Urząd Gminy
Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

POLITYKA OCHRONY I PRZETWARZANIA DANYCH

w środowisku informatycznym i poza tym środowiskiem

e-mail: urzad@chrzypsko.pl **e-Doręczenia:** AE:PL-64773-21728-SBJJD-24

DEKLARACJA STOSOWANIA POLITYKI

Kierownictwo Jednostki uznaje ochronę danych osobowych, bezpieczeństwo informacji oraz cyberbezpieczeństwo za integralny element prawidłowego i zgodnego z prawem wykonywania zadań publicznych.

Niniejsza Polityka określa jednolite zasady ochrony danych i informacji, niezależnie od ich postaci, miejsca przetwarzania oraz wykorzystywanej technologii, obejmując zarówno środowisko teleinformatyczne, jak i dokumentację oraz procesy realizowane poza tym środowiskiem.

Polityka została ustanowiona z uwzględnieniem w szczególności wymagań wynikających z Konstytucji Rzeczypospolitej Polskiej, RODO, ustawy o ochronie danych osobowych, ustawy o krajowym systemie cyberbezpieczeństwa oraz przepisów dotyczących Krajowych Ram Interoperacyjności.

Kierownictwo uznaje ponadto, że Jednostka – jako urząd, przy pomocy którego Wójt Gminy wykonuje zadania gminy (art. 33 ust. 1 ustawy o samorządzie gminnym) – realizuje zadania własne gminy oraz zadania zlecone z zakresu administracji rządowej, w tym sprawy ewidencji ludności i dowodów osobistych, rejestracji stanu cywilnego, podatków i opłat lokalnych, gospodarki odpadami komunalnymi, gospodarki nieruchomościami, planowania przestrzennego, zarządzania kryzysowego i wyborów, w związku z czym przetwarza w dużej skali dane osobowe mieszkańców, w tym dane objęte tajemnicą skarbową i innymi tajemnicami ustawowo chronionymi oraz dane pochodzące z rejestrów państwowych, wymagające podwyższonego poziomu ochrony.

Przyjęte rozwiązania opierają się na podejściu opartym na ryzyku i służą zapewnieniu poufności, integralności, dostępności, autentyczności oraz rozliczalności przetwarzanych informacji.

Przy ich projektowaniu i doskonaleniu uwzględniane są także wymagania i dobre praktyki wynikające z norm ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 oraz ISO/IEC 27701.

Polityka stanowi również element systemu kontroli zarządczej Jednostki i wspiera realizację celów w zakresie zgodności działalności z prawem, ochrony zasobów, zarządzania ryzykiem, ciągłości działania oraz właściwego przepływu informacji.

Kierownictwo zobowiązuje się do zapewnienia odpowiednich warunków organizacyjnych i technicznych dla stosowania niniejszej Polityki oraz do jej okresowego przeglądu i doskonalenia w odpowiedzi na zmiany prawa, technologii, organizacji i zidentyfikowanych zagrożeń.

Wersja dokumentu	1.0
Data obowiązywania od	1 października 2026 r.
Właściciel dokumentu	Wójt Gminy Chrzypsko Wielkie
Opracowanie	Inspektor Ochrony Danych
Zatwierdził	Wójt Gminy Chrzypsko Wielkie
Zastępuje	dotychczasowe regulacje wewnętrzne Jednostki w zakresie ochrony danych osobowych i bezpieczeństwa informacji
Klauzula	Do użytku wewnętrznego

Wójt Gminy Chrzypsko Wielkie
(zatwierdzenie)

METRYKA I HISTORIA ZMIAN DOKUMENTU

Polityka podlega przeglądowi nie rzadziej niż raz w roku oraz każdorazowo po istotnej zmianie przepisów, struktury organizacyjnej, wykorzystywanych systemów teleinformatycznych albo po stwierdzeniu naruszenia. Każda zmiana wymaga nadania nowego numeru wersji i odnotowania w poniższej tabeli. Wersję zmienioną w zakresie merytorycznym oznacza się kolejnym numerem głównym (2.0, 3.0), zmianę redakcyjną lub porządkową - numerem po kropce (1.1, 1.2).

Wersja	Data	Zakres zmian	Opracował	Zatwierdził
1.0	01.10.2026 r.	Wydanie pierwsze. Dokument zastępuje dotychczasowe regulacje wewnętrzne Urzędu w zakresie ochrony danych osobowych i bezpieczeństwa informacji. Uwzględnia rozporządzenie KRI z 2024 r., nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, obsługę systemów centralnych (CRU, KSeF), zasady powierzenia przetwarzania oraz zakaz korzystania z zewnętrznych narzędzi sztucznej inteligencji.	IOD	Wójt

Potwierdzenie przeglądu okresowego

Data przeglądu	Wynik przeglądu (bez zmian / wersja …)	Podpis IOD	Podpis Wójta

SPIS TREŚCI

CZĘŚĆ I	POSTANOWIENIA OGÓLNE	§ 1–5
CZĘŚĆ II	ORGANIZACJA OCHRONY DANYCH I ODPOWIEDZIALNOŚĆ	§ 6–11
CZĘŚĆ III	SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI	§ 12–18
CZĘŚĆ IV	UPOWAŻNIENIA I KONTROLA DOSTĘPU	§ 19–27
CZĘŚĆ V	PRZETWARZANIE W SYSTEMACH CENTRALNYCH (CRU, KSeF)	§ 28–31
CZĘŚĆ VI	BEZPIECZEŃSTWO POZA ŚRODOWISKIEM TELEINFORMATYCZNYM	§ 32–35
CZĘŚĆ VII	BEZPIECZEŃSTWO ŚRODOWISKA TELEINFORMATYCZNEGO	§ 36–43
CZĘŚĆ VIII	SZTUCZNA INTELIGENCJA	§ 44–45
CZĘŚĆ IX	PODMIOTY PRZETWARZAJĄCE I PODWYKONAWCY	§ 46–50
CZĘŚĆ X	INCYDENTY I NARUSZENIA	§ 51–55
CZĘŚĆ XI	PRAWA OSÓB I OBOWIĄZEK INFORMACYJNY	§ 56–59
CZĘŚĆ XII	POSTANOWIENIA KOŃCOWE	§ 60–62

Wykaz załączników

Nr	Tytuł załącznika
1	Upoważnienie do przetwarzania danych osobowych
2	Odwołanie upoważnienia do przetwarzania danych osobowych
3	Oświadczenie osoby upoważnionej o zachowaniu poufności
4	Karta dostępu do systemów teleinformatycznych jednostki
5	Karta dostępu do systemów centralnych (CRU, KSeF i inne)
6	Rejestr upoważnień i kart dostępu
7	Klauzula informacyjna nr 1 - realizacja zadań statutowych
8	Klauzula informacyjna nr 2 - rekrutacja
9	Klauzula informacyjna nr 3 - pracownicy i współpracownicy
10	Klauzula informacyjna nr 4 - umowy, Centralny Rejestr Umów i KSeF
11	Klauzula informacyjna nr 5 - dochodzenie należności i zobowiązań
12	Zgoda pracownika na przetwarzanie dodatkowych danych osobowych, w tym wizerunku, oraz zezwolenie na rozpowszechnianie wizerunku
13	Informacja o stosowaniu monitoringu wizyjnego oraz potwierdzenie jej otrzymania przez pracownika
14	Zgłoszenie naruszenia ochrony danych osobowych / incydentu bezpieczeństwa
15	Rejestr naruszeń ochrony danych i incydentów bezpieczeństwa
16	Wykaz systemów teleinformatycznych i inwentaryzacja zasobów
17	Wykaz umów powierzenia przetwarzania oraz podmiotów przetwarzających i ich podwykonawców

CZĘŚĆ I
POSTANOWIENIA OGÓLNE

§ 1. Cel Polityki

1. Polityka określa zasady ochrony i przetwarzania danych osobowych oraz innych informacji podlegających ochronie w Urzędzie Gminy Chrzypsko Wielkie, zwanym dalej „Jednostką", zarówno **w środowisku teleinformatycznym, jak i poza nim**. Postanowienia Polityki stosuje się również do przetwarzania danych w związku z obsługą Rady Gminy i jej komisji oraz przez Urząd Stanu Cywilnego działający w Jednostce.
2. Celem Polityki jest zapewnienie poufności, integralności, dostępności, autentyczności, rozliczalności i niezaprzeczalności przetwarzanych informacji, wykazanie zgodności przetwarzania z przepisami prawa (zasada rozliczalności) oraz zapewnienie odporności Jednostki na incydenty bezpieczeństwa i cyberzagrożenia.
3. Polityka stanowi jednocześnie **dokumentację systemu zarządzania bezpieczeństwem informacji (SZBI)** w rozumieniu przepisów o Krajowych Ramach Interoperacyjności oraz podstawę realizacji obowiązków wynikających z przepisów o krajowym systemie cyberbezpieczeństwa.

§ 2. Przedmiot i zakres stosowania

1. Polityka obowiązuje wszystkie osoby przetwarzające dane w Jednostce: pracowników, osoby wykonujące pracę na podstawie umów cywilnoprawnych, stażystów i praktykantów, wolontariuszy, a także - w zakresie im właściwym - przedstawicieli podmiotów zewnętrznych wykonujących czynności na terenie Jednostki lub w jej systemach.
2. Polityka obejmuje wszystkie procesy przetwarzania danych, niezależnie od formy i nośnika: dokumentację papierową, systemy teleinformatyczne Jednostki, systemy centralne prowadzone przez organy administracji rządowej, nośniki elektroniczne, urządzenia mobilne oraz środki komunikacji elektronicznej.
3. Polityka obejmuje wszystkie lokalizacje, w których Jednostka przetwarza informacje, w tym siedzibę Urzędu, Urząd Stanu Cywilnego, archiwum zakładowe, salę obrad Rady Gminy i punkty obsługi mieszkańców, a także stanowiska pracy zdalnej – w zakresie i na warunkach określonych w § 41.
4. Postanowień Polityki nie stosuje się do przetwarzania dokonywanego przez osoby fizyczne wyłącznie w celach osobistych lub domowych.

§ 3. Podstawy prawne

Polityka opiera się w szczególności na:

1. rozporządzeniu 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 (RODO), w szczególności art. 5, 24, 25, 28, 29, 30, 32–36;
2. ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych;
3. **rozporządzeniu 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)** - dalej „rozporządzenie KRI";
4. **ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**, w brzmieniu nadanym nowelizacją wdrażającą dyrektywę (UE) 2022/2555 (NIS2) - dalej „ustawa o KSC";
5. ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
6. ustawie z dnia 8 marca 1990 r. o samorządzie gminnym – w szczególności art. 7 i 8 (zadania własne i zlecone gminy), art. 11b (jawność działania organów gminy), art. 20 ust. 1b (transmisja i utrwalanie obrad rady gminy), art. 24h–24i (oświadczenia majątkowe) oraz art. 33 (urząd gminy);
7. ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, w tym w zakresie skarg i wniosków, oraz ustawie z dnia 11 lipca 2014 r. o petycjach;
8. ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, w szczególności w zakresie tajemnicy skarbowej, oraz ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych;
9. ustawie z dnia 24 września 2010 r. o ewidencji ludności, ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych oraz ustawie z dnia 28 listopada 2014 r. – Prawo o aktach stanu cywilnego;
10. ustawie z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach;
11. ustawie z dnia 5 stycznia 2011 r. – Kodeks wyborczy oraz ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
12. ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych;

13. art. 34a i 34b ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych - w zakresie Centralnego Rejestru Umów Jednostek Sektora Finansów Publicznych;
14. art. 106nb–106nh ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług oraz przepisach wykonawczych - w zakresie Krajowego Systemu e-Faktur;
15. ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej - w zakresie ograniczeń jawności;
16. ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz przepisach kancelaryjno-archiwalnych obowiązujących w Jednostce;
17. ustawie z dnia 26 czerwca 1974 r. - Kodeks pracy oraz ustawie z dnia 21 listopada 2008 r. o pracownikach samorządowych.

Publikatory aktów prawnych aktualizuje się przy każdym przeglądzie Polityki.

§ 4. Definicje

Ilekroć w Polityce jest mowa o:

1. **Administratorze** – rozumie się przez to Wójta Gminy Chrzypsko Wielkie, który jako organ wykonawczy gminy i kierownik Jednostki decyduje o celach i środkach przetwarzania danych osobowych w sprawach załatwianych przez Jednostkę, a w zakresie, w jakim przepisy szczególne wskazują innego administratora – odpowiednio Kierownika Urzędu Stanu Cywilnego albo Radę Gminy Chrzypsko Wielkie; w zakresie danych pracowników Jednostki administratorem jest Jednostka jako pracodawca reprezentowany przez Wójta;
2. **IOD** - Inspektorze Ochrony Danych wyznaczonym przez Administratora i zgłoszonym Prezesowi Urzędu Ochrony Danych Osobowych, stanowiącym jednocześnie **Punkt Kontaktowy** Jednostki w sprawach ochrony danych osobowych;
3. **Punkcie Kontaktowym** - wskazanym w Polityce i w klauzulach informacyjnych adresie kontaktu we wszystkich sprawach dotyczących przetwarzania danych osobowych i korzystania z praw związanych z przetwarzaniem, obsługiwanym przez IOD;
4. **ASI** - Administratorze Systemów Informatycznych, odpowiadającym za sprawność, konserwację i zabezpieczenia techniczne systemów teleinformatycznych Jednostki;
5. **Koordynatorze ds. cyberbezpieczeństwa** - osobie wyznaczonej przez Administratora do wykonywania zadań wynikających z ustawy o KSC oraz do kontaktu z właściwym zespołem CSIRT;
6. **Użytkowniku** - osobie posiadającej upoważnienie do przetwarzania danych osobowych oraz nadany dostęp do systemu teleinformatycznego;
7. **Upoważnieniu** - pisemnym oświadczeniu Administratora wskazującym imiennie osobę oraz zakres, w jakim może przetwarzać dane osobowe;
8. **Karcie dostępu** - dokumencie określającym, do których systemów teleinformatycznych i z jakimi rolami użytkownik uzyskał dostęp, stanowiącym mechanizm kontrolny nadawania, zmiany i odbierania uprawnień technicznych;
9. **Systemie Jednostki** - systemie teleinformatycznym eksploatowanym przez Jednostkę lub na jej rzecz, w szczególności systemie finansowo-księgowym, kadrowo-płacowym, systemie elektronicznego zarządzania dokumentacją, poczcie elektronicznej;
10. **Systemie centralnym** - systemie teleinformatycznym prowadzonym przez organ administracji publicznej, do którego Jednostka lub jej pracownicy przekazują dane, w szczególności: Centralnym Rejestrze Umów Jednostek Sektora Finansów Publicznych (CRU JSFP), Krajowym Systemie e-Faktur (KSeF), ePUAP i systemie e-Doręczeń, Systemie Informacji Oświatowej, systemach Zakładu Ubezpieczeń Społecznych i Ministerstwa Finansów;
11. **SZBI** - systemie zarządzania bezpieczeństwem informacji, o którym mowa w rozporządzeniu KRI;
12. **Incydencie bezpieczeństwa** - zdarzeniu, które ma lub może mieć niekorzystny wpływ na poufność, integralność, dostępność, autentyczność lub rozliczalność informacji albo na działanie systemu teleinformatycznego;
13. **Naruszeniu ochrony danych** - naruszeniu bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych (art. 4 pkt 12 RODO);
14. **Podmiocie przetwarzającym** - podmiocie, któremu Administrator powierzył przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO;
15. **Podwykonawcy (dalszym podmiocie przetwarzającym)** - podmiocie, któremu podmiot przetwarzający powierzył wykonanie części czynności przetwarzania;

16. **Narzędziu sztucznej inteligencji** - oprogramowaniu lub usłudze wykorzystującej modele uczenia maszynowego do generowania, przetwarzania lub analizy treści, w tym udostępnianej zdalnie usłudze przetwarzającej dane wprowadzane przez użytkownika;
17. **Wyłączeniu jawności** - nieudostępnieniu w systemie centralnym określonej informacji, wraz z podaniem podstawy prawnej i oznaczeniem osoby albo organu dokonującego wyłączenia.

§ 5. Zasady przetwarzania i atrybuty bezpieczeństwa informacji

1. Dane osobowe przetwarza się zgodnie z zasadami określonymi w art. 5 RODO: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności oraz rozliczalności.
2. Bezpieczeństwo informacji w Jednostce oznacza zapewnienie łącznie następujących atrybutów:
   a) **poufności** - informacja nie jest udostępniana osobom nieuprawnionym;
   b) **integralności** - informacja nie została zmieniona w sposób nieuprawniony;
   c) **dostępności** - informacja jest osiągalna dla osób uprawnionych wtedy, gdy jest potrzebna;
   d) **autentyczności** - tożsamość osoby, systemu lub źródła informacji jest taka, jak deklarowana;
   e) **rozliczalności** - działania w systemie można jednoznacznie przypisać konkretnej osobie;
   f) **niezaprzeczalności** - nie można skutecznie zaprzeczyć dokonaniu czynności;
   g) **niezawodności** - system zachowuje się w sposób przewidywalny i zgodny z przeznaczeniem.
3. Cyberbezpieczeństwo danych osobowych oznacza odporność systemów teleinformatycznych, w których dane te są przetwarzane, na działania naruszające powyższe atrybuty.
4. Zabezpieczenia dobiera się na podstawie **udokumentowanej analizy ryzyka**, z uwzględnieniem stanu wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania, a także ryzyka naruszenia praw lub wolności osób fizycznych (art. 24 i 32 RODO).
5. Obowiązuje **zasada wiedzy koniecznej** - dostęp do danych i systemów przyznaje się wyłącznie w zakresie niezbędnym do wykonywania obowiązków służbowych.
6. Jednostka przetwarza **dane osobowe szczególnych kategorii** (art. 9 RODO) oraz dane dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO) wyłącznie w zakresie wynikającym z przepisów prawa, w szczególności: dane o stanie zdrowia i niepełnosprawności – w sprawach ulg, zwolnień, świadczeń i spraw kadrowych; dane zawarte w aktach stanu cywilnego i dokumentach składanych w sprawach rejestracji stanu cywilnego; dane o karalności – w zakresie wymaganym przepisami, w tym przy naborze na stanowiska urzędnicze i w postępowaniach o wydanie zezwoleń. Podstawę przetwarzania stanowi w szczególności art. 9 ust. 2 lit. b, g lub h RODO oraz art. 10 RODO w związku z przepisami szczególnymi.
7. Dane, o których mowa w ust. 6, a także **dane objęte tajemnicą skarbową** i **dane pozyskiwane z rejestrów państwowych** (w szczególności z rejestru PESEL, rejestru mieszkańców, Rejestru Dowodów Osobistych, rejestru stanu cywilnego i Centralnego Rejestru Wyborców) podlegają **podwyższonemu poziomowi ochrony**: dostęp do nich nadaje się wyłącznie osobom prowadzącym sprawę i ich przełożonym, dokumentację przechowuje się w wydzielonych, zamykanych zbiorach, a przekazywanie takich danych środkami komunikacji elektronicznej wymaga szyfrowania. Dostęp do rejestrów państwowych odbywa się wyłącznie przez imiennie upoważnione osoby, z użyciem przypisanych im środków uwierzytelniania.
8. Osoby przetwarzające dane w Jednostce obowiązane są zachować **tajemnicę zawodową** i tajemnice ustawowo chronione, w szczególności **tajemnicę skarbową** (art. 293 i nast. ustawy – Ordynacja podatkowa). Osoby mające dostęp do informacji objętych tajemnicą skarbową składają pisemne przyrzeczenie, o którym mowa w art. 296 ustawy – Ordynacja podatkowa. Obowiązek zachowania tajemnicy jest niezależny od obowiązku zachowania w tajemnicy danych osobowych i trwa również po ustaniu zatrudnienia.
9. Informacji o mieszkańcach, podatnikach, stronach postępowań i innych osobach, których dane dotyczą, **nie udziela się telefonicznie ani osobom trzecim**, w tym członkom rodziny, bez ustalenia podstawy prawnej udostępnienia i potwierdzenia tożsamości wnioskodawcy. Dane z rejestru PESEL i rejestru mieszkańców udostępnia się wyłącznie w trybie przepisów ustawy o ewidencji ludności, a informacje objęte tajemnicą skarbową wyłącznie w przypadkach określonych w Ordynacji podatkowej.
10. Obrady Rady Gminy są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk, a nagrania udostępnia się w Biuletynie Informacji Publicznej, na stronie internetowej gminy i w inny sposób zwyczajowo przyjęty (art. 20 ust. 1b ustawy o samorządzie gminnym); imienne wykazy głosowań radnych podaje się do publicznej wiadomości. Osoby zabierające głos podczas sesji informuje się o transmisji, a przed publikacją materiałów ogranicza się ujawnianie danych osób trzecich w zakresie, w jakim nie jest to niezbędne do realizacji zasady jawności.

11. Oświadczenia majątkowe podlegające publikacji udostępnia się w Biuletynie Informacji Publicznej z wyłączeniem informacji o adresie zamieszkania składającego oświadczenie oraz o miejscu położenia nieruchomości, zgodnie z art. 24i ustawy o samorządzie gminnym.

CZĘŚĆ II
ORGANIZACJA OCHRONY DANYCH I ODPOWIEDZIALNOŚĆ

§ 6. Administrator

1. Administratorem danych przetwarzanych w Jednostce jest **Wójt Gminy Chrzypsko Wielkie**, wykonujący zadania gminy przy pomocy Urzędu Gminy (Jednostki) z wyjątkiem danych wskazanych w ust. 2 i 3 niniejszego paragrafu.
2. W zakresie rejestracji stanu cywilnego przetwarzanych w formie tradycyjnej dokumentacji papierowej, akt zbiorowych oraz prowadzonych przez siebie postępowań administracyjnych administratorem danych jest Kierownik Urzędu Stanu Cywilnego, natomiast Minister Cyfryzacji jest administratorem danych w zakresie utrzymania, rozwoju oraz technicznego bezpieczeństwa centralnego Rejestru Stanu Cywilnego. Minister Spraw Wewnętrznych i Administracji odpowiada za kształtowanie jednolitej polityki w zakresie rejestracji stanu cywilnego i jest administratorem danych w odniesieniu do bazy elektronicznej Rejestru Stanu Cywilnego.
3. W zakresie danych przetwarzanych w związku z działalnością Rady Gminy – Rada Gminy Chrzypsko Wielkie; w zakresie danych pracowników administratorem jest Jednostka jako pracodawca.
4. Postanowienia Polityki stosuje się do przetwarzania danych przez te podmioty odpowiednio. Administrator ponosi odpowiedzialność za wdrożenie i utrzymanie odpowiednich środków technicznych i organizacyjnych oraz za wykazanie zgodności przetwarzania z prawem.
5. Do zadań Administratora należy w szczególności: zatwierdzanie Polityki i jej zmian, wyznaczanie IOD, ASI i Koordynatora ds. cyberbezpieczeństwa, nadawanie i odwoływanie upoważnień, akceptacja poziomu ryzyka, zatwierdzanie umów powierzenia, podejmowanie decyzji o zgłoszeniu naruszenia organowi nadzorczemu oraz decyzji o wyłączeniu jawności informacji w systemach centralnych.
6. Powierzenie czynności wykonawczych pracownikom nie zwalnia Administratora z odpowiedzialności za prawidłowość ich wykonania.

§ 7. Inspektor Ochrony Danych - Punkt Kontaktowy

1. Administrator wyznacza IOD, publikuje jego dane kontaktowe i zawiadamia o nim Prezesa Urzędu Ochrony Danych Osobowych.
2. IOD stanowi jednocześnie **Punkt Kontaktowy** Jednostki we wszystkich sprawach dotyczących przetwarzania danych osobowych i korzystania z praw związanych z przetwarzaniem - zarówno dla osób, których dane dotyczą, jak i dla pracowników, podmiotów przetwarzających oraz organów.
3. IOD wykonuje zadania określone w art. 39 RODO, a ponadto: opiniuje projekty procedur i umów w zakresie ochrony danych, prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności, prowadzi ewidencję upoważnień, uczestniczy w analizie ryzyka i ocenie skutków dla ochrony danych, prowadzi rejestr naruszeń, opiniuje wyłączenia jawności w zakresie prywatności osób fizycznych oraz realizuje działania szkoleniowe.
4. IOD podlega bezpośrednio Administratorowi, nie otrzymuje instrukcji co do sposobu wykonywania zadań i nie może być z tego powodu odwołany ani ukarany.
5. Pracownicy mają prawo i obowiązek konsultowania z IOD wątpliwości dotyczących przetwarzania danych. Do czasu rozstrzygnięcia wątpliwości wstrzymuje się czynności, których wątpliwość dotyczy.

Dane Punktu Kontaktowego

Funkcję Inspektora Ochrony Danych - Punktu Kontaktowego pełni **Pani Joanna Mrowicka**, Kancelaria Ochrony Danych Osobowych Smart & Standards, tel. +48 602 241239, e-mail: kontakt@smart-standards.com. Kontakt jest możliwy także pisemnie na adres Jednostki. Dane te podaje się w klauzulach informacyjnych (Załączniki nr 7–11), publikuje w Biuletynie Informacji Publicznej i wywiesza w miejscu obsługi mieszkańców.

§ 8. Administrator Systemów Informatycznych

1. ASI odpowiada za utrzymanie, konfigurację i zabezpieczenia techniczne systemów Jednostki, prowadzenie inwentaryzacji sprzętu i oprogramowania, zarządzanie kontami i uprawnieniami technicznymi, wykonywanie i testowanie kopii zapasowych, aktualizowanie oprogramowania, monitorowanie systemów oraz obsługę techniczną incydentów.

2. ASI może być pracownikiem Jednostki albo podmiotem zewnętrznym. W drugim przypadku zakres jego czynności określa umowa, do której obowiązkowo zawiera się umowę powierzenia przetwarzania danych oraz postanowienia o dostępie serwisowym, o których mowa w § 49.
3. ASI nie nadaje sobie samodzielnie uprawnień wykraczających poza zakres niezbędny do administrowania systemami; czynności na kontach uprzywilejowanych podlegają rejestrowaniu.

§ 9. Koordynator do spraw cyberbezpieczeństwa

1. Administrator wyznacza Koordynatora ds. cyberbezpieczeństwa oraz osobę go zastępującą. Funkcję tę może pełnić ASI, o ile nie prowadzi to do konfliktu ról kontrolnych.
2. Do zadań Koordynatora należy: prowadzenie i aktualizowanie oceny statusu Jednostki na gruncie ustawy o KSC, nadzór nad wdrożeniem i utrzymaniem SZBI, obsługa zgłoszeń incydentów do właściwego zespołu CSIRT, utrzymywanie kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa oraz organizacja szkoleń z zakresu cyberbezpieczeństwa.
3. Koordynator prowadzi **rejestr incydentów bezpieczeństwa** oraz przedstawia Administratorowi roczne sprawozdanie ze stanu bezpieczeństwa systemów.

§ 10. Obowiązki użytkowników

Każda osoba przetwarzająca dane w Jednostce jest obowiązana:

1. przetwarzać dane wyłącznie w zakresie i celu wynikającym z udzielonego upoważnienia oraz na polecenie Administratora;
2. zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia - bezterminowo, także po ustaniu zatrudnienia;
3. korzystać wyłącznie z przypisanych sobie indywidualnych środków uwierzytelniania i nie udostępniać ich innym osobom;
4. stosować zasadę czystego biurka i czystego ekranu;
5. niezwłocznie zgłaszać IOD i ASI każde podejrzenie naruszenia ochrony danych lub incydentu bezpieczeństwa - najpóźniej w ciągu **4 godzin** od jego stwierdzenia;
6. uczestniczyć w szkoleniach z zakresu ochrony danych i cyberbezpieczeństwa;
7. przestrzegać zakazu korzystania z narzędzi sztucznej inteligencji, o którym mowa w § 44.

§ 11. Podział odpowiedzialności

Obszar	Decyduje	Wykonuje	Nadzoruje / opiniuje
Upoważnienia do przetwarzania danych	Administrator	Kadry	IOD
Karta dostępu - systemy Jednostki	Administrator	ASI	IOD
Karta dostępu - systemy centralne	Administrator	Administrator konta w systemie	IOD
Analiza ryzyka i ocena skutków (DPIA)	Administrator	ASI, właściciele procesów	IOD
Kopie zapasowe i testy odtwarzania	Administrator	ASI	Koordynator
Zgłoszenie naruszenia do PUODO	Administrator	IOD	IOD
Zgłoszenie incydentu do CSIRT	Administrator	Koordynator	ASI
Wyłączenie jawności w CRU	Administrator	Osoba prowadząca sprawę	IOD, radca prawny
Umowy powierzenia przetwarzania	Administrator	Komórka merytoryczna	IOD
Dopuszczenie narzędzia AI	Administrator	-	IOD, ASI
Audyt bezpieczeństwa informacji	Administrator	Audytor	Koordynator

CZĘŚĆ III
SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

§ 12. Ustanowienie SZBI

1. W Jednostce ustanawia się, wdraża, eksploatuje, monitoruje, przegląda, utrzymuje i doskonali system zarządzania bezpieczeństwem informacji, obejmujący wszystkie systemy i procesy przetwarzania informacji, niezależnie od nośnika.
2. SZBI opiera się na cyklu: planowanie - wdrożenie - sprawdzenie - doskonalenie, i jest udokumentowany niniejszą Polityką wraz z załącznikami oraz rejestrami prowadzonymi na jej podstawie.
3. Za funkcjonowanie SZBI odpowiada Administrator; koordynację powierza się Koordynatorowi ds. cyberbezpieczeństwa we współpracy z IOD i ASI.
4. Przy budowie SZBI stosuje się dobre praktyki wynikające z norm PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 27002 oraz - w zakresie ciągłości działania - PN-EN ISO 22301, w zakresie odpowiednim do wielkości Jednostki i wyników analizy ryzyka.

§ 13. Inwentaryzacja zasobów

1. Jednostka prowadzi i aktualizuje **wykaz zasobów informacyjnych i teleinformatycznych** obejmujący: sprzęt komputerowy i sieciowy, oprogramowanie wraz z licencjami, systemy Jednostki, systemy centralne, z których korzysta, nośniki danych, konta w systemach oraz zbiory dokumentacji papierowej.
2. Dla każdego systemu wskazuje się: właściciela merytorycznego, administratora technicznego, kategorie przetwarzanych danych, podstawę prawną przetwarzania, lokalizację danych, sposób uwierzytelniania oraz podmiot zewnętrzny obsługujący system.
3. Wykaz prowadzi ASI według wzoru stanowiącego **Załącznik nr 16**; aktualizacja następuje niezwłocznie po każdej zmianie, a przegląd całościowy - co najmniej raz w roku.
4. Do eksploatacji dopuszcza się wyłącznie sprzęt i oprogramowanie ujęte w wykazie. Instalowanie oprogramowania przez użytkowników jest zabronione.

§ 14. Analiza ryzyka i ocena skutków dla ochrony danych

1. Analizę ryzyka przeprowadza się **co najmniej raz w roku**, a ponadto przed wdrożeniem nowego systemu lub istotną zmianą istniejącego, po incydencie o poważnych skutkach oraz po istotnej zmianie przepisów.
2. Analiza obejmuje identyfikację zasobów, zagrożeń i podatności, oszacowanie prawdopodobieństwa i skutku, wyznaczenie poziomu ryzyka oraz wybór postępowania z ryzykiem: ograniczenie, przeniesienie, unikanie albo akceptacja.
3. Ryzyka zaakceptowane wymagają pisemnej decyzji Administratora wraz z uzasadnieniem.
4. Ocenę skutków dla ochrony danych (DPIA) przeprowadza się, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w szczególności przy przetwarzaniu na dużą skalę danych szczególnych kategorii, systematycznym monitorowaniu, wdrażaniu nowych technologii lub przekazywaniu danych do systemów centralnych o charakterze jawnym.
5. Wyniki analizy ryzyka i DPIA dokumentuje się; stanowią one podstawę doboru zabezpieczeń.

§ 15. Monitorowanie i testowanie systemów

1. Systemy teleinformatyczne Jednostki podlegają **stałemu monitorowaniu** obejmującemu co najmniej: rejestrowanie zdarzeń (logi) dotyczących uwierzytelniania, dostępu do danych i czynności administracyjnych, monitorowanie dostępności usług oraz kontrolę aktualności oprogramowania i sygnatur ochrony antywirusowej.
2. Logi przechowuje się przez okres nie krótszy niż **12 miesięcy**, w sposób uniemożliwiający ich modyfikację przez użytkowników. Przeglądu logów dokonuje ASI co najmniej raz na kwartał; wynik odnotowuje.
3. Jednostka prowadzi **testy bezpieczeństwa**, w tym co najmniej:
   a) test odtworzenia danych z kopii zapasowej - nie rzadziej niż **raz na pół roku**;
   b) sprawdzenie podatności systemów i aktualności oprogramowania - nie rzadziej niż **raz na kwartał**;
   c) test świadomości pracowników (kontrolowana wiadomość phishingowa lub sprawdzian wiedzy) - nie rzadziej niż **raz w roku**;
   d) test procedury postępowania w razie incydentu (ćwiczenie na scenariuszu) - nie rzadziej niż **raz w roku**;
   e) przegląd uprawnień użytkowników we wszystkich systemach - nie rzadziej niż **raz na pół roku**.

1. Z każdego testu sporządza się notatkę zawierającą: zakres, datę, wynik, stwierdzone nieprawidłowości i zalecane działania naprawcze wraz z terminem ich wykonania.
2. Testy o charakterze inwazyjnym (testy penetracyjne) przeprowadza się wyłącznie na podstawie pisemnej zgody Administratora i umowy określającej zakres oraz zasady zachowania poufności.

§ 16. Audyt bezpieczeństwa informacji

1. Jednostka poddaje się **okresowemu audytowi bezpieczeństwa informacji, nie rzadziej niż raz w roku**, obejmującemu zgodność z rozporządzeniem KRI, RODO oraz niniejszą Polityką.
2. Audyt przeprowadza osoba posiadająca odpowiednie kwalifikacje, niezależna od obszaru audytowanego. Audytorem nie może być osoba pełniąca funkcję ASI w zakresie własnych czynności.
3. Sprawozdanie z audytu przedstawia się Administratorowi. Stwierdzone nieprawidłowości są przedmiotem planu działań naprawczych z przypisaniem osób odpowiedzialnych i terminów.
4. Wykonanie zaleceń poaudytowych podlega weryfikacji przy kolejnym audycie.

§ 17. Szkolenia i budowanie świadomości

1. Każda osoba przed dopuszczeniem do przetwarzania danych odbywa szkolenie wstępne z zakresu ochrony danych osobowych i cyberbezpieczeństwa, potwierdzone pisemnie.
2. Szkolenia okresowe organizuje się **nie rzadziej niż raz w roku**; obejmują one w szczególności: rozpoznawanie phishingu i socjotechniki, zasady pracy w systemach centralnych, postępowanie w razie incydentu, bezpieczeństwo pracy zdalnej oraz ograniczenia dotyczące narzędzi sztucznej inteligencji.
3. Odrębne szkolenie kierownictwa obejmuje odpowiedzialność za cyberbezpieczeństwo i zarządzanie ryzykiem.
4. IOD prowadzi ewidencję odbytych szkoleń.

§ 18. Harmonogram wdrożenia obowiązków z zakresu cyberbezpieczeństwa

Jednostka realizuje obowiązki wynikające z ustawy o KSC według poniższego harmonogramu; Koordynator ds. cyberbezpieczeństwa monitoruje jego wykonanie i informuje Administratora o zagrożeniu terminu.

Zadanie	Termin	Odpowiedzialny
Udokumentowana ocena statusu Jednostki na gruncie ustawy o KSC (podmiot kluczowy / ważny / pozostały) wraz z mapą usług i systemów	niezwłocznie po wejściu Polityki w życie	Koordynator
Wpis do Wykazu podmiotów krajowego systemu cyberbezpieczeństwa - jeżeli ocena wykaże taki obowiązek	do 3 października 2026 r.	Administrator
Wdrożenie i udokumentowanie SZBI, procedur zarządzania incydentami oraz zabezpieczeń wynikających z analizy ryzyka	do 3 kwietnia 2027 r.	Koordynator, ASI
Podłączenie do systemu teleinformatycznego S46 - jeżeli dotyczy	do 3 kwietnia 2027 r.	ASI
Pierwszy przegląd/audyt bezpieczeństwa w trybie ustawy o KSC	do 3 kwietnia 2028 r.	Administrator

Terminy wskazane w tabeli odpowiadają terminom wynikającym z przepisów przejściowych nowelizacji ustawy o KSC. Przy każdym przeglądzie Polityki weryfikuje się ich aktualność.

CZĘŚĆ IV
UPOWAŻNIENIA I KONTROLA DOSTĘPU

§ 19. Upoważnienia do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby posiadające **imienne upoważnienie** Administratora, nadane przed rozpoczęciem przetwarzania.
2. Upoważnienie określa: imię i nazwisko oraz stanowisko osoby, zakres przetwarzanych kategorii danych, cele przetwarzania, okres obowiązywania oraz - jeżeli dotyczy - systemy, w których osoba przetwarza dane.
3. Upoważnienie jest **imienne i nieprzenoszalne**; wygasa z chwilą odwołania, ustania zatrudnienia albo zmiany zakresu obowiązków wykluczającej przetwarzanie danych.
4. Wraz z upoważnieniem osoba składa **oświadczenie o zachowaniu poufności** (Załącznik nr 3). Obowiązek zachowania tajemnicy jest bezterminowy.
5. Osoby, które przebywają w obszarach przetwarzania, lecz nie przetwarzają danych (np. obsługa techniczna, sprzątanie), składają wyłącznie oświadczenie o zachowaniu poufności i odbywają skrócone szkolenie.
6. Wzory upoważnienia i jego odwołania stanowią **Załączniki nr 1 i 2**.

7. Jeżeli upoważnienie obejmuje **dane szczególnych kategorii** albo dane dotyczące wyroków skazujących i czynów zabronionych, wskazuje się to w jego treści wprost. Zakres takiego upoważnienia podlega przeglądowi przy każdej zmianie stanowiska oraz nie rzadziej niż raz w roku.

§ 20. Zgoda pracownika na przetwarzanie dodatkowych danych osobowych

1. Dane osobowe pracowników niezbędne do nawiązania i realizacji stosunku pracy, wykonania obowiązków prawnych ciążących na pracodawcy, realizacji uprawnień wynikających ze stosunku pracy oraz wykonywania innych obowiązków określonych przepisami prawa przetwarzane są na właściwych podstawach prawnych i nie wymagają uzyskiwania zgody pracownika.
2. Zgoda pracownika może stanowić podstawę przetwarzania wyłącznie takich danych osobowych lub dla takich celów, dla których Administrator nie dysponuje inną właściwą podstawą prawną, a udzielenie zgody ma charakter rzeczywiście dobrowolny.
3. Brak zgody albo jej późniejsze wycofanie nie może powodować niekorzystnego traktowania pracownika ani jakichkolwiek negatywnych konsekwencji w zakresie zatrudnienia.
4. W szczególności zgoda może dotyczyć przetwarzania i rozpowszechniania wizerunku pracownika dla dobrowolnych celów informacyjnych, promocyjnych, edukacyjnych lub związanych z dokumentowaniem działalności Administratora, jeżeli wykorzystanie wizerunku nie jest niezbędne do wykonywania obowiązków pracowniczych ani nie znajduje oparcia w innej podstawie prawnej.
5. Poszczególne cele wykorzystania wizerunku powinny być wskazane odrębnie, w sposób pozwalający pracownikowi na dokonanie rzeczywistego wyboru. Nie stosuje się jednej, ogólnej zgody obejmującej bliżej nieokreślone sposoby i cele przyszłego wykorzystywania wizerunku.
6. Zgoda może zostać wycofana w każdym czasie, w sposób równie łatwy jak jej udzielenie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.
7. Wzór oświadczenia stanowi **Załącznik nr 12 do Polityki – Zgoda pracownika na przetwarzanie dodatkowych danych osobowych, w tym wizerunku, oraz zezwolenie na rozpowszechnianie wizerunku.**

§ 21. Monitoring wizyjny pracowników

1. Monitoring wizyjny stosowany na terenie zakładu pracy lub na terenie wokół zakładu pracy nie jest prowadzony na podstawie zgody pracownika.
2. Monitoring może zostać wprowadzony wyłącznie w przypadkach i dla celów przewidzianych przepisami prawa pracy, w szczególności jeżeli jest niezbędny do:
    a. zapewnienia bezpieczeństwa pracowników;
    b. ochrony mienia;
    c. kontroli produkcji;
    d. zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.
3. Monitoring wizyjny obejmuje wyłącznie rejestrację obrazu. W ramach monitoringu wizyjnego nie dokonuje się rejestracji dźwięku.
4. Cele, zakres oraz sposób zastosowania monitoringu określa się w układzie zbiorowym pracy, regulaminie pracy albo jeżeli Administrator nie jest objęty układem zbiorowym lub nie jest obowiązany do ustalenia regulaminu pracy w obwieszczeniu pracodawcy.
5. Pracownicy są informowani o wprowadzeniu monitoringu w sposób przyjęty u pracodawcy, nie później niż na dwa tygodnie przed jego uruchomieniem.
6. Przed dopuszczeniem pracownika do pracy Administrator przekazuje mu w postaci pisemnej informacje dotyczące celu, zakresu i sposobu stosowania monitoringu.
7. Pomieszczenia i obszary objęte monitoringiem oznacza się w sposób widoczny i czytelny, nie później niż jeden dzień przed uruchomieniem monitoringu. Oznaczenie obszaru monitorowanego nie zastępuje obowiązku przekazania informacji wymaganych przepisami RODO.
8. Nagrania obrazu mogą być wykorzystywane wyłącznie do celów, dla których zostały zebrane. Co do zasady przechowuje się je przez okres nieprzekraczający trzech miesięcy od dnia nagrania. Jeżeli nagranie stanowi lub może stanowić dowód w postępowaniu prowadzonym na podstawie prawa, okres jego przechowywania może zostać przedłużony do czasu prawomocnego zakończenia tego postępowania. Po upływie właściwego okresu nagrania podlegają usunięciu, chyba że przepisy odrębne stanowią inaczej.
9. Podpis pracownika pod informacją dotyczącą monitoringu służy wyłącznie udokumentowaniu wykonania obowiązku informacyjnego i **nie stanowi zgody na objęcie pracownika monitoringiem ani podstawy prawnej przetwarzania jego danych osobowych.**

10. Wzór informacji stanowi **Załącznik nr 13 do Polityki pn. Informacja o stosowaniu monitoringu wizyjnego oraz potwierdzenie jej otrzymania przez pracownika**.

§ 22. Karta dostępu do systemów teleinformatycznych Jednostki

1. Upoważnienie do przetwarzania danych **nie jest równoznaczne z nadaniem dostępu do systemu**. Dostęp techniczny nadaje się odrębnie, na podstawie **Karty dostępu** (Załącznik nr 4), zatwierdzonej przez Administratora i wykonanej przez ASI.
2. Karta dostępu wskazuje: system, rolę lub poziom uprawnień, zakres danych, sposób uwierzytelniania, datę nadania oraz - w razie potrzeby - termin wygaśnięcia dostępu.
3. Nadanie, zmiana i odebranie dostępu następuje wyłącznie na podstawie Karty. Ustne polecenia nie stanowią podstawy do zmiany uprawnień.
4. ASI potwierdza na Karcie faktyczne wykonanie czynności w systemie wraz z datą; Karta bez takiego potwierdzenia nie dokumentuje nadania dostępu.
5. Uprawnienia nadaje się zgodnie z zasadą wiedzy koniecznej i zasadą rozdzielenia obowiązków - w szczególności rozdziela się rolę wprowadzającą dane od roli je zatwierdzającej, jeżeli pozwala na to obsada kadrowa.

§ 23. Dostęp do systemów centralnych

1. Dostęp do systemów centralnych, w szczególności do **Centralnego Rejestru Umów JSFP** oraz **Krajowego Systemu e-Faktur**, wymaga łącznie: upoważnienia do przetwarzania danych osobowych, **Karty dostępu do systemów centralnych** (Załącznik nr 5) oraz dokonania czynności nadania uprawnień w danym systemie przez uprawnioną osobę.
2. Karta dostępu do systemów centralnych określa odrębnie dla każdego systemu: rolę użytkownika, zakres przedmiotowy czynności, sposób uwierzytelniania (podpis zaufany, kwalifikowany podpis elektroniczny, certyfikat, token) oraz datę i numer referencyjny czynności nadania uprawnień w systemie.
3. W odniesieniu do CRU JSFP wyróżnia się role: **administrator konta jednostki (administrator JSFP)**, **wprowadzający** oraz **publikujący**.
4. W odniesieniu do KSeF wyróżnia się uprawnienia: administratora, wystawiania faktur, dostępu do faktur, nadawania i odbierania uprawnień, samofakturowania, wystawiania faktur VAT RR, przeglądania uprawnień i historii sesji oraz zarządzania certyfikatami.
5. Rolę nadającą uprawnienia w systemie centralnym powinny pełnić **co najmniej dwie osoby** - podstawowa i zastępująca - dla zapewnienia ciągłości działania.
6. Zabrania się korzystania z konta w systemie centralnym przez osobę inną niż ta, której konto nadano, a także udostępniania środków uwierzytelniania.

§ 24. Konta uprzywilejowane i dostęp serwisowy

1. Konta o podwyższonych uprawnieniach (administracyjne, techniczne, serwisowe) prowadzi się w odrębnym wykazie i przypisuje **imiennie**. Konta wspólne są zabronione, z wyjątkiem kont technicznych systemów, których nie da się przypisać osobie - te zabezpiecza się hasłem zdeponowanym u Administratora.
2. Codzienna praca administratora odbywa się na koncie zwykłym; konto uprzywilejowane wykorzystuje się wyłącznie do czynności administracyjnych.
3. Dostęp serwisowy dostawcy zewnętrznego jest **domyślnie wyłączony** i włączany na czas wykonania określonej czynności, na wniosek zgłoszony ASI, z odnotowaniem: kto, kiedy, w jakim zakresie i w jakim celu uzyskał dostęp.
4. Zdalny dostęp serwisowy odbywa się wyłącznie kanałem szyfrowanym, po uwierzytelnieniu, z możliwością rejestrowania sesji.
5. Konta uprzywilejowane podlegają przeglądowi **co najmniej raz na kwartał**.

§ 25. Uwierzytelnianie i zarządzanie hasłami

1. Każdy użytkownik posiada indywidualny identyfikator. Identyfikatora nie przypisuje się ponownie innej osobie.
2. Hasło do systemu musi liczyć **co najmniej 12 znaków** i zawierać wielkie i małe litery, cyfrę oraz znak specjalny; nie może zawierać danych osobowych użytkownika ani nazwy systemu.
3. Hasła zmienia się niezwłocznie w razie podejrzenia ujawnienia, a w systemach nieobjętych uwierzytelnianiem wieloskładnikowym - nie rzadziej niż **co 90 dni**.
4. Tam, gdzie system to umożliwia, stosuje się **uwierzytelnianie wieloskładnikowe (MFA)** - obowiązkowo dla kont uprzywilejowanych, dostępu zdalnego, poczty elektronicznej i systemów centralnych.

5. Zabronione jest zapisywanie haseł w miejscach dostępnych dla osób trzecich, przekazywanie ich innym osobom oraz stosowanie tego samego hasła w systemach służbowych i prywatnych. Dopuszcza się korzystanie z menedżera haseł zatwierdzonego przez ASI.
6. Hasło początkowe nadane przez ASI podlega zmianie przy pierwszym logowaniu.

§ 26. Przegląd i odbieranie uprawnień

1. Uprawnienia we wszystkich systemach podlegają przeglądowi **nie rzadziej niż raz na pół roku**. Przegląd obejmuje weryfikację, czy zakres uprawnień odpowiada aktualnemu zakresowi obowiązków.
2. W razie zmiany stanowiska lub zakresu obowiązków uprawnienia dostosowuje się **niezwłocznie**, nie później niż w dniu zmiany.
3. W razie ustania zatrudnienia lub rozwiązania umowy uprawnienia odbiera się i konta blokuje **najpóźniej w ostatnim dniu obowiązywania stosunku prawnego**, a upoważnienie odwołuje się na piśmie.
4. W razie długotrwałej nieobecności przekraczającej 30 dni dostęp zawiesza się.
5. Odebranie uprawnień obejmuje również systemy centralne oraz zwrot środków uwierzytelniania, nośników i sprzętu; fakt ten odnotowuje się na Karcie dostępu.

§ 27. Rejestry prowadzone w zakresie dostępu

1. Jednostka prowadzi: **rejestr upoważnień i kart dostępu** (Załącznik nr 6), wykaz kont uprzywilejowanych, wykaz systemów (Załącznik nr 16) oraz rejestr wyłączeń jawności w systemach centralnych.
2. Rejestry prowadzi się w postaci elektronicznej, z zapewnieniem rozliczalności zmian; dopuszcza się postać papierową.
3. Rejestr upoważnień prowadzi IOD, wykazy techniczne - ASI.

CZĘŚĆ V
PRZETWARZANIE W SYSTEMACH CENTRALNYCH

§ 28. Centralny Rejestr Umów JSFP

1. Jednostka udostępnia i aktualizuje informacje o umowach w CRU JSFP na zasadach określonych w art. 34a i 34b ustawy o finansach publicznych oraz przepisach wykonawczych.
2. Do rejestru wprowadza się **wyłącznie informacje o umowie** w zakresie przewidzianym przepisami. **Nie zamieszcza się treści umowy ani jej skanu.**
3. Informacje udostępnia się bez zbędnej zwłoki, nie później niż w terminie **30 dni** od dnia zawarcia umowy albo od dnia zmiany objętych rejestrem informacji. W Jednostce ustala się wewnętrzny termin przekazania danych przez komórkę merytoryczną wynoszący **14 dni**.
4. Przed wprowadzeniem informacji do rejestru dokonuje się przeglądu pod kątem ochrony danych osobowych i informacji prawnie chronionych - obejmuje on ocenę, czy zachodzi podstawa wyłączenia jawności oraz czy opis przedmiotu umowy nie ujawnia informacji chronionej.
5. Osoby wykonujące czynności w CRU działają wyłącznie w granicach nadanej roli, na podstawie Karty dostępu do systemów centralnych.

§ 29. Krajowy System e-Faktur

1. Faktury wystawia się, przesyła i odbiera za pośrednictwem KSeF na zasadach określonych w przepisach o podatku od towarów i usług.
2. Uprawnienia w KSeF nadaje podatnik. W przypadku jednostek objętych centralizacją rozliczeń podatku od towarów i usług uprawnienia dla pracowników Jednostki wynikają z uprawnień nadanych przez gminę oraz z pełnomocnictwa jej organu wykonawczego, jeżeli jest wymagane.
3. Uwierzytelnianie w KSeF odbywa się wyłącznie przy użyciu środków przypisanych imiennie użytkownikowi. Certyfikaty wystawcy faktur wydaje się imiennie; ich unieważnienie następuje niezwłocznie po ustaniu podstawy dostępu.
4. Dane przetwarzane w KSeF objęte są **tajemnicą skarbową** (art. 293 Ordynacji podatkowej). W zakresie danych zgromadzonych w KSeF odrębnym administratorem jest organ prowadzący ten system.
5. Pobrane z KSeF faktury i urzędowe poświadczenia odbioru przechowuje się w systemach Jednostki zgodnie z zasadami retencji określonymi w § 59.

§ 30. Wyłączenia jawności w systemach centralnych

1. Jeżeli informacja podlegająca udostępnieniu w systemie centralnym objęta jest ograniczeniem jawności wynikającym z przepisów o dostępie do informacji publicznej, informacji tej **nie wprowadza się do systemu**, wskazując w przewidzianych do tego polach podstawę prawną wyłączenia oraz osobę albo organ, które go dokonały.
2. Wyłączenie jawności **nie jest anonimizacją w rozumieniu przepisów o ochronie danych osobowych** - informacji nie usuwa się ani nie zaciera.
3. Decyzję o wyłączeniu jawności podejmuje **Administrator**, na piśmie, po zaopiniowaniu przez IOD (gdy podstawą jest prywatność osoby fizycznej) albo przez radcę prawnego (gdy podstawą jest tajemnica ustawowo chroniona lub tajemnica przedsiębiorcy). Decyzji tej nie powierza się osobie wprowadzającej ani publikującej dane.
4. Wyłączenia stosuje się w najwęższym możliwym zakresie; jawność jest zasadą, a ograniczenie wyjątkiem podlegającym ścisłej wykładni.
5. Szczegółowy tryb oceny, dokumentowania i przeglądu wyłączeń jawności określa odrębna **Procedura oceny i dokumentowania wyłączeń jawności w CRU JSFP**, przyjęta zarządzeniem Administratora.

§ 31. Rozliczalność czynności w systemach centralnych

1. Każda czynność dokonana w systemie centralnym musi być możliwa do przypisania konkretnej osobie. Zabronione jest wykonywanie czynności „za kogoś" na cudzym koncie.
2. Potwierdzenia czynności (numery referencyjne, urzędowe poświadczenia odbioru, potwierdzenia publikacji) pobiera się i przechowuje w aktach sprawy.
3. Zestawienie czynności wykonanych w systemach centralnych podlega przeglądowi w ramach półrocznego przeglądu uprawnień.

CZĘŚĆ VI
BEZPIECZEŃSTWO POZA ŚRODOWISKIEM TELEINFORMATYCZNYM

§ 32. Obszary przetwarzania i zabezpieczenia fizyczne

1. Obszarem przetwarzania są pomieszczenia i miejsca, w których Jednostka przetwarza dane; ich wykaz prowadzi ASI w ramach Załącznika nr 16.
2. Dokumenty zawierające dane osobowe przechowuje się w zamykanych szafach, w pomieszczeniach zamykanych na klucz. Po zakończeniu pracy pomieszczenia i szafy zamyka się.
3. Klucze wydaje się osobom uprawnionym; ich przekazywanie osobom nieuprawnionym jest zabronione. Utratę klucza zgłasza się niezwłocznie Administratorowi i ASI.
4. Osoby postronne przebywają w obszarze przetwarzania wyłącznie w obecności pracownika Jednostki.
5. Pomieszczenie serwerowe lub szafę teleinformatyczną zabezpiecza się przed dostępem osób nieuprawnionych, zalaniem, pożarem i skutkami zaniku zasilania.

§ 33. Zasada czystego biurka i czystego ekranu

1. Dokumenty zawierające dane osobowe nie mogą pozostawać bez nadzoru na biurku, w drukarce, na kserokopiarce ani w innych miejscach dostępnych dla osób nieuprawnionych.
2. Opuszczając stanowisko pracy, użytkownik blokuje ekran; system blokuje się samoczynnie po **nie więcej niż 10 minutach** bezczynności.
3. Monitory ustawia się tak, aby ich zawartość nie była widoczna dla osób postronnych, w szczególności przy stanowiskach obsługi interesantów.

§ 34. Obieg, kopiowanie i niszczenie dokumentacji

1. Dokumenty przekazuje się wyłącznie osobom uprawnionym, za pokwitowaniem, jeżeli wymaga tego charakter sprawy.
2. Kopie dokumentów sporządza się wyłącznie w zakresie niezbędnym; kopie zbędne niszczy się niezwłocznie.
3. Dokumenty przeznaczone do zniszczenia niszczy się w niszczarce zapewniającej co najmniej **poziom bezpieczeństwa P-4** według normy DIN 66399, albo przekazuje wyspecjalizowanemu podmiotowi na podstawie umowy powierzenia przetwarzania i za protokołem.

4. Brakowanie dokumentacji następuje zgodnie z przepisami kancelaryjno-archiwalnymi i wymaga zgody właściwego archiwum państwowego.
5. Korespondencję zawierającą dane osobowe wysyła się w sposób uniemożliwiający zapoznanie się z jej treścią przez osoby nieuprawnione.

§ 35. Dokumenty poza siedzibą Jednostki

1. Wynoszenie dokumentów zawierających dane osobowe poza siedzibę Jednostki wymaga zgody Administratora, z wyjątkiem czynności wykonywanych w terenie w ramach obowiązków służbowych.
2. Dokumenty przewozi się w sposób uniemożliwiający dostęp osób nieuprawnionych; nie pozostawia się ich w pojazdach bez nadzoru.
3. Utratę dokumentu zgłasza się niezwłocznie IOD jako podejrzenie naruszenia ochrony danych.

CZĘŚĆ VII
BEZPIECZEŃSTWO ŚRODOWISKA TELEINFORMATYCZNEGO

§ 36. Stacje robocze i oprogramowanie

1. Do przetwarzania danych służbowych używa się wyłącznie sprzętu Jednostki. Korzystanie ze sprzętu prywatnego wymaga zgody Administratora i spełnienia warunków określonych w § 41.
2. Instalowanie oprogramowania należy wyłącznie do ASI. Użytkownicy nie posiadają uprawnień administracyjnych na stacjach roboczych.
3. Stosuje się wyłącznie oprogramowanie licencjonowane i wspierane przez producenta. Oprogramowanie, dla którego producent zakończył wsparcie, wycofuje się z eksploatacji albo - gdy jest to niemożliwe - izoluje i obejmuje dodatkowymi zabezpieczeniami na podstawie decyzji Administratora poprzedzonej analizą ryzyka.
4. Aktualizacje zabezpieczeń instaluje się niezwłocznie, a krytyczne - **nie później niż w ciągu 7 dni** od udostępnienia.
5. Dyski stacji roboczych i komputerów przenośnych podlegają szyfrowaniu.
6. Stanowiska z dostępem do rejestrów państwowych (w szczególności do systemu Źródło, Rejestru Dowodów Osobistych i CEIDG) zabezpiecza się zgodnie z wymaganiami określonymi dla tych systemów przez ich administratorów; dostęp do nich odbywa się wyłącznie z urządzeń wskazanych przez ASI i przy użyciu imiennych środków uwierzytelniania.
7. Systemy dziedzinowe Jednostki (w szczególności podatków i opłat lokalnych, gospodarki odpadami, księgowości, kadr i płac oraz elektronicznego obiegu dokumentów) udostępnia się zgodnie z zasadą wiedzy koniecznej; jeżeli dostawca świadczy usługi zdalnie lub w chmurze, wiąże go umowa powierzenia przetwarzania danych.

§ 37. Poczta elektroniczna i doręczenia elektroniczne

1. Służbowa poczta elektroniczna służy wyłącznie celom służbowym. Zabronione jest przekierowywanie służbowej korespondencji na skrzynki prywatne.
2. Przed wysłaniem wiadomości weryfikuje się adresata. Przy wysyłce do wielu odbiorców zewnętrznych stosuje się pole ukrytej kopii (UDW).
3. Załączniki zawierające dane osobowe - w szczególności zestawienia, wykazy i dokumenty kadrowe - **szyfruje się**, a hasło przekazuje odrębnym kanałem (telefonicznie lub wiadomością SMS).
4. Zabronione jest otwieranie załączników i odnośników z wiadomości niespodziewanych lub budzących wątpliwości. Podejrzaną wiadomość zgłasza się ASI i nie usuwa do czasu jej analizy.
5. Doręczenia elektroniczne realizuje się przez adres do doręczeń elektronicznych Jednostki; obsługę skrzynki powierza się imiennie wskazanym osobom.

§ 38. Sieci i dostęp do internetu

1. Dostęp do internetu służy celom służbowym. Zabronione jest korzystanie ze stron i usług niezwiązanych z pracą, w szczególności serwisów wymiany plików oraz stron o nieustalonej reputacji.
2. Zabronione jest wyłączanie lub omijanie zabezpieczeń sieciowych, w tym filtrowania treści i ochrony antywirusowej.
3. Sieć bezprzewodową udostępnianą interesantom i gościom oddziela się logicznie od sieci służbowej.

4. Korzystanie z publicznych, otwartych sieci bezprzewodowych do pracy służbowej jest dopuszczalne wyłącznie przez połączenie VPN.
5. Konfigurację urządzeń sieciowych, w tym zmianę haseł domyślnych, dokumentuje ASI.

§ 39. Nośniki danych i szyfrowanie

1. Do przenoszenia danych używa się wyłącznie nośników Jednostki, ujętych w wykazie i **zaszyfrowanych**.
2. Zabronione jest podłączanie nośników niewiadomego pochodzenia do sprzętu Jednostki.
3. Nośniki przeznaczone do wycofania poddaje się trwałemu usunięciu danych albo zniszczeniu fizycznemu; czynność dokumentuje się protokołem.
4. Nośniki przechowuje się w zamykanych szafach; nie pozostawia się ich bez nadzoru.

§ 40. Urządzenia mobilne

1. Służbowe komputery przenośne, tablety i telefony zabezpiecza się kodem dostępu lub danymi biometrycznymi oraz szyfrowaniem pamięci.
2. Urządzenia mobilne nie mogą być udostępniane osobom trzecim, w tym członkom rodziny.
3. Utratę urządzenia zgłasza się niezwłocznie ASI i IOD; ASI podejmuje działania zdalnego zablokowania lub usunięcia danych, jeżeli jest to technicznie możliwe.

§ 41. Praca zdalna

1. Praca zdalna z dostępem do danych osobowych wymaga zgody Administratora i odbywa się wyłącznie na sprzęcie Jednostki, przez połączenie VPN.
2. Miejsce wykonywania pracy zdalnej musi zapewniać, że osoby postronne nie mają wglądu w dane ani dostępu do sprzętu i dokumentów.
3. Zabronione jest drukowanie dokumentów zawierających dane osobowe poza siedzibą Jednostki, chyba że Administrator wyrazi zgodę i zapewniono warunki bezpiecznego zniszczenia wydruków.
4. Rozmowy służbowe dotyczące spraw obejmujących dane osobowe prowadzi się w warunkach zapewniających poufność.

§ 42. Kopie zapasowe i ciągłość działania

1. Dane przetwarzane w systemach Jednostki podlegają kopiowaniu zapasowemu **nie rzadziej niż raz na dobę** w odniesieniu do danych zmieniających się codziennie oraz **nie rzadziej niż raz w tygodniu** w odniesieniu do pozostałych.
2. Stosuje się zasadę **3–2–1**: co najmniej trzy kopie danych, na dwóch różnych nośnikach, w tym jedna kopia przechowywana poza podstawową lokalizacją.
3. Co najmniej jedna kopia zabezpieczona jest przed modyfikacją i usunięciem (kopia niezmienna lub odłączona od sieci) - jako zabezpieczenie przed oprogramowaniem szyfrującym dane.
4. Skuteczność kopii weryfikuje się **testem odtworzenia nie rzadziej niż raz na pół roku**; wynik dokumentuje się.
5. Jednostka określa dopuszczalny czas niedostępności usługi oraz dopuszczalny zakres utraty danych dla każdego systemu krytycznego i dokumentuje je w wykazie systemów.
6. Na wypadek utraty dostępności systemów Jednostka utrzymuje plan postępowania awaryjnego obejmujący sposób realizacji zadań w trybie zastępczym, kolejność przywracania systemów oraz listę kontaktów awaryjnych.

§ 43. Ochrona przed szkodliwym oprogramowaniem i socjotechniką

1. Na wszystkich stacjach roboczych i serwerach działa oprogramowanie chroniące przed szkodliwym oprogramowaniem, z automatyczną aktualizacją i skanowaniem.
2. Wyłączanie ochrony antywirusowej jest zabronione; czasowe wyłączenie na potrzeby czynności serwisowych wymaga zgody ASI i jest odnotowywane.
3. W razie podejrzenia zainfekowania użytkownik **niezwłocznie odłącza komputer od sieci, nie wyłączając go**, i zawiadamia ASI.
4. Prób wyłudzenia informacji (phishing, vishing, podszywanie się pod przełożonego) nie realizuje się; polecenia dotyczące przelewów, zmiany numerów rachunków lub przekazania danych, otrzymane drogą elektroniczną, weryfikuje się dodatkowym kanałem.

CZĘŚĆ VIII
SZTUCZNA INTELIGENCJA

§ 44. Zakaz korzystania z zewnętrznych narzędzi sztucznej inteligencji

> **Zakaz podstawowy.** Zabrania się wprowadzania jakichkolwiek danych osobowych, informacji prawnie chronionych oraz niepublikowanych dokumentów Jednostki do zewnętrznych narzędzi sztucznej inteligencji, w tym do publicznie dostępnych asystentów konwersacyjnych, generatorów treści, translatorów, narzędzi transkrypcji i analizy dokumentów, niezależnie od tego, czy korzystanie z nich jest odpłatne.

1. Zakaz, o którym mowa w ust. 1, obejmuje również narzędzia wbudowane w oprogramowanie biurowe, przeglądarki i pocztę elektroniczną, jeżeli przetwarzają one dane poza infrastrukturą kontrolowaną przez Jednostkę.
2. Uzasadnieniem zakazu jest brak podstawy prawnej powierzenia danych takim narzędziom, brak umowy powierzenia przetwarzania spełniającej wymagania art. 28 RODO, brak kontroli nad miejscem i celem dalszego przetwarzania oraz ryzyko wykorzystania wprowadzonych treści do trenowania modeli.
3. Zabronione jest w szczególności: wprowadzanie treści dokumentów zawierających dane osobowe w celu ich streszczenia, tłumaczenia lub redakcji, wprowadzanie fragmentów akt spraw, danych kadrowych, płacowych, finansowych i danych uczniów, a także wykorzystywanie narzędzi AI do przygotowywania rozstrzygnięć w sprawach indywidualnych.
4. Dopuszcza się korzystanie z narzędzi AI wyłącznie do celów niezwiązanych z danymi Jednostki, na sprzęcie prywatnym, poza godzinami pracy - co pozostaje poza zakresem regulacji Polityki.
5. Naruszenie zakazu traktuje się jako naruszenie podstawowych obowiązków pracowniczych oraz jako potencjalne naruszenie ochrony danych podlegające zgłoszeniu w trybie Części X.

§ 45. Tryb dopuszczenia narzędzia własnego Jednostki

1. Administrator może dopuścić do stosowania narzędzie wykorzystujące sztuczną inteligencję, jeżeli łącznie: narzędzie działa w infrastrukturze Jednostki albo w infrastrukturze podmiotu przetwarzającego związanego umową powierzenia; dane nie są wykorzystywane do trenowania modeli udostępnianych innym podmiotom; zapewniono rozliczalność i możliwość kontroli działania narzędzia.
2. Dopuszczenie poprzedza się **analizą ryzyka oraz - gdy jest wymagana - oceną skutków dla ochrony danych**, a także opinią IOD i ASI.
3. Dopuszczenie następuje w formie pisemnej decyzji Administratora określającej: nazwę narzędzia, dopuszczalne zastosowania, kategorie danych, osoby uprawnione do korzystania oraz obowiązek weryfikacji wyników przez człowieka.
4. Wyniki działania narzędzia AI **nigdy nie stanowią samodzielnej podstawy rozstrzygnięcia**; odpowiedzialność za treść dokumentu ponosi osoba go sporządzająca.
5. Jednostka prowadzi **rejestr dopuszczonych narzędzi AI** zawierający: nazwę, dostawcę, podstawę dopuszczenia, datę decyzji, zakres zastosowania, datę ostatniego przeglądu. Rejestr podlega przeglądowi raz w roku.
6. Postanowienia niniejszego paragrafu stosuje się niezależnie od obowiązków, które mogą wynikać z przepisów o sztucznej inteligencji obowiązujących w Unii Europejskiej.

CZĘŚĆ IX
PODMIOTY PRZETWARZAJĄCE I PODWYKONAWCY

§ 46. Zasady powierzenia przetwarzania

1. Powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu wymaga zawarcia **pisemnej umowy powierzenia** spełniającej wymagania art. 28 ust. 3 RODO, przed rozpoczęciem przetwarzania.
2. Umowa powierzenia określa co najmniej: przedmiot i czas przetwarzania, charakter i cel przetwarzania, rodzaj danych i kategorie osób, obowiązki i prawa Administratora, zobowiązanie do przetwarzania wyłącznie na udokumentowane polecenie, zobowiązanie do zachowania poufności, obowiązek stosowania środków bezpieczeństwa, zasady dalszego powierzenia, wsparcie w realizacji praw osób i obowiązków z art. 32–36 RODO, sposób postępowania po zakończeniu świadczenia usług oraz prawo Administratora do kontroli.

3. Powierzenia wymagają w szczególności: obsługa informatyczna i serwis systemów, hosting i usługi chmurowe, obsługa prawna świadcząca usługi na danych, niszczenie dokumentacji, obsługa BHP i medycyny pracy, obsługa kadrowo-płacowa realizowana zewnętrznie, archiwizacja dokumentacji.
4. Nie stanowi powierzenia udostępnienie danych podmiotowi, który przetwarza je we własnym celu i na własną odpowiedzialność (odrębny administrator) - w takim przypadku podstawę udostępnienia stanowi przepis prawa.

§ 47. Weryfikacja podmiotu przetwarzającego

1. Przed zawarciem umowy powierzenia Administrator weryfikuje, czy podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.
2. Weryfikacja obejmuje co najmniej: oświadczenie podmiotu o stosowanych zabezpieczeniach, informację o wyznaczeniu IOD, informację o lokalizacji przetwarzania danych, informację o stosowaniu szyfrowania i kopii zapasowych, informację o dotychczasowych naruszeniach ochrony danych oraz - jeżeli podmiot je posiada - certyfikaty lub sprawozdania z audytów.
3. Wynik weryfikacji dokumentuje się i przechowuje wraz z umową.
4. Weryfikację powtarza się przy przedłużeniu umowy oraz nie rzadziej niż **raz na trzy lata** w przypadku umów wieloletnich.

§ 48. Dalsze powierzenie i podwykonawcy

1. Podmiot przetwarzający może korzystać z usług podwykonawcy wyłącznie na podstawie **uprzedniej pisemnej zgody Administratora** albo ogólnej pisemnej zgody z obowiązkiem informowania o zamierzonych zmianach.
2. W przypadku zgody ogólnej Administratorowi przysługuje **prawo sprzeciwu** wobec zamierzonej zmiany, zgłaszane w terminie określonym w umowie, nie krótszym niż 14 dni.
3. Podwykonawca musi zostać związany tymi samymi obowiązkami ochrony danych, które ciążą na podmiocie przetwarzającym. Podmiot przetwarzający ponosi wobec Administratora pełną odpowiedzialność za działania podwykonawcy.
4. Jednostka prowadzi **wykaz podmiotów przetwarzających i ich podwykonawców** (Załącznik nr 17), aktualizowany niezwłocznie po każdej zmianie.
5. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej - w tym korzystanie z usług chmurowych z serwerami poza Europejskim Obszarem Gospodarczym - wymaga odrębnej podstawy z rozdziału V RODO i pisemnej decyzji Administratora poprzedzonej analizą ryzyka.

§ 49. Postanowienia w umowach z dostawcami usług informatycznych

W umowach z dostawcami usług informatycznych zamieszcza się, poza umową powierzenia, postanowienia określające co najmniej:

a) czas reakcji i czas usunięcia awarii dla poszczególnych kategorii zgłoszeń;
b) zasady dostępu serwisowego: imienne konta, włączanie dostępu na czas czynności, rejestrowanie sesji;
c) obowiązek niezwłocznego - nie później niż w ciągu **24 godzin** - powiadomienia Administratora o naruszeniu ochrony danych lub incydencie bezpieczeństwa;
d) obowiązek współdziałania przy obsłudze incydentu i przy realizacji praw osób, których dane dotyczą;
e) zasady przekazania danych i ich trwałego usunięcia po zakończeniu umowy, wraz z terminem i formą potwierdzenia;
f) zakaz wykorzystywania danych Jednostki do celów własnych dostawcy, w tym do rozwoju lub trenowania narzędzi.

§ 50. Rejestr i kontrola podmiotów przetwarzających

1. IOD prowadzi rejestr umów powierzenia zawierający: podmiot, przedmiot powierzenia, kategorie danych, datę zawarcia i obowiązywania, informację o podwykonawcach oraz datę ostatniej weryfikacji.
2. Administratorowi przysługuje prawo kontroli podmiotu przetwarzającego. Kontrolę przeprowadza się w razie potrzeby, a w przypadku podmiotów przetwarzających dane szczególnych kategorii lub dane na dużą skalę - nie rzadziej niż **raz na dwa lata**.
3. Kontrola może przyjąć formę audytu na miejscu albo weryfikacji na podstawie kwestionariusza i dokumentów; z czynności sporządza się protokół.

CZĘŚĆ X
INCYDENTY I NARUSZENIA

§ 51. Zgłoszenie wewnętrzne

1. Każda osoba, która stwierdzi lub podejrzewa naruszenie ochrony danych albo incydent bezpieczeństwa, zgłasza to **niezwłocznie, nie później niż w ciągu 4 godzin** od stwierdzenia, IOD oraz ASI - telefonicznie, a następnie na formularzu stanowiącym **Załącznik nr 14**.
2. Zgłoszeniu podlegają w szczególności: wysłanie danych do niewłaściwego odbiorcy, utrata dokumentu, nośnika lub urządzenia, ujawnienie hasła, podejrzenie zainfekowania systemu, nieuprawniony dostęp do konta lub pomieszczenia, awaria powodująca utratę danych, opublikowanie w systemie centralnym informacji objętej ograniczeniem jawności.
3. Do czasu decyzji IOD nie podejmuje się działań mogących zatrzeć ślady zdarzenia; w szczególności nie usuwa się podejrzanych wiadomości i nie formatuje nośników.
4. Zgłoszenie zdarzenia w dobrej wierze nie może stanowić podstawy negatywnych konsekwencji wobec zgłaszającego.

§ 52. Ocena naruszenia i zgłoszenie organowi nadzorczemu

1. IOD ocenia zdarzenie pod kątem wystąpienia naruszenia ochrony danych oraz poziomu ryzyka naruszenia praw lub wolności osób fizycznych, uwzględniając rodzaj naruszenia, charakter i liczbę danych, łatwość identyfikacji osób, możliwe skutki oraz szczególne cechy osób i administratora.
2. Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych **bez zbędnej zwłoki, nie później niż w terminie 72 godzin** od stwierdzenia naruszenia. Zgłoszenie po tym terminie wymaga wyjaśnienia przyczyn opóźnienia.
3. Jeżeli pełna informacja nie jest dostępna, dokonuje się zgłoszenia częściowego i uzupełnia je sukcesywnie.
4. Decyzję o niezgłaszaniu naruszenia dokumentuje się wraz z uzasadnieniem oceny ryzyka.

§ 53. Zawiadomienie osób, których dane dotyczą

1. Jeżeli naruszenie może powodować **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, Administrator zawiadamia te osoby bez zbędnej zwłoki, jasnym i prostym językiem.
2. Zawiadomienie zawiera: opis charakteru naruszenia, dane kontaktowe IOD, opis możliwych konsekwencji, opis środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu oraz zalecenia dla osoby.
3. Zawiadomienie nie jest wymagane, jeżeli dane były zabezpieczone w sposób uniemożliwiający ich odczytanie (np. skuteczne szyfrowanie), zastosowano środki eliminujące wysokie ryzyko albo zawiadomienie wymagałoby niewspółmiernie dużego wysiłku - wówczas stosuje się publiczny komunikat.

§ 54. Incydenty cyberbezpieczeństwa

1. Incydent dotyczący systemu teleinformatycznego obsługuje Koordynator ds. cyberbezpieczeństwa we współpracy z ASI, według procedury: wykrycie - zabezpieczenie śladów - ograniczenie skutków - usunięcie przyczyny - przywrócenie działania - analiza poincydentalna.
2. Jeżeli Jednostka podlega obowiązkom wynikającym z ustawy o KSC, incydent zgłasza się właściwemu zespołowi CSIRT w terminach wynikających z tej ustawy; zgłoszenie obejmuje wczesne ostrzeżenie, zgłoszenie właściwe oraz sprawozdanie końcowe.
3. Zdarzenie może być jednocześnie incydentem bezpieczeństwa i naruszeniem ochrony danych - w takim przypadku prowadzi się **obie ścieżki równolegle**, a terminy liczy się niezależnie.
4. Po zakończeniu obsługi incydentu sporządza się analizę zawierającą przyczynę źródłową oraz działania zapobiegające powtórzeniu; działania te wprowadza się do planu doskonalenia SZBI.

§ 55. Rejestry i działania naprawcze

1. IOD prowadzi **rejestr naruszeń ochrony danych**, a Koordynator - **rejestr incydentów bezpieczeństwa**; dopuszcza się prowadzenie jednego rejestru wspólnego według wzoru stanowiącego Załącznik nr 15.
2. Rejestr zawiera co najmniej: datę i sposób stwierdzenia, opis zdarzenia, kategorie i przybliżoną liczbę osób oraz wpisów danych, skutki, zastosowane środki, ocenę ryzyka, informację o zgłoszeniu organowi nadzorczemu i zawiadomieniu osób oraz działania naprawcze.
3. Rejestry przechowuje się przez okres **5 lat** od zakończenia obsługi zdarzenia.

4. Administrator raz w roku dokonuje analizy zbiorczej zdarzeń i na jej podstawie aktualizuje analizę ryzyka oraz plan szkoleń.

CZĘŚĆ XI
PRAWA OSÓB I OBOWIĄZEK INFORMACYJNY

§ 56. Zasady realizacji obowiązku informacyjnego wobec osób, których dane dotyczą

1. Administrator zapewnia realizację obowiązków informacyjnych wobec osób, których dane dotyczą, zgodnie z zasadami określonymi w RODO, w szczególności w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny, przy zastosowaniu jasnego i prostego języka, stosownie do art. 12 ust. 1 RODO. Wymóg ten podlega szczególnemu uwzględnieniu w przypadku, gdy informacje lub komunikaty są kierowane do osób małoletnich.
2. W przypadku pozyskiwania danych osobowych bezpośrednio od osoby, której dane dotyczą, Administrator przekazuje informacje wymagane przepisami art. 13 RODO w chwili pozyskania danych.
3. Jeżeli dane osobowe nie zostały pozyskane od osoby, której dotyczą, Administrator realizuje obowiązek informacyjny zgodnie z art. 14 RODO, w terminie odpowiednim do okoliczności przetwarzania, nie później jednak niż:
   a) w rozsądnym terminie po pozyskaniu danych osobowych, nieprzekraczającym jednego miesiąca z uwzględnieniem konkretnych okoliczności przetwarzania danych;
   b) przy pierwszej komunikacji z osobą, której dane dotyczą - jeżeli dane osobowe mają być wykorzystane do komunikowania się z tą osobą;
   c) najpóźniej przy pierwszym ujawnieniu danych - jeżeli planowane jest ujawnienie danych osobowych innemu odbiorcy.
4. Obowiązku informacyjnego nie realizuje się ponownie w zakresie, w jakim osoba, której dane dotyczą, dysponuje już wymaganymi informacjami (art. 13 ust. 4 i art. 14 ust. 5 lit. a RODO), a także w pozostałych przypadkach, w których przepisy RODO przewidują odstępstwo od obowiązku przekazania informacji, w szczególności określonych w art. 14 ust. 5 lit. b–d RODO. Skorzystanie z odstępstwa wymaga odnotowania jego podstawy w dokumentacji danego procesu przetwarzania.
5. Informacje przekazywane są w formie pisemnej lub w inny sposób, w tym – stosownie do okoliczności – w formie elektronicznej. Na żądanie osoby, której dane dotyczą, informacje mogą zostać przekazane ustnie, pod warunkiem potwierdzenia jej tożsamości w sposób adekwatny do charakteru żądania i kategorii przetwarzanych danych.
6. Za organizacyjne zapewnienie prawidłowej realizacji obowiązków informacyjnych odpowiada Administrator. Osoby upoważnione do przetwarzania danych osobowych, w zakresie powierzonych im obowiązków służbowych lub wykonywanych czynności, zobowiązane są do stosowania właściwych klauzul informacyjnych oraz dokumentów związanych z pozyskiwaniem i przetwarzaniem danych osobowych. Inspektor Ochrony Danych opiniuje wzory klauzul informacyjnych oraz ich zmiany.
7. Każdorazowo należy zapewnić, aby zakres przekazywanych informacji odpowiadał celowi i podstawie prawnej przetwarzania, kategoriom przetwarzanych danych, źródłu ich pozyskania, przewidywanym odbiorcom danych, okresowi przechowywania danych oraz charakterowi procesu, w ramach którego dane są przetwarzane. Stosowanie wzorów klauzul informacyjnych nie zwalnia osoby realizującej dany proces z obowiązku oceny ich adekwatności do konkretnego przypadku.
8. Administrator realizuje obowiązki informacyjne wynikające z art. 13 i art. 14 RODO w szczególności przy wykorzystaniu wzorów klauzul informacyjnych stanowiących załączniki do niniejszej Polityki. Podstawowy katalog klauzul obejmuje:

Nr	Rodzaj klauzuli	Podstawowe zastosowanie	Załącznik
1	Ogólna – realizacja zadań statutowych	obsługa interesantów, prowadzenie korespondencji, w tym doręczeń elektronicznych, realizacja spraw administracyjnych i organizacyjnych, strona internetowa, BIP, tablice informacyjne, punkty obsługi	nr 7
2	Rekrutacyjna	nabór na wolne stanowiska pracy, przyjmowanie i rozpatrywanie dokumentów aplikacyjnych	nr 8
3	Pracownicza	pracownicy, osoby świadczące pracę lub usługi na innej podstawie prawnej, praktykanci, stażyści oraz inne osoby wykonujące czynności na rzecz Administratora	nr 9
4	Umowy, CRU i KSeF	zawieranie i wykonywanie umów, w tym umów sprzedaży, dostawy, zlecenia, o dzieło, najmu, dzierżawy oraz umów nienazwanych; realizacja	nr 10

		obowiązków dotyczących Centralnego Rejestru Umów oraz Krajowego Systemu e-Faktur	
5	Dochodzenie należności i wykonywanie zobowiązań	windykacja należności, wezwania do zapłaty, zawieranie ugód, postępowania sądowe, administracyjne i egzekucyjne oraz czynności związane z wykonywaniem zobowiązań	nr 11

9. W celu zapewnienia spójności, przejrzystości i aktualności dokumentacji stosuje się w pierwszej kolejności podstawowe wzory klauzul określone w ust. 8. Nie tworzy się odrębnej klauzuli dla każdego pojedynczego procesu przetwarzania, jeżeli wymagane informacje mogą zostać prawidłowo przekazane przez odpowiednie dostosowanie klauzuli podstawowej.
10. W przypadku procesu nietypowego, wymagającego przekazania informacji wykraczających poza zakres podstawowego wzoru, właściwa klauzula podlega odpowiedniemu uzupełnieniu lub modyfikacji.
11. Jeżeli ze względu na odmienny cel, podstawę prawną, kategorię osób, zakres danych albo sposób ich przetwarzania zastosowanie lub dostosowanie istniejącego wzoru nie zapewnia prawidłowej realizacji obowiązku informacyjnego, dopuszczalne jest opracowanie odrębnej klauzuli informacyjnej. Katalog klauzul ma zatem charakter otwarty, przy czym tworzenie nowych wzorów powinno następować wyłącznie wówczas, gdy jest to uzasadnione charakterem procesu przetwarzania.
12. Właściwą klauzulę informacyjną przekazuje się osobie, której dane dotyczą, w sposób umożliwiający rzeczywiste zapoznanie się z jej treścią.
13. Klauzule informacyjne mogą być dodatkowo publikowane w Biuletynie Informacji Publicznej, na stronie internetowej Administratora, udostępniane w miejscach obsługi interesantów albo zamieszczane w formularzach, umowach, systemach teleinformatycznych lub innych dokumentach wykorzystywanych w danym procesie przetwarzania.
14. Samo opublikowanie klauzuli w Biuletynie Informacji Publicznej lub wywieszenie jej w siedzibie Administratora nie zastępuje indywidualnego wykonania obowiązku informacyjnego, jeżeli przepisy RODO wymagają przekazania informacji konkretnej osobie, której dane dotyczą.
15. Co do zasady nie wymaga się od osoby, której dane dotyczą, składania odrębnego oświadczenia o zapoznaniu się z klauzulą informacyjną ani potwierdzania jej treści podpisem. Obowiązek informacyjny ma charakter jednostronnego obowiązku Administratora, a jego wykonanie nie jest uzależnione od wyrażenia zgody, akceptacji ani podpisania klauzuli przez osobę, której dane dotyczą. W szczególności należy unikać rozwiązań, które mogłyby prowadzić do błędnego utożsamiania wykonania obowiązku informacyjnego z udzieleniem zgody na przetwarzanie danych osobowych.
16. Administrator zapewnia możliwość wykazania wykonania obowiązku informacyjnego, stosownie do charakteru danego procesu, w szczególności poprzez:
    a) odnotowanie przekazania klauzuli w aktach sprawy lub w systemie teleinformatycznym,
    b) zamieszczenie klauzuli w formularzu lub wniosku,
    c) wskazanie w umowie, że właściwa klauzula stanowi jej integralny załącznik,
    d) zachowanie dowodu wysłania informacji drogą elektroniczną,
    e) zastosowanie innego rozwiązania pozwalającego wykazać, kiedy i w jaki sposób obowiązek został zrealizowany.
17. Zgoda osoby, której dane dotyczą, jest pozyskiwana wyłącznie wówczas, gdy stanowi właściwą i rzeczywistą podstawę prawną przetwarzania danych osobowych. Nie należy żądać zgody, jeżeli przetwarzanie jest niezbędne w szczególności do:
    a) wypełnienia obowiązku prawnego ciążącego na Administratorze,
    b) wykonania umowy lub podjęcia działań przed jej zawarciem na żądanie osoby, której dane dotyczą,
    c) wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
    d) realizacji innej podstawy przetwarzania wynikającej z obowiązujących przepisów prawa.
18. W przypadku gdy podstawą przetwarzania jest zgoda, Administrator zapewnia, aby została ona wyrażona dobrowolnie, konkretnie, świadomie i jednoznacznie oraz aby osoba, której dane dotyczą, została poinformowana o możliwości jej wycofania w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem. Wycofanie zgody powinno być równie łatwe jak jej wyrażenie (art. 7 ust. 3 RODO).

§ 57. Realizacja praw osób, których dane dotyczą

1. Wnioski o realizację praw przyjmuje się w każdej formie; rejestruje je i przekazuje niezwłocznie IOD.
2. Odpowiedzi udziela się **bez zbędnej zwłoki, nie później niż w terminie miesiąca** od otrzymania wniosku. Termin można przedłużyć o kolejne dwa miesiące ze względu na skomplikowany charakter lub liczbę wniosków, informując o tym osobę w ciągu miesiąca.
3. Przed realizacją wniosku potwierdza się tożsamość wnioskodawcy w sposób proporcjonalny; nie żąda się przy tym danych nadmiarowych.
4. Prawo do usunięcia danych i prawo do przenoszenia danych są ograniczone i nie przysługują w zakresie, w jakim przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego albo wykonania zadania realizowanego w interesie publicznym - dotyczy to w szczególności danych publikowanych w CRU i przekazanych do KSeF.
5. Odmowę realizacji wniosku uzasadnia się i poucza o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz o środkach ochrony prawnej przed sądem.

§ 58. Rejestr czynności przetwarzania

1. Administrator prowadzi rejestr czynności przetwarzania (art. 30 ust. 1 RODO), a w zakresie danych powierzonych - rejestr kategorii czynności (art. 30 ust. 2 RODO).
2. Rejestr zawiera dla każdej czynności: nazwę i cel, podstawę prawną, kategorie osób i danych, kategorie odbiorców, planowane terminy usunięcia, informację o przekazaniu do państwa trzeciego oraz ogólny opis zabezpieczeń.
3. Rejestr aktualizuje IOD niezwłocznie po każdej zmianie; przegląd całościowy przeprowadza się raz w roku, łącznie z przeglądem Polityki.

§ 59. Okresy przechowywania i usuwanie danych

1. Dane przechowuje się przez okres wynikający z przepisów prawa, w szczególności przepisów kancelaryjno-archiwalnych, prawa pracy, prawa podatkowego i przepisów o rachunkowości, a w zakresie roszczeń - do upływu terminu przedawnienia.
2. Po upływie okresu przechowywania dane usuwa się albo poddaje anonimizacji, a dokumentację brakuje zgodnie z przepisami archiwalnymi.
3. Usunięcie danych z systemu obejmuje również kopie zapasowe - w zakresie technicznie możliwym, z uwzględnieniem cyklu nadpisywania kopii; sposób postępowania dokumentuje ASI.
4. Przegląd okresów przechowywania przeprowadza się raz w roku.

CZĘŚĆ XII
POSTANOWIENIA KOŃCOWE

§ 60. Przegląd, aktualizacja i wersjonowanie

1. Polityka podlega przeglądowi **nie rzadziej niż raz w roku**, a ponadto po: istotnej zmianie przepisów, zmianie struktury organizacyjnej, wdrożeniu lub wycofaniu systemu teleinformatycznego, naruszeniu ochrony danych o poważnych skutkach oraz po audycie bezpieczeństwa.
2. Zmiana Polityki wymaga nadania nowego numeru wersji i odnotowania w tabeli historii zmian zamieszczonej na początku dokumentu. Wersję archiwalną przechowuje się przez okres **5 lat**.
3. Przegląd, który nie skutkuje zmianą treści, odnotowuje się w tabeli potwierdzenia przeglądu okresowego.
4. Za inicjowanie przeglądu odpowiada IOD; zmiany zatwierdza Administrator.

§ 61. Odpowiedzialność

1. Naruszenie postanowień Polityki stanowi naruszenie podstawowych obowiązków pracowniczych i może skutkować odpowiedzialnością porządkową oraz rozwiązaniem stosunku pracy.
2. Niezależnie od odpowiedzialności pracowniczej, naruszenie przepisów o ochronie danych osobowych może rodzić odpowiedzialność cywilną, administracyjną i karną, a w przypadku osób odpowiedzialnych za gospodarkę finansową - także odpowiedzialność za naruszenie dyscypliny finansów publicznych.
3. Odpowiedzialność za wdrożenie i skuteczność środków ochrony ponosi Administrator; powierzenie zadań pracownikom nie zwalnia go z tej odpowiedzialności.

§ 62. Wejście w życie

1. Polityka wchodzi w życie z dniem określonym w zarządzeniu wprowadzającym.
2. Z dniem wejścia w życie Polityki tracą moc dotychczasowe regulacje wewnętrzne Jednostki w zakresie ochrony danych osobowych i bezpieczeństwa informacji wraz z załącznikami.
3. Postanowienia Polityki dotyczące systemów centralnych stosuje się z uwzględnieniem odrębnej Procedury oceny i dokumentowania wyłączeń jawności w CRU JSFP.
4. Polityka udostępniana jest wszystkim osobom przetwarzającym dane; zapoznanie się z nią potwierdza się pisemnie przed dopuszczeniem do przetwarzania.
5. Integralną część Polityki stanowią załączniki nr 1–17.

Wójt
mgr inż. Edmund Ziółek

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Chrzypsko Wielkie, dnia ..... r.

Na podstawie art. 29 rozporządzenia (UE) 2016/679 (RODO) oraz § 19 Polityki ochrony i przetwarzania danych **upoważniam**

.....
(imię i nazwisko, stanowisko służbowe)

do przetwarzania danych osobowych w Urzędzie Gminy Chrzypsko Wielkie w następującym zakresie:

Kategorie danych (zwykłe / szczególnych kategorii - wskazać)	
Cele i procesy przetwarzania	
Operacje objęte upoważnieniem (zbieranie, utrwalanie, przechowywanie, zmienianie, udostępnianie, usuwanie)	
Systemy, w których osoba przetwarza dane (zgodnie z Kartą dostępu)	
Okres obowiązywania upoważnienia	

Upoważnienie jest imienne i nieprzenoszalne. Osoba upoważniona przetwarza dane wyłącznie na polecenie Administratora, w zakresie wskazanym powyżej, i obowiązana jest zachować w tajemnicy dane oraz sposoby ich zabezpieczenia - bezterminowo, także po ustaniu zatrudnienia.

Upoważnienie wygasa z chwilą jego odwołania, ustania zatrudnienia albo zmiany zakresu obowiązków wykluczającej przetwarzanie danych.

Upoważnienie **nie jest równoznaczne z nadaniem dostępu do systemu teleinformatycznego** - dostęp nadaje się odrębnie, na podstawie Karty dostępu (Załącznik nr 4 lub 5).

data i podpis osoby upoważnionej
(przyjmuję do wiadomości i stosowania)

Wójt Gminy Chrzypsko Wielkie

Wpisano do rejestru upoważnień pod nr ..... w dniu ..... r.

Wójt
mgr inż. Edmund Ziółek

podpis IOD .....

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Chrzypsko Wielkie, dnia ..... r.

Z dniem ..... r. **odwołuję** upoważnienie nr .....

z dnia ..... r., udzielone Pani/Panu

.....
(imię i nazwisko, stanowisko służbowe)

Przyczyna odwołania:

☐ ustanie zatrudnienia,

☐ zmiana stanowiska lub zakresu obowiązków,

☐ zmiana organizacji pracy,

☐ naruszenie zasad ochrony danych lub bezpieczeństwa informacji,

☐ inna: .....

Równocześnie polecam **odebranie odpowiadających uprawnień we wszystkich systemach** - w systemach Jednostki i w systemach centralnych - najpóźniej w dniu odwołania upoważnienia, oraz odnotowanie tej czynności na Karcie dostępu i w rejestrze upoważnień.

Osoba, której upoważnienie odwołano, obowiązana jest zwrócić powierzone dokumenty, nośniki, sprzęt oraz środki uwierzytelniania. **Obowiązek zachowania tajemnicy trwa również po odwołaniu upoważnienia.**

data i podpis osoby, której odwołano upoważnienie

Wójt Gminy Chrzypsko Wielkie

Uprawnienia odebrane:

systemy Jednostki - dnia ..... (ASI .....);

systemy centralne - dnia ..... (administrator konta .....).

Wójt
mgr inż. Edmund Ziółek

OŚWIADCZENIE

osoby upoważnionej do przetwarzania danych osobowych
w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Chrzypsko Wielkie, dnia ..... r.

Ja, niżej podpisana/podpisany .....,

zatrudniona/zatrudniony na stanowisku ....., **oświadczam, że:**

1. zapoznałam się / zapoznałem się z Polityką ochrony i przetwarzania danych obowiązującą w Urzędzie Gminy Chrzypsko Wielkie oraz z treścią udzielonego mi upoważnienia i przyjmuję je do stosowania;
2. odbyłam / odbyłem szkolenie z zakresu ochrony danych osobowych i cyberbezpieczeństwa;
3. zobowiązuję się przetwarzać dane osobowe wyłącznie na polecenie Administratora i w zakresie wynikającym z upoważnienia;
4. zobowiązuję się zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia - bezterminowo, również po ustaniu zatrudnienia;
5. zobowiązuję się korzystać wyłącznie z przypisanych mi indywidualnych środków uwierzytelniania i nie udostępniać ich innym osobom;
6. zobowiązuję się stosować zasadę czystego biurka i czystego ekranu oraz zabezpieczać dokumenty i nośniki przed dostępem osób nieuprawnionych;
7. przyjmuję do wiadomości **zakaz wprowadzania danych Jednostki do zewnętrznych narzędzi sztucznej inteligencji**, określony w § 44 Polityki;
8. zobowiązuję się niezwłocznie, nie później niż w ciągu 4 godzin od stwierdzenia, zgłaszać Inspektorowi Ochrony Danych i Administratorowi Systemów Informatycznych każde podejrzenie naruszenia ochrony danych lub incydentu bezpieczeństwa;
9. zobowiązuję się zwrócić powierzone dokumenty, nośniki, sprzęt i środki uwierzytelniania z chwilą odwołania upoważnienia lub ustania zatrudnienia;
10. przyjmuję do wiadomości, że naruszenie powyższych obowiązków stanowi naruszenie podstawowych obowiązków pracowniczych i może rodzić odpowiedzialność porządkową, cywilną, administracyjną oraz karną.

podpis Inspektora Ochrony Danych

czytelny podpis składającego oświadczenie

Wójt
mgr inż. Edmund Ziółek

KARTA DOSTĘPU

do systemów teleinformatycznych Urzędu Gminy Chrzypsko Wielkie [w skrócie: UG]
ul. Główna 156, 64-412 Chrzypsko Wielkie

Imię i nazwisko / stanowisko	
Identyfikator użytkownika	
Numer i data upoważnienia	
Data wniosku / wnioskujący	

Zakres nadawanego dostępu

System	Rola / poziom uprawnień	Zakres danych	MFA	Data nadania	Podpis ASI

Zmiana i odebranie dostępu

System	Rodzaj czynności (zmiana / odebranie / blokada)	Przyczyna	Data	Podpis ASI

Dostęp nadaje się zgodnie z zasadą wiedzy koniecznej. Karta bez potwierdzenia wykonania czynności przez ASI nie dokumentuje nadania dostępu. Zwrot sprzętu i środków uwierzytelniania odnotowuje się poniżej.

data i podpis użytkownika

akceptacja - Wójt

Wójt
mgr inż. Edmund Ziółek

KARTA DOSTĘPU DO SYSTEMÓW CENTRALNYCH

w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Centralny Rejestr Umów JSFP • Krajowy System e-Faktur • inne systemy centralne

Imię i nazwisko / stanowisko	
PESEL lub NIP (identyfikator wymagany w systemie)	
Numer i data upoważnienia	
Podmiot, w imieniu którego działa użytkownik	**Urząd Gminy Chrzypsko Wielkie** [w skrócie: UG] ul. Główna 156, 64-412 Chrzypsko Wielkie

I. Centralny Rejestr Umów JSFP

☐ Administrator konta jednostki (administrator JSFP) ☐ Wprowadzający ☐ Publikujący

Zakres przedmiotowy: .....

II. Krajowy System e-Faktur

☐ Administrator ☐ Wystawianie faktur ☐ Dostęp do faktur ☐ Nadawanie i odbieranie uprawnień

☐ Samofakturowanie ☐ Faktury VAT RR ☐ Przeglądanie uprawnień i historii sesji ☐ Certyfikaty KSeF

Identyfikator jednostki wewnętrznej: .....

III. Inne systemy centralne

System	Rola / zakres uprawnień	Sposób uwierzytelniania	Data nadania	Nr referencyjny

IV. Odebranie uprawnień

System	Data odebrania	Osoba wykonująca	Nr referencyjny

Uwierzytelnianie w systemach centralnych odbywa się wyłącznie środkami przypisanymi imiennie użytkownikowi (podpis zaufany, kwalifikowany podpis elektroniczny, certyfikat, token). Ich udostępnianie innym osobom jest zabronione.

data i podpis użytkownika

akceptacja - Wójt

Wójt
mgr inż. Edmund Ziółek

REJESTR UPOWAŻNIEŃ I KART DOSTĘPU

w Urzędzie Gminy Chrzypsko Wielkie

ul. Główna 156, 64-412 Chrzypsko Wielkie

Lp.	Imię i nazwisko / stanowisko	Nr i data upoważnienia	Zakres przetwarzania	Systemy Jednostki (role)	Systemy centralne (role)	Data odwołania / odebrania	Uwagi

Rejestr prowadzi Inspektor Ochrony Danych. Podlega przeglądowi nie rzadziej niż raz na pół roku, łącznie z przeglądem uprawnień, o którym mowa w § 26 Polityki.

Wójt

mgr inż. Edmund Ziółek

KLAUZULA INFORMACYJNA NR 1

przetwarzanie danych osobowych w związku z realizacją zadań gminy i załatwianiem spraw w Urzędzie Gminy

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest **Wójt Gminy Chrzypsko Wielkie**, z siedzibą w Urzędzie Gminy Chrzypsko Wielkie, ul. Główna 156, 64-412 Chrzypsko Wielkie. W sprawach z zakresu rejestracji stanu cywilnego administratorem danych jest Kierownik Urzędu Stanu Cywilnego w Chrzypsku Wielkim (adres jak wyżej). Z Administratorem można się kontaktować:
   - na adres jego siedziby lub pod numerem tel. +48 61 295 10 11,
   - na adres **e-mail:** urzad@chrzypsko.pl
   - poprzez e-Doręczenia: AE:PL-64773-21728-SBJJD-24
2. W sprawach dotyczących ochrony danych Administrator wyznaczył **Punkt Kontaktowy** - jest nim Pani Joanna Mrowicka, Inspektor Ochrony Danych Osobowych: e-mail kontakt@smart-standards.com, tel. +48 602 241239.
3. **Cele i podstawy prawne.** Dane przetwarzamy w celu realizacji zadań własnych gminy oraz zadań zleconych z zakresu administracji rządowej, w szczególności prowadzenia postępowań administracyjnych i podatkowych, ewidencji ludności i dowodów osobistych, wymiaru i poboru podatków i opłat lokalnych, gospodarki odpadami komunalnymi, gospodarki nieruchomościami, planowania przestrzennego, ochrony środowiska, wydawania zezwoleń, rozpatrywania skarg, wniosków i petycji, obsługi Rady Gminy, organizacji wyborów i referendów oraz zarządzania kryzysowego - na podstawie **art. 6 ust. 1 lit. c RODO** (obowiązek prawny) oraz **art. 6 ust. 1 lit. e RODO** (zadanie realizowane w interesie publicznym) w związku z ustawą z dnia 8 marca 1990 r. o samorządzie gminnym, Kodeksem postępowania administracyjnego, Ordynacją podatkową oraz przepisami szczególnymi regulującymi daną sprawę. W zakresie danych szczególnych kategorii podstawę stanowi art. 9 ust. 2 lit. b, g lub h RODO, a w zakresie danych dotyczących wyroków skazujących i czynów zabronionych - art. 10 RODO w związku z przepisami szczególnymi. Jeżeli przetwarzanie opiera się na zgodzie (np. podanie numeru telefonu lub adresu e-mail w celu ułatwienia kontaktu) – podstawą jest **art. 6 ust. 1 lit. a RODO**, a zgodę można wycofać w każdej chwili bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.
4. **Odbiorcy danych.** Odbiorcami mogą być: organy administracji publicznej, sądy i inne podmioty uprawnione na podstawie przepisów prawa, organy odwoławcze (w szczególności samorządowe kolegium odwoławcze i wojewoda), podmioty przetwarzające dane na zlecenie Administratora na podstawie umów powierzenia (w szczególności dostawcy systemów dziedzinowych i elektronicznego obiegu dokumentów, obsługa prawna), operatorzy pocztowi, a w zakresie informacji podlegających publikacji (w szczególności obwieszczeń, transmisji obrad Rady Gminy i oświadczeń majątkowych) - nieograniczony krąg odbiorców.
5. **Okres przechowywania.** Dane przechowujemy przez okres wynikający z przepisów prawa oraz z jednolitego rzeczowego wykazu akt obowiązującego w Jednostce, właściwego dla danej kategorii sprawy.
6. **Prawa.** Przysługuje Pani/Panu prawo dostępu do danych i otrzymania ich kopii, sprostowania, ograniczenia przetwarzania, a w przypadkach przewidzianych przepisami - usunięcia danych oraz wniesienia sprzeciwu wobec przetwarzania opartego na art. 6 ust. 1 lit. e lub f RODO. Prawo do usunięcia danych nie przysługuje w zakresie, w jakim przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego albo wykonania zadania realizowanego w interesie publicznym.
7. Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, **ul. Moniuszki 1A, 00-014 Warszawa**.
8. **Wymóg podania danych.** Podanie danych jest wymogiem ustawowym, gdy przetwarzanie służy wypełnieniu obowiązku prawnego - niepodanie danych uniemożliwia załatwienie sprawy. W pozostałym zakresie podanie danych jest dobrowolne.
9. **Zautomatyzowane podejmowanie decyzji, profilowanie oraz przekazywanie danych poza Europejski Obszar Gospodarczy.** Administrator nie podejmuje wobec Pani/Pana decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, które wywoływałyby wobec Pani/Pana skutki prawne lub w podobny sposób istotnie na Panią/Pana wpływały. Natomiast w związku z korzystaniem przez Administratora z usług dostawców systemów teleinformatycznych, usług chmurowych, komunikacyjnych lub serwisowych dane osobowe mogą być, w zakresie niezbędnym do świadczenia tych usług, przekazywane lub udostępniane odbiorcom mającym siedzibę poza Europejskim Obszarem Gospodarczym. Przekazywanie danych do państw trzecich odbywa się wyłącznie zgodnie z rozdziałem V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych, zgodnie z art. 45 RODO, albo przy zastosowaniu odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, w szczególności standardowych klauzul umownych oraz - gdy jest to wymagane - dodatkowych środków ochrony. Administrator dokonuje oceny podstawy i warunków przekazywania danych poza EOG oraz stosowanych zabezpieczeń z uwzględnieniem wymagań RODO, stanowisk Prezesa UODO oraz wytycznych Europejskiej Rady Ochrony Danych. Informację o państwie trzecim, podstawie prawnej przekazania danych oraz stosowanych zabezpieczeniach, a także o sposobie uzyskania ich kopii lub informacji o miejscu ich udostępnienia można uzyskać, kontaktując się z Administratorem lub Inspektorem Ochrony Danych.

KLAUZULA INFORMACYJNA NR 2

przetwarzanie danych osobowych kandydatów do pracy

Zgodnie z art. 13 ust. 1 i 2 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest **Urząd Gminy Chrzypsko Wielkie** [w skrócie: UG], ul. Główna 156, 64-412 Chrzypsko Wielkie, reprezentowany przez Wójta Gminy. Z Administratorem można się kontaktować:
   - na adres jego siedziby lub pod numerem tel. +48 61 295 10 11,
   - na adres **e-mail:** urzad@chrzypsko.pl
   - poprzez e-Doręczenia: AE:PL-64773-21728-SBJJD-24
2. W sprawach dotyczących ochrony danych Administrator wyznaczył **Punkt Kontaktowy** - jest nim Pani Joanna Mrowicka, Inspektor Ochrony Danych Osobowych: e-mail kontakt@smart-standards.com, tel. +48 602 241239.
3. **Cel i podstawy prawne.** Dane przetwarzamy w celu przeprowadzenia naboru na wolne stanowisko, na podstawie: **art. 6 ust. 1 lit. c RODO** w związku z art. 22^1 Kodeksu pracy oraz ustawą z dnia 21 listopada 2008 r. o pracownikach samorządowych - w zakresie danych wskazanych w przepisach; **art. 6 ust. 1 lit. b RODO** - w zakresie działań przed zawarciem umowy; **art. 6 ust. 1 lit. a RODO** (zgoda) - w odniesieniu do danych podanych z własnej inicjatywy, wykraczających poza zakres wymagany przepisami, w tym wizerunku; **art. 9 ust. 2 lit. b RODO** - w zakresie danych o niepełnosprawności, jeżeli kandydat zamierza skorzystać z uprawnień z tym związanych.
4. **Dane nadmiarowe.** Dokumenty aplikacyjne zawierające dane wykraczające poza zakres wymagany przepisami i niepoparte zgodą **nie będą brane pod uwagę**. Prosimy o niezamieszczanie w dokumentach danych szczególnych kategorii.
5. **Odbiorcy danych.** Odbiorcami mogą być podmioty przetwarzające dane na zlecenie Administratora oraz - w zakresie wynikającym z ustawy o pracownikach samorządowych - odbiorcy informacji o wyniku naboru publikowanej w Biuletynie Informacji Publicznej i na tablicy ogłoszeń, obejmującej imię i nazwisko oraz miejscowość zamieszkania osoby wybranej.
6. **Okres przechowywania.** Dokumenty aplikacyjne kandydatów niewybranych przechowujemy przez okres **3 miesięcy** od zakończenia naboru, a w zakresie dokumentacji naboru wymaganej przepisami - przez okres wynikający z jednolitego rzeczowego wykazu akt. Po tym terminie dokumenty są niszczone albo - na wniosek złożony przed upływem terminu - zwracane.
7. **Prawa.** Przysługuje Pani/Panu prawo dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, a w zakresie danych przetwarzanych na podstawie zgody - prawo do jej wycofania w każdej chwili oraz prawo do przenoszenia danych.
8. Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, **ul. Moniuszki 1A, 00-014 Warszawa**.
9. **Wymóg podania danych.** Podanie danych w zakresie wynikającym z przepisów jest warunkiem udziału w naborze; podanie pozostałych danych jest dobrowolne.
10. **Zautomatyzowane podejmowanie decyzji, profilowanie oraz przekazywanie danych poza Europejski Obszar Gospodarczy.** Administrator nie podejmuje wobec Pani/Pana decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, które wywoływałyby wobec Pani/Pana skutki prawne lub w podobny sposób istotnie na Panią/Pana wpływały. Natomiast w związku z korzystaniem przez Administratora z usług dostawców systemów teleinformatycznych, usług chmurowych, komunikacyjnych lub serwisowych dane osobowe mogą być, w zakresie niezbędnym do świadczenia tych usług, przekazywane lub udostępniane odbiorcom mającym siedzibę poza Europejskim Obszarem Gospodarczym. Przekazywanie danych do państw trzecich odbywa się wyłącznie zgodnie z rozdziałem V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych, zgodnie z art. 45 RODO, albo przy zastosowaniu odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, w szczególności standardowych klauzul umownych przyjętych przez Komisję Europejską oraz - gdy jest to wymagane - dodatkowych środków ochrony wynikających z oceny warunków danego transferu. Administrator dokonuje oceny podstawy i warunków przekazywania danych poza EOG oraz stosowanych zabezpieczeń z uwzględnieniem wymagań RODO, stanowisk Prezesa Urzędu Ochrony Danych Osobowych oraz wytycznych Europejskiej Rady Ochrony Danych. Informację o państwie trzecim, podstawie prawnej przekazania danych oraz stosowanych zabezpieczeniach, a także o sposobie uzyskania ich kopii lub informacji o miejscu ich udostępnienia można uzyskać, kontaktując się z Administratorem lub Inspektorem Ochrony Danych.

KLAUZULA INFORMACYJNA NR 3

przetwarzanie danych osobowych pracowników i osób świadczących pracę

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest **Urząd Gminy Chrzypsko Wielkie** [w skrócie: UG], ul. Główna 156, 64-412 Chrzypsko Wielkie, reprezentowany przez Wójta Gminy. Z Administratorem można się kontaktować:
   - na adres jego siedziby lub pod numerem tel. +48 61 295 10 11,
   - na adres **e-mail:** urzad@chrzypsko.pl
   - poprzez e-Doręczenia: AE:PL-64773-21728-SBJJD-24
2. W sprawach dotyczących ochrony danych Administrator wyznaczył **Punkt Kontaktowy** - jest nim Pani Joanna Mrowicka, Inspektor Ochrony Danych Osobowych: e-mail kontakt@smart-standards.com, tel. +48 602 241239.
3. **Cele i podstawy prawne.** Dane przetwarzamy w celu: nawiązania, przebiegu i rozwiązania stosunku pracy lub innego stosunku prawnego - **art. 6 ust. 1 lit. b i c RODO** w związku z Kodeksem pracy, ustawą o pracownikach samorządowych i przepisami wykonawczymi; realizacji obowiązków płatnika składek i zaliczek - **art. 6 ust. 1 lit. c RODO** w związku z przepisami o ubezpieczeniach społecznych i podatku dochodowym; zapewnienia bezpieczeństwa i higieny pracy oraz medycyny pracy - **art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. b RODO**; prowadzenia zakładowego funduszu świadczeń socjalnych - **art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. b RODO**; ustalenia, dochodzenia lub obrony roszczeń - **art. 6 ust. 1 lit. f RODO**; w zakresie danych podawanych dobrowolnie (np. prywatny numer telefonu, wizerunek) - **art. 6 ust. 1 lit. a RODO**.
4. **Źródło danych.** Dane pozyskujemy bezpośrednio od Pani/Pana, a w przypadku danych członków rodziny zgłaszanych do ubezpieczenia lub do świadczeń socjalnych - od pracownika, który je podaje.
5. **Odbiorcy danych.** Odbiorcami mogą być: Zakład Ubezpieczeń Społecznych, urząd skarbowy, Państwowa Inspekcja Pracy, instytucje finansowe obsługujące wypłaty i pracownicze plany kapitałowe, podmiot medycyny pracy, podmioty przetwarzające dane na zlecenie Administratora, a w zakresie danych podlegających udostępnieniu - podmioty uprawnione na podstawie przepisów.
6. **Okres przechowywania.** Dokumentację pracowniczą przechowujemy przez okres **10 lat** od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł, a w przypadku zatrudnienia sprzed 1 stycznia 2019 r. - przez **50 lat**, chyba że przepisy szczególne stanowią inaczej. Dokumentację podatkową i ubezpieczeniową przechowujemy przez okresy wynikające z przepisów prawa.
7. **Prawa.** Przysługuje Pani/Panu prawo dostępu do danych i otrzymania ich kopii, sprostowania, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania opartego na art. 6 ust. 1 lit. f RODO, a w zakresie danych przetwarzanych na podstawie zgody - prawo do jej wycofania. Prawo do usunięcia danych jest ograniczone w zakresie, w jakim przetwarzanie wynika z obowiązku prawnego.
8. Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, **ul. Moniuszki 1A, 00-014 Warszawa**.
9. **Wymóg podania danych.** Podanie danych wskazanych w przepisach prawa pracy jest obowiązkowe; podanie pozostałych danych jest dobrowolne i nie wpływa na sytuację pracownika.
10. **Zautomatyzowane podejmowanie decyzji, profilowanie oraz przekazywanie danych poza Europejski Obszar Gospodarczy.** Administrator nie podejmuje wobec Pani/Pana decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, które wywoływałyby wobec Pani/Pana skutki prawne lub w podobny sposób istotnie na Panią/Pana wpływały. Natomiast w związku z korzystaniem przez Administratora z usług dostawców systemów teleinformatycznych, usług chmurowych, komunikacyjnych lub serwisowych dane osobowe mogą być, w zakresie niezbędnym do świadczenia tych usług, przekazywane lub udostępniane odbiorcom mającym siedzibę poza Europejskim Obszarem Gospodarczym. Przekazywanie danych do państw trzecich odbywa się wyłącznie zgodnie z rozdziałem V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych, zgodnie z art. 45 RODO, albo przy zastosowaniu odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, w szczególności standardowych klauzul umownych przyjętych przez Komisję Europejską oraz - gdy jest to wymagane - dodatkowych środków ochrony wynikających z oceny warunków danego transferu. Administrator dokonuje oceny podstawy i warunków przekazywania danych poza EOG oraz stosowanych zabezpieczeń z uwzględnieniem wymagań RODO, stanowisk Prezesa Urzędu Ochrony Danych Osobowych oraz wytycznych Europejskiej Rady Ochrony Danych. Informację o państwie trzecim, podstawie prawnej przekazania danych oraz stosowanych zabezpieczeniach, a także o sposobie uzyskania ich kopii lub informacji o miejscu ich udostępnienia można uzyskać, kontaktując się z Administratorem lub Inspektorem Ochrony Danych.

KLAUZULA INFORMACYJNA NR 4

przetwarzanie danych w związku z zawieraniem i realizacją umów oraz udostępnianiem informacji w Centralnym Rejestrze Umów i przesyłaniem faktur w KSeF

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest **Wójt Gminy Chrzypsko Wielkie**, z siedzibą w Urzędzie Gminy Chrzypsko Wielkie, ul. Główna 156, 64-412 Chrzypsko Wielkie. Z Administratorem można się kontaktować:
   - na adres jego siedziby lub pod numerem tel. +48 61 295 10 11,
   - na adres **e-mail:** urzad@chrzypsko.pl
   - poprzez e-Doręczenia: AE:PL-64773-21728-SBJJD-24
2. W sprawach dotyczących ochrony danych Administrator wyznaczył **Punkt Kontaktowy** - jest nim Pani Joanna Mrowicka, Inspektor Ochrony Danych Osobowych: e-mail kontakt@smart-standards.com, tel. +48 602 241239.
3. **Zakres i źródło danych.** Przetwarzamy dane niezbędne do zawarcia i wykonania umowy: imię i nazwisko, firmę, adres, NIP, REGON, PESEL (gdy wymagają tego przepisy), dane kontaktowe, numer rachunku bankowego, dane o przedmiocie, wartości i okresie obowiązywania umowy oraz dane niezbędne do rozliczeń podatkowych i ubezpieczeniowych. Dane pozyskujemy od Pani/Pana, a w przypadku osób reprezentujących kontrahenta lub wskazanych do kontaktu - od kontrahenta oraz z rejestrów publicznych (CEIDG, KRS).
4. **Cele i podstawy prawne.** Zawarcie i wykonanie umowy - **art. 6 ust. 1 lit. b RODO**, a wobec osób reprezentujących kontrahenta - **art. 6 ust. 1 lit. f RODO**; udostępnienie informacji o umowie w Centralnym Rejestrze Umów JSFP - **art. 6 ust. 1 lit. c RODO** w związku z art. 34a ustawy o finansach publicznych; wystawianie, przesyłanie i odbieranie faktur w Krajowym Systemie e-Faktur - **art. 6 ust. 1 lit. c RODO** w związku z art. 106nb–106nh ustawy o podatku od towarów i usług; prowadzenie ksiąg rachunkowych i rozliczenia podatkowe - **art. 6 ust. 1 lit. c RODO**; zgłoszenia i rozliczenia z ZUS oraz obowiązki płatnika (umowy zlecenia i o dzieło) - **art. 6 ust. 1 lit. c RODO**; realizacja zadań publicznych i archiwizacja - **art. 6 ust. 1 lit. e RODO**; dochodzenie lub obrona roszczeń - **art. 6 ust. 1 lit. f RODO**.

   Udostępnienie informacji o umowie w Centralnym Rejestrze Umów

   Informacje o umowach są - na podstawie art. 34a ustawy o finansach publicznych - **udostępniane publicznie** w prowadzonym przez organ administracji rządowej systemie Centralnego Rejestru Umów JSFP, dostępnym dla **nieograniczonego kręgu odbiorców** za pośrednictwem internetu. Publikacji podlegają w szczególności: numer umowy, data zawarcia, okres obowiązywania, **oznaczenie stron (w przypadku osoby fizycznej - imię i nazwisko)**, przedmiot, wartość, informacja o finansowaniu ze środków publicznych, status umowy i dane o jej zmianach. W rejestrze **nie zamieszcza się** numeru PESEL, daty urodzenia ani adresu zamieszkania. Administrator stosuje minimalizację danych oraz ograniczenia jawności przewidziane przepisami.
5. **Krajowy System e-Faktur.** Dane zawarte w fakturze przekazywane są do KSeF i przechowywane w tym systemie przez okres wynikający z przepisów o podatku od towarów i usług (co do zasady 10 lat od końca roku wystawienia faktury). W zakresie danych zgromadzonych w KSeF **odrębnym administratorem jest organ prowadzący ten system.**
6. **Odbiorcy danych.** Organy prowadzące CRU JSFP i KSeF; nieograniczony krąg odbiorców - w zakresie informacji publikowanych w CRU oraz udostępnianych w trybie dostępu do informacji publicznej i przepisów o zamówieniach publicznych; Zakład Ubezpieczeń Społecznych, urzędy skarbowe, organy kontroli i sądy; banki i operatorzy pocztowi; podmioty przetwarzające dane na zlecenie Administratora.
7. **Okres przechowywania.** Przez okres obowiązywania i rozliczenia umowy; przez okres wymagany przepisami o rachunkowości i prawa podatkowego (co do zasady 5 lat od końca roku, w którym upłynął termin płatności podatku); w zakresie faktur w KSeF i informacji w CRU - przez okresy wynikające z przepisów regulujących te systemy; przez okres wynikający z jednolitego rzeczowego wykazu akt; w zakresie roszczeń - do upływu terminu przedawnienia.
8. **Prawa.** Przysługuje Pani/Panu prawo dostępu do danych i otrzymania ich kopii, sprostowania, ograniczenia przetwarzania, a w zakresie danych przetwarzanych na podstawie umowy - prawo do przenoszenia danych. **Prawo do usunięcia danych nie przysługuje** w zakresie, w jakim przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego lub wykonania zadania w interesie publicznym - dotyczy to w szczególności danych publikowanych w CRU i przekazanych do KSeF. Wobec przetwarzania opartego na art. 6 ust. 1 lit. e lub f RODO przysługuje prawo sprzeciwu.
9. Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, **ul. Moniuszki 1A, 00-014 Warszawa**.

10. **Wymóg podania danych.** Podanie danych niezbędnych do zawarcia i wykonania umowy jest warunkiem jej zawarcia. Podanie danych podlegających udostępnieniu w CRU, przekazaniu do KSeF oraz niezbędnych do rozliczeń jest obowiązkiem ustawowym.
11. **Zautomatyzowane podejmowanie decyzji, profilowanie oraz przekazywanie danych poza Europejski Obszar Gospodarczy.** Administrator nie podejmuje wobec Pani/Pana decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, które wywoływałyby wobec Pani/Pana skutki prawne lub w podobny sposób istotnie na Panią/Pana wpływały. Natomiast w związku z korzystaniem przez Administratora z usług dostawców systemów teleinformatycznych, usług chmurowych, komunikacyjnych lub serwisowych dane osobowe mogą być, w zakresie niezbędnym do świadczenia tych usług, przekazywane lub udostępniane odbiorcom mającym siedzibę poza Europejskim Obszarem Gospodarczym. Przekazywanie danych do państw trzecich odbywa się wyłącznie zgodnie z rozdziałem V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych, zgodnie z art. 45 RODO, albo przy zastosowaniu odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, w szczególności standardowych klauzul umownych przyjętych przez Komisję Europejską oraz - gdy jest to wymagane - dodatkowych środków ochrony wynikających z oceny warunków danego transferu. Administrator dokonuje oceny podstawy i warunków przekazywania danych poza EOG oraz stosowanych zabezpieczeń z uwzględnieniem wymagań RODO, stanowisk Prezesa Urzędu Ochrony Danych Osobowych oraz wytycznych Europejskiej Rady Ochrony Danych. Informację o państwie trzecim, podstawie prawnej przekazania danych oraz stosowanych zabezpieczeniach, a także o sposobie uzyskania ich kopii lub informacji o miejscu ich udostępnienia można uzyskać, kontaktując się z Administratorem lub Inspektorem Ochrony Danych.

KLAUZULA INFORMACYJNA NR 5

przetwarzanie danych w związku z dochodzeniem należności i regulowaniem zobowiązań

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest **Wójt Gminy Chrzypsko Wielkie**, z siedzibą w Urzędzie Gminy Chrzypsko Wielkie, ul. Główna 156, 64-412 Chrzypsko Wielkie. Z Administratorem można się kontaktować:
   - na adres jego siedziby lub pod numerem tel. +48 61 295 10 11,
   - na adres **e-mail:** urzad@chrzypsko.pl
   - poprzez e-Doręczenia: AE:PL-64773-21728-SBJJD-24
2. W sprawach dotyczących ochrony danych Administrator wyznaczył **Punkt Kontaktowy** - jest nim Pani Joanna Mrowicka, Inspektor Ochrony Danych Osobowych: e-mail kontakt@smart-standards.com, tel. +48 602 241239.
3. **Cele i podstawy prawne.** Dane przetwarzamy w celu: ustalenia stanu rozliczeń, wystawiania wezwań do zapłaty, naliczania odsetek i kosztów - **art. 6 ust. 1 lit. c RODO** w związku z przepisami o finansach publicznych i o rachunkowości oraz **art. 6 ust. 1 lit. e RODO**; dochodzenia należności w postępowaniu polubownym, sądowym, klauzulowym i egzekucyjnym oraz obrony przed roszczeniami - **art. 6 ust. 1 lit. f RODO** (prawnie uzasadniony interes polegający na ochronie praw majątkowych) oraz **art. 6 ust. 1 lit. c RODO** w związku z przepisami o postępowaniu egzekucyjnym w administracji; zawierania ugód, układów ratalnych, odraczania i umarzania należności - **art. 6 ust. 1 lit. c i e RODO**; regulowania zobowiązań Jednostki wobec kontrahentów - **art. 6 ust. 1 lit. b i c RODO**.
4. **Źródło danych.** Dane pozyskujemy od Pani/Pana, z dokumentów źródłowych (umowy, faktury, decyzje), a także - w zakresie niezbędnym do dochodzenia należności - z rejestrów publicznych i od organów, w tym z ewidencji ludności, CEIDG, KRS oraz od organów egzekucyjnych.
5. **Odbiorcy danych.** Odbiorcami mogą być: sądy, komornicy sądowi i organy egzekucji administracyjnej, kancelarie prawne obsługujące Jednostkę, banki, operatorzy pocztowi, podmioty przetwarzające dane na zlecenie Administratora, a w przypadkach przewidzianych przepisami - biura informacji gospodarczej.
6. **Okres przechowywania.** Do czasu zaspokojenia, wygaśnięcia albo przedawnienia należności, a następnie przez okres wynikający z przepisów o rachunkowości i prawa podatkowego oraz z jednolitego rzeczowego wykazu akt. W przypadku prowadzenia postępowania - do jego prawomocnego zakończenia i upływu terminów przechowywania dokumentacji.
7. **Prawa.** Przysługuje Pani/Panu prawo dostępu do danych i otrzymania ich kopii, sprostowania, ograniczenia przetwarzania oraz **prawo wniesienia sprzeciwu** wobec przetwarzania opartego na art. 6 ust. 1 lit. e lub f RODO - z przyczyn związanych ze szczególną sytuacją. Prawo do usunięcia danych jest ograniczone w zakresie, w jakim przetwarzanie wynika z obowiązku prawnego albo jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.
8. Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, **ul. Moniuszki 1A, 00-014 Warszawa**.
9. **Wymóg podania danych.** Podanie danych wynika z przepisów prawa albo z łączącego strony stosunku prawnego; ich niepodanie nie wstrzymuje dochodzenia należności.
10. **Zautomatyzowane podejmowanie decyzji, profilowanie oraz przekazywanie danych poza Europejski Obszar Gospodarczy.** Administrator nie podejmuje wobec Pani/Pana decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, które wywoływałyby wobec Pani/Pana skutki prawne lub w podobny sposób istotnie na Panią/Pana wpływały. Natomiast w związku z korzystaniem przez Administratora z usług dostawców systemów teleinformatycznych, usług chmurowych, komunikacyjnych lub serwisowych dane osobowe mogą być, w zakresie niezbędnym do świadczenia tych usług, przekazywane lub udostępniane odbiorcom mającym siedzibę poza Europejskim Obszarem Gospodarczym. Przekazywanie danych do państw trzecich odbywa się wyłącznie zgodnie z rozdziałem V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych, zgodnie z art. 45 RODO, albo przy zastosowaniu odpowiednich zabezpieczeń, o których mowa w art. 46 RODO, w szczególności standardowych klauzul umownych przyjętych przez Komisję Europejską oraz - gdy jest to wymagane - dodatkowych środków ochrony wynikających z oceny warunków danego transferu. Administrator dokonuje oceny podstawy i warunków przekazywania danych poza EOG oraz stosowanych zabezpieczeń z uwzględnieniem wymagań RODO, stanowisk Prezesa Urzędu Ochrony Danych Osobowych oraz wytycznych Europejskiej Rady Ochrony Danych. Informację o państwie trzecim, podstawie prawnej przekazania danych oraz stosowanych zabezpieczeniach, a także o sposobie uzyskania ich kopii lub informacji o miejscu ich udostępnienia można uzyskać, kontaktując się z Administratorem lub Inspektorem Ochrony Danych.

ZGODA PRACOWNIKA NA PRZETWARZANIE DODATKOWYCH DANYCH OSOBOWYCH, W TYM WIZERUNKU, ORAZ ZEZWOLENIE NA ROZPOWSZECHNIANIE WIZERUNKU

Administrator/Pracodawca:
Urząd Gminy Chrzypsko Wielkie [w skrócie: UG]
ul. Główna 156, 64-412 Chrzypsko Wielkie, reprezentowany przez Wójta Gminy

Imię i nazwisko pracownika:

.....

Stanowisko:.....

I. Dobrowolność zgody
Oświadczam, że zostałem/am poinformowany/a, iż udzielenie poniższych zgód jest **dobrowolne** i nie stanowi warunku zatrudnienia ani wykonywania przeze mnie obowiązków pracowniczych.
Przyjmuję do wiadomości, że odmowa udzielenia którejkolwiek ze zgód albo jej późniejsze wycofanie nie może stanowić podstawy niekorzystnego traktowania mnie ani powodować jakichkolwiek negatywnych konsekwencji w zakresie zatrudnienia.

II. Zgoda na przetwarzanie wizerunku
Wyrażam zgodę na przetwarzanie przez Administratora mojego wizerunku utrwalonego w postaci fotografii lub materiału audiowizualnego, w tym na jego utrwalanie, zapisywanie, przechowywanie i wykorzystywanie w niżej wskazanych celach.
Wyrażam zgodę na wykorzystanie mojego wizerunku:
☐ **TAK** ☐ **NIE**
w materiałach informacyjnych dotyczących działalności Administratora, w tym relacjach z wydarzeń, uroczystości, szkoleń, konferencji i innych przedsięwzięć organizowanych przez Administratora;
☐ **TAK** ☐ **NIE**
na stronie internetowej Administratora;
☐ **TAK** ☐ **NIE**
w Biuletynie Informacji Publicznej – jeżeli charakter publikowanego materiału uzasadnia zamieszczenie wizerunku;
☐ **TAK** ☐ **NIE**
w oficjalnych profilach Administratora prowadzonych w serwisach społecznościowych;
☐ **TAK** ☐ **NIE**
w materiałach promocyjnych, edukacyjnych i informacyjnych Administratora publikowanych w formie papierowej;
☐ **TAK** ☐ **NIE**
w elektronicznych materiałach promocyjnych, prezentacjach, publikacjach oraz materiałach szkoleniowych Administratora;
☐ **TAK** ☐ **NIE**
w komunikacji wewnętrznej Administratora, w tym w intranecie, wewnętrznych materiałach informacyjnych i dokumentacji fotograficznej wydarzeń pracowniczych.

III. Zezwolenie na rozpowszechnianie wizerunku
W zakresie odpowiadającym zaznaczonym przeze mnie powyżej celom zezwalam Administratorowi na rozpowszechnianie mojego wizerunku na podstawie art. 81 ustawy o prawie autorskim i prawach pokrewnych.
Zezwolenie obejmuje wyłącznie sposoby wykorzystania wizerunku wynikające z zakresu udzielonych przeze mnie zgód i nie może być interpretowane jako zgoda na wykorzystanie wizerunku w dowolnym, nieokreślonym celu.
Wizerunek nie może być wykorzystywany w sposób naruszający moją godność, dobre imię, prywatność ani inne dobra osobiste.

IV. Inne dodatkowe dane osobowe
Wyrażam zgodę na przetwarzanie następujących dodatkowych danych osobowych przekazanych przeze mnie dobrowolnie Administratorowi:
.....

w celu: .....
☐ **TAK** ☐ **NIE**
Niniejsza zgoda nie obejmuje danych, których przetwarzanie przez Administratora jest niezbędne z mocy prawa, dla wykonania umowy o pracę, wykonania obowiązków pracodawcy albo realizacji innych prawnie uzasadnionych celów posiadających odrębną podstawę prawną.

V. Wycofanie zgody
Zostałem/am poinformowany/a, że każdą z powyższych zgód mogę wycofać **w dowolnym momencie i niezależnie od pozostałych zgód**, bez konieczności podawania przyczyny.
Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego na jej podstawie przed wycofaniem.
Oświadczenie o wycofaniu zgody może zostać złożone w formie pisemnej Administratorowi lub drogą elektroniczną na adres jednostki lub Inspektorowi Ochrony Danych na adres: kontakt@smart-standards.com
Wycofanie zgody nie może powodować wobec pracownika żadnych negatywnych konsekwencji w zakresie zatrudnienia.

VI. Oświadczenie pracownika
Oświadczam, że treść niniejszego dokumentu jest dla mnie zrozumiała, otrzymałem/am informacje o dobrowolności udzielanych zgód oraz możliwości ich wycofania i miałem/am możliwość dokonania odrębnego wyboru w odniesieniu do każdego ze wskazanych sposobów przetwarzania mojego wizerunku.

.....
miejscowość i data

.....
czytelny podpis pracownika

INFORMACJA O STOSOWANIU MONITORINGU WIZYJNEGO
ORAZ POTWIERDZENIE JEJ OTRZYMANIA PRZEZ PRACOWNIKA
w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Administrator/Pracodawca:
Urząd Gminy Chrzypsko Wielkie [w skrócie: UG]
ul. Główna 156, 64-412 Chrzypsko Wielkie, reprezentowany przez Wójta Gminy
..

Imię i nazwisko pracownika:

.....

Stanowisko: .....

1. Informacja o stosowaniu monitoringu
Informuję, że na terenie: .....

.....

stosowany jest monitoring wizyjny polegający na szczególnym nadzorze przy wykorzystaniu środków technicznych umożliwiających **rejestrację obrazu**.
Monitoring wizyjny nie obejmuje rejestracji dźwięku.

2. Cel stosowania monitoringu
Monitoring stosowany jest wyłącznie w zakresie niezbędnym do realizacji następujących celów:
☐ zapewnienia bezpieczeństwa pracowników;
☐ ochrony mienia;
☐ kontroli produkcji;
☐ zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

3. Zakres monitoringu
Monitoringiem objęte są pomieszczenia jednostki z wyłączeniem toalet, miejsc socjalnych i siedzib zakładowych organizacji związkowych oraz teren wokół siedziby jednostki.
Rozmieszczenie urządzeń monitorujących powinno odpowiadać zasadzie niezbędności i minimalizacji danych oraz pozostawać adekwatne do celu, dla którego monitoring został wprowadzony.
Monitoring nie może prowadzić do nieuzasadnionej ingerencji w prywatność, godność ani inne dobra osobiste pracowników.

4. Sposób oznaczenia obszaru
Pomieszczenia oraz teren objęte monitoringiem są oznaczone w sposób widoczny i czytelny odpowiednimi znakami informującymi o stosowaniu monitoringu wizyjnego.

5. Okres przechowywania nagrań
Nagrania obrazu pochodzące z monitoringu przechowywane są przez okres do 90 dni, nie dłużej jednak - co do zasady - niż przez **3 miesiące od dnia nagrania**.
Jeżeli nagranie stanowi dowód w postępowaniu prowadzonym na podstawie przepisów prawa albo Administrator powziął wiadomość, że może ono stanowić dowód w takim postępowaniu, okres przechowywania może zostać przedłużony do czasu prawomocnego zakończenia postępowania.
Po upływie właściwego okresu nagrania zawierające dane osobowe podlegają usunięciu lub trwałemu zniszczeniu, chyba że obowiązek ich dalszego przechowywania wynika z przepisów prawa.

6. Dostęp do nagrań
Dostęp do nagrań z monitoringu posiadają wyłącznie osoby upoważnione przez Administratora oraz inne podmioty lub organy uprawnione do uzyskania dostępu na podstawie przepisów prawa.
Nagrania nie mogą być wykorzystywane do celów innych niż cele, dla których monitoring został wprowadzony, chyba że obowiązek lub uprawnienie do ich dalszego wykorzystania wynika z przepisów prawa.

7. Zasady ochrony danych osobowych
Wizerunek pracownika utrwalony za pomocą monitoringu stanowi daną osobową.
Administrator realizuje obowiązek informacyjny wynikający z przepisów RODO zgodnie z właściwą klauzulą informacyjną dotyczącą monitoringu wizyjnego, określającą w szczególności:

- tożsamość i dane kontaktowe Administratora,
- dane kontaktowe Inspektora Ochrony Danych, jeżeli został wyznaczony,
- cel i podstawę prawną przetwarzania,
- odbiorców lub kategorie odbiorców danych,
- okres przechowywania nagrań,
- prawa osoby, której dane dotyczą,
- prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

8. Potwierdzenie pracownika
Oświadczam, że przed dopuszczeniem mnie do pracy zostałem/am poinformowany/a o:

1. stosowaniu przez Pracodawcę monitoringu wizyjnego;
2. celu jego stosowania;
3. zakresie obszaru objętego monitoringiem;
4. sposobie stosowania monitoringu;
5. zasadach przechowywania i wykorzystywania nagrań;
6. zasadach przetwarzania danych osobowych utrwalonych za pomocą monitoringu.

Potwierdzam otrzymanie powyższej informacji.

Niniejsze oświadczenie nie stanowi zgody na stosowanie monitoringu ani zgody na przetwarzanie danych osobowych w ramach monitoringu. Podpis pracownika potwierdza wyłącznie otrzymanie informacji wymaganych przepisami prawa.

.....
miejscowość i data

.....
czytelny podpis pracownika

Wójt
mgr inż. Edmund Ziółek

ZGŁOSZENIE

naruszenia ochrony danych osobowych / incydentu bezpieczeństwa
w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Zgłaszający (imię, nazwisko, stanowisko)	
Data i godzina zgłoszenia	
Data i godzina stwierdzenia zdarzenia	
Miejsce / system, którego dotyczy	
Opis zdarzenia (co się stało, w jakich okolicznościach)	
Kategorie danych, których dotyczy zdarzenie	
Przybliżona liczba osób i wpisów danych	
Działania podjęte natychmiast przez zgłaszającego	

Wypełnia Inspektor Ochrony Danych

Czy zdarzenie stanowi naruszenie ochrony danych? (TAK / NIE - uzasadnienie)	
Czy zdarzenie stanowi incydent bezpieczeństwa? (TAK / NIE)	
Ocena ryzyka naruszenia praw lub wolności (brak / niskie / wysokie)	
Zgłoszenie do PUODO (TAK / NIE - data, uzasadnienie)	
Zawiadomienie osób (TAK / NIE - data, sposób)	
Zgłoszenie do CSIRT (TAK / NIE - data)	
Działania naprawcze i termin ich wykonania	
Numer wpisu w rejestrze	

podpis zgłaszającego

podpis IOD / Wójt

Wójt
mgr inż. Edmund Ziółek

REJESTR NARUSZEŃ OCHRONY DANYCH I INCYDENTÓW BEZPIECZEŃSTWA

w Urzędzie Gminy Chrzypsko Wielkie

ul. Główna 156, 64-412 Chrzypsko Wielkie

Lp.	Data stwierdzenia	Opis zdarzenia	Kategorie danych / liczba osób	Ocena ryzyka	Zgłoszenie PUODO / CSIRT	Zawiadomienie osób	Działania naprawcze	Zamknięcie

Rejestr prowadzi Inspektor Ochrony Danych we współpracy z Koordynatorem ds. cyberbezpieczeństwa. Wpisy przechowuje się przez 5 lat od zamknięcia sprawy. Raz w roku sporządza się analizę zbiorczą stanowiącą podstawę aktualizacji analizy ryzyka i planu szkoleń.

Wójt
mgr inż. Edmund Ziółek

WYKAZ SYSTEMÓW TELEINFORMATYCZNYCH

i inwentaryzacja zasobów **w Urzędzie Gminy Chrzypsko Wielkie**
ul. Główna 156, 64-412 Chrzypsko Wielkie

I. Systemy teleinformatyczne

Lp.	Nazwa systemu	Rodzaj (Jednostki / centralny)	Właściciel merytoryczny	Administrator techniczny	Kategorie danych	Podstawa prawna	Umowa powierzenia (TAK/NIE)	Kopie zapasowe

II. Sprzęt i oprogramowanie

Lp.	Rodzaj zasobu	Oznaczenie / nr inwentarzowy	Użytkownik / lokalizacja	Szyfrowanie	Licencja / wsparcie producenta do	Uwagi

Lp.	Rodzaj zasobu	Oznaczenie / nr inwentarzowy	Użytkownik / lokalizacja	Szyfrowanie	Licencja / wsparcie producenta do	Uwagi

III. Obszary przetwarzania (pomieszczenia)

Lp.	Pomieszczenie	Rodzaj przetwarzanych danych	Zabezpieczenia	Dysponenci kluczy

Wykaz prowadzi Administrator Systemów Informatycznych. Aktualizacja - niezwłocznie po każdej zmianie; przegląd całościowy - co najmniej raz w roku.

Wójt
mgr inż. Edmund Ziółek

WYKAZ UMÓW POWIERZENIA PRZETWARZANIA

oraz podmiotów przetwarzających i ich podwykonawców
w Urzędzie Gminy Chrzypsko Wielkie
ul. Główna 156, 64-412 Chrzypsko Wielkie

Lp.	Podmiot przetwarzający	Przedmiot powierzenia	Kategorie danych	Data i nr umowy	Okres obowiązywania	Podwykonawcy (zgoda: ogólna / szczegółowa)	Data ostatniej weryfikacji	Data kontroli

Zakres weryfikacji podmiotu przetwarzającego (§ 47 Polityki)

1. oświadczenie o stosowanych środkach technicznych i organizacyjnych;
2. informacja o wyznaczeniu Inspektora Ochrony Danych i jego dane kontaktowe;
3. lokalizacja przetwarzania danych, w tym informacja o przetwarzaniu poza Europejskim Obszarem Gospodarczym;
4. stosowanie szyfrowania, kopii zapasowych i uwierzytelniania wieloskładnikowego;
5. informacja o naruszeniach ochrony danych w okresie ostatnich 24 miesięcy;
6. posiadane certyfikaty lub sprawozdania z audytów - jeżeli podmiot je posiada;
7. wykaz podwykonawców, którym podmiot zamierza powierzyć czynności.

Wykaz prowadzi Inspektor Ochrony Danych. Weryfikację powtarza się przy przedłużeniu umowy oraz nie rzadziej niż raz na trzy lata; kontrolę podmiotów przetwarzających dane szczególnych kategorii lub dane na dużą skalę - nie rzadziej niż raz na dwa lata.

Wójt
mgr inż. Edmund Ziółek