WÓJT GMINY
CHRZYPSKO WIELKIE
ul. Główna 15
34-412 Chrzypsko Wielkie

Zarządzenie nr 47/2026

Wójta Gminy Chrzypsko Wielkie

z dnia 1 października 2026 r.

w sprawie wprowadzenia Polityki ochrony i przetwarzania danych osobowych w środowisku teleinformatycznym i poza tym środowiskiem

Na podstawie art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2026 r. poz. 662, ze zm.), art. 68 oraz art. 69 ust. 1 pkt 2 i 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2025 r. poz. 1483, ze zm.), w związku z art. 24 ust. 1 i 2, art. 25 ust. 1 i art. 32 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „RODO", zarządzam, co następuje:

§ 1. Wprowadzenie Polityki

1. Wprowadza się do stosowania w Urzędzie Gminy Chrzypsko Wielkie, zwanej dalej „Jednostką", Politykę ochrony i przetwarzania danych osobowych w środowisku teleinformatycznym i poza tym środowiskiem, zwaną dalej „Polityką", stanowiącą **załącznik nr 1** do zarządzenia.
2. Ilekroć w zarządzeniu jest mowa o:
   1) Kierowniku Jednostki – należy przez to rozumieć Wójta Gminy Chrzypsko Wielkie;
   2) IOD – należy przez to rozumieć Inspektora Ochrony Danych wyznaczonego przez administratora danych w Jednostce;
   3) ASI – należy przez to rozumieć Administratora Systemów Informatycznych;
   4) Koordynatorze – należy przez to rozumieć Koordynatora do spraw cyberbezpieczeństwa.
3. Integralną część Polityki stanowią załączniki do Polityki, obejmujące w szczególności wzory upoważnień, oświadczeń, kart dostępu, rejestrów, formularzy zgłoszeniowych oraz klauzul informacyjnych.
4. Politykę stosuje się łącznie ze Standardami Ochrony Małoletnich wprowadzonymi w Jednostce Zarządzeniem Nr 66/2024 Wójta Gminy Chrzypsko Wielkie z dnia 10 października 2024 r. W sprawach przetwarzania danych osobowych małoletnich pierwszeństwo mają rozwiązania zapewniające wyższy poziom ich ochrony.

§ 2. Zakres i charakter Polityki

1. Polityka określa jednolite zasady ochrony danych osobowych i innych informacji podlegających ochronie, niezależnie od ich postaci, miejsca przetwarzania oraz wykorzystywanej technologii – zarówno w systemach teleinformatycznych Jednostki i w systemach centralnych prowadzonych przez organy administracji publicznej, jak i w dokumentacji papierowej oraz w procesach realizowanych poza środowiskiem teleinformatycznym.
2. Polityka stanowi jednocześnie:
   1) politykę ochrony danych, o której mowa w art. 24 ust. 2 RODO, określającą odpowiednie środki techniczne i organizacyjne oraz służącą wykazaniu zgodności przetwarzania z prawem (art. 5 ust. 2 RODO);
   2) dokumentację systemu zarządzania bezpieczeństwem informacji, o którym mowa w rozporządzeniu Krajowych Ram Interoperacyjności;
   3) podstawę realizacji obowiązków Jednostki wynikających z ustawy o krajowym systemie cyberbezpieczeństwa – w zakresie, w jakim przepisy tej ustawy mają do Jednostki zastosowanie;

4) element systemu kontroli zarządczej Jednostki, o którym mowa w art. 68 ustawy o finansach publicznych, służący w szczególności zapewnieniu zgodności działalności z przepisami prawa i procedurami wewnętrznymi, ochronie zasobów oraz zarządzaniu ryzykiem.

3. Polityka uwzględnia wymagania wynikające w szczególności z:
   1) RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   2) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz rozporządzenia 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. poz. 773), zwanego dalej „rozporządzeniem Krajowych Ram Interoperacyjności";
   3) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
   4) ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych;
   5) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej - w zakresie ograniczeń jawności;
   6) ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz przepisów kancelaryjno-archiwalnych obowiązujących w Jednostce;
   7) ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych – w zakresie kontroli zarządczej oraz Centralnego Rejestru Umów, a także ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług - w zakresie Krajowego Systemu e-Faktur;
   8) ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy;
   9) przepisów ustrojowych i szczególnych właściwych dla Jednostki: ustawa z dnia 8 marca 1990 r. o samorządzie gminnym i ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych;
   10) aktów wewnętrznych Jednostki: Regulaminu Organizacyjnego Urzędu Gminy Chrzypsko Wielkie, Zarządzenia Nr 11/2021 Wójta Gminy Chrzypsko Wielkie z dnia 12 lutego 2021r. w sprawie wskazania systemu wykonywania czynności kancelaryjnych.

§ 3. Zakres podmiotowy

1. Polityka obowiązuje wszystkie osoby przetwarzające dane osobowe w Jednostce, bez względu na podstawę prawną wykonywania czynności: pracowników, osoby wykonujące pracę lub usługi na podstawie umów cywilnoprawnych, stażystów, praktykantów i wolontariuszy, a także – w zakresie im właściwym – przedstawicieli podmiotów zewnętrznych wykonujących czynności na terenie Jednostki lub w jej systemach teleinformatycznych.
2. Polityka obowiązuje we wszystkich lokalizacjach, w których Jednostka przetwarza informacje, w tym na stanowiskach pracy zdalnej.

§ 4. Osoby pełniące funkcje w systemie ochrony danych

1. Inspektorem Ochrony Danych w Jednostce jest Joanna Mrowicka - Kancelaria Ochrony Danych Osobowych Smart & Standards z siedzibą w Warszawie, zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych. IOD pełni jednocześnie funkcję Punktu Kontaktowego Jednostki we wszystkich sprawach dotyczących przetwarzania danych osobowych i wykonywania praw osób, których dane dotyczą.
2. Funkcję Administratora Systemów Informatycznych pełni Pan Dominik Kozber.
3. Funkcję Koordynatora do spraw cyberbezpieczeństwa pełni Pani Aneta Skrzypczak-Kurzawa.
4. Zmiana osoby lub podmiotu pełniącego funkcję, o której mowa w ust. 1–3, następuje w drodze pisemnego wyznaczenia przez Kierownika Jednostki. Aktualny wykaz osób pełniących te funkcje prowadzi IOD.
5. Kierownik Jednostki zapewnia opublikowanie danych kontaktowych IOD w Biuletynie Informacji Publicznej i na stronie internetowej Jednostki, ich udostępnienie w miejscu obsługi interesantów oraz – jeżeli nie nastąpiło to wcześniej – zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD (art. 37 ust. 7 RODO).

§ 5. Zapoznanie się z Polityką

1. Osoby, o których mowa w § 3 ust. 1, są obowiązane zapoznać się z Polityką i stosować jej postanowienia.
2. Zapoznanie się z Polityką potwierdza się pisemnym oświadczeniem, którego wzór stanowi **załącznik nr 2** do zarządzenia, składanym w terminie 14 dni od dnia wejścia w życie zarządzenia.
3. Osoba przyjmowana do pracy albo dopuszczana do wykonywania czynności na rzecz Jednostki po dniu wejścia w życie zarządzenia składa oświadczenie, o którym mowa w ust. 2, przed dopuszczeniem do przetwarzania danych osobowych. Oświadczenie może zostać złożone łącznie z oświadczeniem o zachowaniu poufności, którego wzór określa Polityka.
4. Oświadczenia pracowników włącza się do akt osobowych, a oświadczenia pozostałych osób przechowuje się w dokumentacji prowadzonej przez IOD.
5. Nieprzestrzeganie postanowień Polityki przez pracownika stanowi naruszenie obowiązków pracowniczych i może skutkować odpowiedzialnością porządkową, dyscyplinarną lub inną przewidzianą w przepisach prawa pracy i przepisach szczególnych, a w przypadku osób niebędących pracownikami - odpowiedzialnością wynikającą z łączącej je z Jednostką umowy; nie wyłącza to odpowiedzialności cywilnej i karnej przewidzianej w przepisach odrębnych.

§ 6. Upoważnienia i uprawnienia w okresie przejściowym

1. Upoważnienia do przetwarzania danych osobowych nadane przed dniem wejścia w życie zarządzenia zachowują ważność do dnia nadania upoważnień według wzoru określonego w Polityce, nie dłużej jednak niż przez 60 dni od dnia wejścia w życie zarządzenia.
2. W terminie, o którym mowa w ust. 1:
   1) nadaje się upoważnienia według wzoru określonego w Polityce wszystkim osobom przetwarzającym dane osobowe;
   2) sporządza się karty dostępu do systemów teleinformatycznych dla wszystkich użytkowników;
   3) przeprowadza się pierwszy przegląd uprawnień we wszystkich systemach, z którego sporządza się notatkę.

§ 7. Harmonogram wdrożenia

1. Ustala się harmonogram czynności wdrożeniowych; terminy liczy się od dnia wejścia w życie zarządzenia:

Lp.	Zadanie	Termin	Odpowiedzialny
1	Przekazanie Polityki osobom, o których mowa w § 3 ust. 1, i odebranie oświadczeń (§ 5 ust. 2)	14 dni	kadry / sekretariat
2	Udokumentowana ocena statusu Jednostki na gruncie ustawy o krajowym systemie cyberbezpieczeństwa	30 dni – *z zachowaniem terminów ustawowych*	Koordynator
3	Szkolenie wstępne z zakresu ochrony danych i cyberbezpieczeństwa	60 dni	IOD
4	Aktualizacja rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania	60 dni	IOD
5	Inwentaryzacja zasobów informacyjnych i teleinformatycznych oraz obszarów przetwarzania	60 dni	ASI
6	Nadanie upoważnień, sporządzenie kart dostępu i przegląd uprawnień (§ 6)	60 dni	kadry, ASI, IOD
7	Weryfikacja treści klauzul informacyjnych i sposobu ich udostępniania	60 dni	IOD
8	Przegląd umów powierzenia przetwarzania i umów z dostawcami usług informatycznych	90 dni	IOD, komórki merytoryczne

Lp.	Zadanie	Termin	Odpowiedzialny
9	Przeprowadzenie i udokumentowanie analizy ryzyka	90 dni	ASI, właściciele procesów, IOD
10	Test odtworzenia danych z kopii zapasowej	90 dni	ASI
11	Przegląd Standardów Ochrony Małoletnich pod kątem spójności z Polityką	30 dni	osoba wyznaczona w SOM, IOD

2. IOD przedstawia Kierownikowi Jednostki informację o stanie realizacji harmonogramu w terminie 100 dni od dnia wejścia w życie zarządzenia.

§ 8. Przegląd i zmiana Polityki

1. Polityka podlega przeglądowi nie rzadziej niż raz w roku, a ponadto po istotnej zmianie przepisów lub struktury organizacyjnej, po wdrożeniu lub wycofaniu systemu teleinformatycznego, po naruszeniu ochrony danych o poważnych skutkach oraz po audycie bezpieczeństwa informacji.
2. Przegląd przeprowadza IOD we współpracy z ASI i Koordynatorem; wynik przeglądu wraz z propozycjami zmian przedstawia się Kierownikowi Jednostki.
3. Zmiany Polityki, w tym jej załączników, wprowadza Kierownik Jednostki w drodze zarządzenia. Każda zmiana otrzymuje nowy numer wersji i jest odnotowywana w historii zmian Polityki.
4. Wyniki przeglądu uwzględnia się w samoocenie systemu kontroli zarządczej, a w Jednostce obowiązanej do złożenia oświadczenia o stanie kontroli zarządczej – także przy jego sporządzaniu.

§ 9. Przepisy uchylające

Traci moc zarządzenie Nr 58/2024 Wójta Gminy Chrzypsko Wielkie z dnia 2 września 2024r. w sprawie: wprowadzenia „Polityki bezpieczeństwa i ochrony danych osobowych w Urzędzie Gminy Chrzypsko Wielkie".

§ 10. Wykonanie zarządzenia

Wykonanie zarządzenia powierza się Sekretarzowi Gminy oraz - w zakresie zadań określonych w § 4–8 - IOD, ASI i Koordynatorowi.

§ 11. Wejście w życie

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt
mgr inż. Edmund Ziółek

UZASADNIENIE

1. **Potrzeba wydania zarządzenia.** Dotychczasowe regulacje wewnętrzne Jednostki w zakresie ochrony danych osobowych i bezpieczeństwa informacji nie uwzględniają zmian stanu prawnego, w szczególności rozporządzenia Krajowych Ram Interoperacyjności z 2024 r., nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa wdrażającej dyrektywę (UE) 2022/2555 (NIS2), obowiązków związanych z Centralnym Rejestrem Umów i Krajowym Systemem e-Faktur, a także upowszechnienia pracy zdalnej i narzędzi sztucznej inteligencji. Rozproszenie regulacji w kilku dokumentach utrudniało ich stosowanie i wykazanie zgodności przetwarzania z prawem.
2. **Zakres regulacji.** Polityka zastępuje dotychczasowe dokumenty jednolitą regulacją obejmującą przetwarzanie danych niezależnie od postaci i miejsca - w systemach teleinformatycznych Jednostki, w systemach centralnych, w dokumentacji papierowej i poza środowiskiem teleinformatycznym - co odpowiada zasadzie rozliczalności (art. 5 ust. 2 RODO) i obowiązkowi wdrożenia polityki ochrony danych (art. 24 ust. 2 RODO).
3. **Związek z kontrolą zarządczą.** Zgodnie z art. 68 ust. 2 ustawy o finansach publicznych celem kontroli zarządczej jest w szczególności zapewnienie zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi, ochrony zasobów oraz efektywnego zarządzania ryzykiem. Polityka realizuje w szczególności następujące standardy kontroli zarządczej dla sektora finansów publicznych, ogłoszone w Komunikacie Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. Min. Fin. Nr 15, poz. 84):

Grupa standardów	Standard	Realizacja w Polityce
A. Środowisko wewnętrzne	3. Struktura organizacyjna 4. Delegowanie uprawnień	podział ról i odpowiedzialności, upoważnienia do przetwarzania danych
B. Cele i zarządzanie ryzykiem	7. Identyfikacja ryzyka 8. Analiza ryzyka 9. Reakcja na ryzyko	analiza ryzyka, ocena skutków dla ochrony danych (DPIA), dobór zabezpieczeń
C. Mechanizmy kontroli	10. Dokumentowanie systemu kontroli zarządczej	Polityka wraz z załącznikami i rejestrami
	11. Nadzór	nadzór IOD, przeglądy uprawnień, kontrola podmiotów przetwarzających
	12. Ciągłość działalności	kopie zapasowe, testy odtwarzania, postępowanie w sytuacjach awaryjnych
	13. Ochrona zasobów	zabezpieczenia fizyczne i techniczne, zasada wiedzy koniecznej
	15. Mechanizmy kontroli dotyczące systemów informatycznych	karty dostępu, uwierzytelnianie, rejestrowanie zdarzeń, zarządzanie zmianą
D. Informacja i komunikacja	16. Bieżąca informacja 17. Komunikacja wewnętrzna 18. Komunikacja zewnętrzna	obowiązek informacyjny, klauzule informacyjne, Punkt Kontaktowy, e-Doręczenia
E. Monitorowanie i ocena	19. Monitorowanie systemu kontroli zarządczej 20. Samoocena 21. Uzyskanie zapewnienia o stanie kontroli zarządczej	przeglądy Polityki, testy bezpieczeństwa, audyt bezpieczeństwa informacji

4. **Skutki finansowe.** Wydanie zarządzenia nie powoduje skutków finansowych. Koszty dostosowania zabezpieczeń technicznych, szkoleń oraz audytu bezpieczeństwa informacji pokrywa się ze środków przewidzianych w planie finansowym Jednostki.
5. **Opracowanie projektu.** Projekt Polityki opracował Inspektor Ochrony Danych.

Załącznik nr 2 do Zarządzenia Nr 47/2026 Wójta Gminy Chrzypsko Wielkie z dnia 1 października 2026r.

OŚWIADCZENIE
o zapoznaniu się z Polityką ochrony i przetwarzania danych osobowych

Chrzypsko Wielkie, dnia ..... r.

Ja, niżej podpisana / podpisany

.....,

zatrudniona / zatrudniony na stanowisku .....

/ wykonująca / wykonujący czynności na rzecz Urzędu Gminy Chrzypsko Wielkie na podstawie

umowy o pracę, oświadczam, że:

1. zapoznałam się / zapoznałem się z Zarządzeniem Nr 47/2026 Wójta Gminy Chrzypsko Wielkie z dnia 1 października 2026r. w sprawie wprowadzenia Polityki ochrony i przetwarzania danych osobowych w środowisku teleinformatycznym i poza tym środowiskiem oraz z Polityką stanowiącą załącznik nr 1 do tego zarządzenia, wraz z załącznikami do Polityki;
2. treść tych dokumentów jest dla mnie zrozumiała, a w razie wątpliwości mogę je konsultować z Inspektorem Ochrony Danych;
3. zobowiązuję się przestrzegać postanowień Polityki, w tym przetwarzać dane osobowe wyłącznie w zakresie udzielonego mi upoważnienia i na polecenie administratora;
4. zobowiązuję się zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia – bezterminowo, również po ustaniu zatrudnienia lub innego stosunku prawnego łączącego mnie z Jednostką;
5. zobowiązuję się niezwłocznie, w terminie określonym w Polityce, zgłaszać Inspektorowi Ochrony Danych i Administratorowi Systemów Informatycznych każde podejrzenie naruszenia ochrony danych osobowych lub incydentu bezpieczeństwa;
7. przyjmuję do wiadomości, że nieprzestrzeganie postanowień Polityki może skutkować odpowiedzialnością porządkową, dyscyplinarną lub wynikającą z łączącej mnie z Jednostką umowy, a także odpowiedzialnością cywilną i karną przewidzianą w przepisach odrębnych.

.....
czytelny podpis składającego oświadczenie

Adnotacja:
oświadczenie złożono dnia ..... r.;
włączono do [akt osobowych / dokumentacji IOD].

Podpis osoby przyjmującej .....

Wójt
mgr inż. Edmund Ziółek

ROZDZIELNIK

Lp.	Adresat	Sposób przekazania
1	Pracownicy Jednostki	[za pokwitowaniem / przez system EZD / pocztą służbową]
2	Inspektor Ochrony Danych	pocztą elektroniczną
3	Administrator Systemów Informatycznych	pocztą elektroniczną
4	Koordynator do spraw cyberbezpieczeństwa	pocztą elektroniczną
5	Kierownicy komórek organizacyjnych	za pokwitowaniem
6	Osoby wykonujące czynności na podstawie umów cywilnoprawnych, stażyści, praktykanci, wolontariusze	za pokwitowaniem – przed dopuszczeniem do przetwarzania
7	Zbiór zarządzeń (a/a)	oryginał

Wykaz załączników do zarządzenia:

1) załącznik nr 1 - Polityka ochrony i przetwarzania danych osobowych w środowisku teleinformatycznym i poza tym środowiskiem, wraz z załącznikami nr 1 -..... do Polityki;
2) załącznik nr 2 - wzór oświadczenia o zapoznaniu się z Polityką ochrony i przetwarzania danych osobowych.