć wiedzę w zakresie europejskiego i krajowego prawa ochrony danych oraz praktyk ochrony danych, a także szczegółową wiedzę na temat RODO,
   5) posiadać wiedzę na temat systemów informatycznych służących do przetwarzania, a także potrzeb i sposobów zabezpieczania danych osobowych przetwarzanych i nie może być karany za przestępstwo popełnione z winy umyślnej.

3. Administrator danych może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w niniejszym Zarządzeniu ODO.

4. W przypadku powołania IOD Administrator jest zobowiązany dokonać stosownego zgłoszenia zgodnie z wymogami prawa powszechnie obowiązującego. Jego wykreślenie z Rejestru następuje po powiadomieniu Prezesa Urzędu Ochrony Danych Osobowych o jego odwołaniu przez Administratora albo w przypadku jego śmierci.

5. Dane Inspektora ochrony danych publikowane są na stronie Biuletynu Informacji Publicznej oraz stronie internetowej Gminy.

6. Za publikację aktualnych danych, w tym danych teleadresowych Inspektora ochrony danych odpowiada Kierownik Referatu Administracyjno-Organizacyjnego Urzędu.

7. Kierownicy komórek organizacyjnych Urzędu odpowiadają za terminowe aktualizowanie dokumentacji ochrony danych osobowych, w zakresie merytorycznym funkcjonowania komórki.

8. Kierownicy komórek organizacyjnych Urzędu mogą wyznaczyć do realizacji zadań wynikających z ust. ochrony danych osobowych i bezpieczeństwa informacji oraz bezpośredniej współpracy z Inspektorem ochrony danych pracownika zarządzanej przez siebie komórki organizacyjnej, nie jest jednak możliwe delegowanie odpowiedzialności, za wyjątkiem przypadków wskazanych przez Administratora.

§4. 1. Administrator może powołać Administratora Systemów Informatycznych osobnym zarządzeniem.

2. ASI odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio kierownikowi jednostki organizacyjnej, który reprezentuje Administratora.

4. W przypadku niepowołania ASI bezpieczeństwo przetwarzania danych osobowych w systemie informatycznym spoczywa na Administratorze.

4. Szczegółowy zakres obowiązków ASI określa **załącznik nr 5** do Zarządzenia ODO/KSC.

§5. 1. Znajdujące się z zasobach Urzędu Gminy w Szczytnikach wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej przetwarzane zarówno w formie tradycyjnej (papierowej), jak i elektronicznej stanowią dane osobowe i podlegają ochronie stosownie do przepisów RODO oraz przepisów krajowych regulujących ochronę danych osobowych.

2. Dane osobowe przetwarzane w Urzędzie winny być przetwarzane wyłącznie w przypadkach o których mowa w art. 6, art. 9 oraz art. 10 RODO.

3. Przetwarzanie danych osobowych w Urzędzie dopuszcza się tylko w obszarze przetwarzania danych osobowych, określonym w **załączniku nr 13** do Zarządzenia ODO/KSC.

4. Za aktualność określenia obszaru przetwarzania danych osobowych odpowiadają Kierownicy komórek organizacyjnych.

5. Wprowadza się do stosowania Instrukcję Zarządzania Systemem Informatycznym Urzędu Gminy w Szczytnikach, stanowiącą **załącznik nr 11** do Zarządzenia ODO/KSC.

§6. 1. Zgodnie z art. 32 ust.1 lit. a) oraz art. 25 RODO wdraża się w Urzędzie Gminy w Szczytnikach System Zarządzania Ryzykiem Ochrony Danych Osobowych, który pozwala (przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia) wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Sposób wdrożenia Systemu Zarządzania Ryzykiem Ochrony Danych Osobowych w tym metodykę przeprowadzania analizy ryzyka reguluje odrębne zarządzenie Wójta Gminy w Szczytnikach.

3. Ocena skutków dla ochrony danych oraz gdy przetwarzanie powoduje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą odbywa się zgodnie z art. 35 i 36 RODO z zastosowaniem procedur opisanych w zarządzeniu Wójta Gminy Szczytniki, o którym mowa w ust. 2.

4. Analiza oceny ryzyka jest podstawą podejmowania działań zapobiegawczych i ich priorytetyzacji, a jej posiadanie pozwala szerzej spojrzeć na własną organizację. Aby dobrze podejść do analizy, należy pamiętać o kilku bardzo ważnych aspektach:

1) należy zidentyfikować zagrożenia, z którymi można spotkać się podczas przetwarzania danych,
2) należy zidentyfikować aktywa, które mogą być zagrożone,
3) należy określić prawdopodobieństwo wystąpienia ryzyka, a także ewentualny wpływ zdarzenia na aktywa,
4) na tej podstawie należy podjąć odpowiednie kroki zaradcze,
5) konieczne są okresowe przeglądy i zmiany w analizie, w miarę pojawiania się nowych zagrożeń.

5. Jako podstawowe środki techniczne i organizacyjne zapewniające ochronę danych osobowych mają być zastosowane środki określone w **załączniku nr 10** do Zarządzenia ODO/KSC.

§7. 1. Mając na uwadze, że przetwarzane dane mają być adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane, pracownicy Urzędu są zobligowani do przetwarzania tylko tych danych, które są niezbędne do wykonywania powierzonych zadań i są przetwarzane na podstawie art.6 ust.1 lit. b), c), d) lub e) RODO z zastrzeżeniem ust. 2.

2. W przypadku jeśli przetwarzanie danych osobowych odbywa się na podstawie art. 6 ust. 1 lit. a) RODO (czyli na podstawie zgody osoby, której dane dotyczą) pracownicy Urzędu są zobligowani do uzyskania (przed przystąpieniem do przetwarzania) zgody osoby której dane dotyczą zgodnie z przepisami prawa w szczególności z art. 7 i 8 RODO, dopełnienia obowiązku informacyjnego zgodnie z art. 12 - 14 RODO oraz respektowania i ułatwiania osobie, której dane dotyczą wykonania praw przysługujących na mocy art. 15 – 22 oraz art. 34 RODO.

§8. 1. Udostępnianie danych osobowych odbiorcom oraz organom publicznym, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem krajowym, następuje wyłącznie na mocy przepisów prawa.

2. Przetwarzanie danych osobowych dokonywane w imieniu Administratora przez podmiot przetwarzający jest dopuszczalne wyłącznie po uprzednim pisemnym powierzeniu przetwarzania danych osobowych zgodnym z RODO.

3. Za powierzenie przetwarzania danych osobowych odpowiadają Kierownicy komórek organizacyjnych Urzędu w zakresie realizacji zadań merytorycznych w podległej im komórce. Przed powierzeniem przetwarzania danych osobowych Kierownicy komórek organizacyjnych Urzędu zobligowani są do przedłożenia projektu umowy powierzenia przetwarzania danych osobowych do konsultacji Inspektorowi ochrony danych i uwzględnienia jego wytycznych.

§9. 1. Wprowadza się Instrukcję postępowania w sytuacji naruszenia zasad ochrony danych osobowych, stanowiącą **załącznik nr 14** do Zarządzenia ODO/KSC.

2. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych odbywa się zgodnie z art. 33

oraz art. 34 RODO z zastosowaniem procedury opisanej w instrukcji postępowania w sytuacji naruszenia zasad ochrony danych osobowych, o której mowa w ust. 1.

§10. Upoważnienia do przetwarzania danych osobowych wydane przed 25 maja 2018 r., które są zgodne z RODO i przepisami krajowymi obowiązującymi na dzień 25 maja 2018 r., podpisane przez osobę do tego upoważnioną, zachowują ważność.

§ 11. Wykonanie Zarządzenia ODO/KSC powierza się wszystkim pracownikom Urzędu Gminy w Szczytnikach.

§12. Nadzór nad wykonaniem Zarządzenia ODO/KSC powierza się Sekretarzowi Gminy.

§13. Traci moc zarządzenie:

1) Zarządzenie Nr 26/2019 Wójta Gminy Szczytniki z dnia 31 lipca 2019 r. w sprawie ochrony danych osobowych w Urzędzie Gminy w Szczytnikach.

§14. Zarządzenie ODO/KSC wchodzi w życie z dniem podpisania.

Wójt
/-/ Marek Albrecht