Załącznik do zarządzenia nr 40/2020
Wójta Gminy Chrzypsko Wielkie
z dnia 04 maja 2020r.

GMINA CHRZYPSKO WIELKIE

Polityka bezpieczeństwa i ochrony danych osobowych

27 KWIETNIA 2020

Cel

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Podstawy prawne

1. rozporządzenie Parlamentu Europejskiego i Rady Europy (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 (RODO) (4.5.2016, L 119);
2. ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. 2019 poz. 730);
3. ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018 r., poz. 1000 z późn. zm.).

Przedmiot

Przedmiotem Polityki ochrony danych osobowych są zasady i tryb postępowania podczas przetwarzania danych osobowych w formie tradycyjnej i elektronicznej. Mając na względzie obowiązek stosowania odpowiednich zabezpieczeń przetwarzanych danych osobowych w odniesieniu do zakresu, kontekstu i celu, a także ryzyka naruszenia ochrony przetwarzanych danych, zgodnie z art. 32 RODO, wdraża się odpowiednie środki techniczne i organizacyjne.

Zakres stosowania

Polityka ochrony danych osobowych obowiązuje wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informacyjne, w których przetwarzane są dane osobowe. Politykę tę stosuje się we wszystkich lokalizacjach, w których przetwarzane są informacje podlegające ochronie, na wszystkich nośnikach informacji (tradycyjnych - papierowych, elektronicznych, optycznych, magnetycznych), które zawierają dane podlegające ochronie. Polityka obowiązuje wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, w tym stażystów i osób, z którymi podpisane są umowy cywilno-prawne wykonujących prace na rzecz Administratora oraz innych osób mających dostęp do danych.

ZATWIERDZAM I POLECAM STOSOWAĆ

Wójt
mgr inż. Edward Zięba

.....

WÓJT – Kierownik Jednostki

SPIS TREŚCI

DEFINICJE

Ilekroć w niniejszej Polityce jest mowa o:

1) Administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych, a w niniejszej Polityce **Wójta Gminy Chrzypsko Wielkie z siedzibą Urzędu Gminy w Chrzypsku Wielkim,** ul. Główna 15, 64-412 Chrzypsko Wielkie, zwanego „Administratorem";
2) Inspektor Ochrony Danych Osobowych (lub IODO) – rozumie się przez to osobę wyznaczoną przez Administratora, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami prawa;
3) Administratorze Systemów Informatycznych (lub ASI) – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane przepisami prawa;
4) Danych osobowych (lub danych) – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;
6) Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
7) Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska oraz stanowiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
8) RODO - Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO);
9) PUDO lub Urząd nadzoru – Prezes Urzędu Ochrony Danych Osobowych;
10) Zbiorze danych – rozumie się przez to dane zebrane w postaci zbioru lub według kategorii:
    a) danych osobowych podopiecznych/klientów UG Chrzypsko Wielkie z podzbiorami,
    b) danych pracowniczych z podzbiorami,
    c) danych administracyjnych z podzbiorami,
    d) danych doraźnych,

przy czym każdy zbiór danych to zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

§ 1.

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, co nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§ 2.

1. Administrator wyznacza i zgłasza do rejestru prowadzonego przez Urząd nadzoru Inspektora Ochrony Danych, który jest odpowiedzialny za przetwarzanie danych.
2. Administrator wyznacza Administratora Systemów Informatycznych
3. Administrator wyznacza osoby współdziałające z IODO w zakresie ochrony danych osobowych.

§ 3.

W przypadku niewyznaczenia IODO lub ASI za zapewnienie należytego przestrzegania zasad ochrony danych osobowych odpowiada Administrator.

§ 4.

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IODO z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez IODO odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 5.

Do przetwarzania danych osobowych w UG Chrzypsko Wielkie są dopuszczone wyłącznie osoby upoważnione przez Administratora.

§ 6.

1. Upoważnienia nadawane są indywidualnie, przed rozpoczęciem przez osobę upoważnianą przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy oraz osoby fizyczne współpracujące z Administratorem, które uzyskują dostęp do danych osobowych w związku ze świadczeniem na jego rzecz usług na podstawie umów cywilnoprawnych lub jako osoby fizyczne wykonujące obowiązki na podstawie jednoosobowej działalności (zatrudnieni).
3. Upoważnienie nadawane jest niezwłocznie po przyjęciu do pracy lub po zawarciu umowy cywilnoprawnej, w sytuacjach gdy zakres wykonywanych obowiązków wiąże się z potrzebą uzyskania dostępu do danych osobowych.
4. Upoważnienie nadawane jest na czas zatrudnienia na danym stanowisku pracy lub na czas realizacji zleconych czynności.
5. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora.
6. Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania w zakresie i czasie wskazanym w upoważnieniu.
7. Inspektor Ochrony Danych na podstawie wydanych upoważnień prowadzi ewidencję (rejestr) osób upoważnionych do przetwarzania danych.
8. Każda osoba upoważniana do przetwarzania danych osobowych składa pisemne oświadczenie o zachowaniu w tajemnicy przetwarzanych danych osobowych oraz znanych jej informacji o stosowanych wobec danych środkach bezpieczeństwa.
9. Zatrudnieni, którzy w ramach swoich obowiązków przebywają w strefach gdzie przetwarzane są dane osobowe ale do ich obowiązków nie należy przetwarzanie danych osobowych muszą uzyskać przeszkolenie w zakresie ochrony danych osobowych i złożyć stosowne oświadczenie o przestrzeganiu zasad ochrony danych oraz zachowaniu tajemnicy.

§ 7.

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w innym środkiem komunikacji elektronicznej.

§ 8.

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do osoby małoletniej – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14

RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator jest obowiązany spełnić obowiązek informacyjny, wobec osoby, której dane uzyskano bezpośrednio po utrwaleniu zebranych danych.
3. Powyższy obowiązek Administrator nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonywania zgodnie z treścią dokumentów oraz klauzul informacyjnych. Przykładowe klauzule informacyjne stanowią załączniki do niniejszej Polityki, co nie zwalnia pracowników operujących na danych osobowych od zgłaszania Inspektorowi Ochrony Danych Osobowych potrzeb w zakresie opracowania nowych klauzul.

§ 9
REALIZACJA PRAW PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ

1. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa dostępu przysługującego osobie, której dane dotyczą należy:
   a) wniosek należy przekazać do IODO,
   b) IODO przygotowuje projekt odpowiedzi na wniosek,
   c) odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
   d) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   e) IODO prowadzi rejestr wpływających wniosków.
2. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do sprostowania danych należy:
   A. wniosek należy przekazać do IODO,
   B. IODO zwraca się do ASI z prośbą o sprostowanie danych,
   C. ASI jest zobowiązany do sprostowania danych, o które wnioskował IODO w ciągu 10 dni,
   D. IODO przygotowuje projekt odpowiedzi na wniosek,
   E. odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
   F. odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   G. IODO prowadzi rejestr wpływających wniosków.
3. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do:
   A. usunięcia danych („prawo do bycia zapomnianym"),
   B. ograniczenia przetwarzania,
   C. przenoszenia danych,
   D. sprzeciwu,

należy wniosek należy przekazać do IODO,

4. IODO ocenia zasadność wniosku:
   a) w przypadku, gdy żądanie nie jest zasadne:
      A. IODO przygotowuje odpowiedź do akceptacji i podpisu Administratora lub osoby upoważnionej,
      B. odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   b) w przypadku, gdy żądanie jest zasadne:
      A. IODO zwraca się do ASI z prośbą o realizację żądań zawartych we wniosku,
      B. ASI jest zobowiązany do realizacji wniosku IODO w ciągu 10 dni,
      C. IODO przygotowuje projekt odpowiedzi na wniosek,
      D. odpowiedź na wniosek podpisuje Administrator lub osoba upoważniona,
      E. odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   c) IODO prowadzi rejestr wniosków.
5. ADM udziela odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki, najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania zobowiązany jest do podania przyczyny. Jeżeli żądanie ma skomplikowany charakter podmiot danych skierował dużą liczbę żądań, ADM czas udzielenia odpowiedzi może wydłużyć o kolejne dwa miesiące, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi.
6. W przypadku jakichkolwiek zmian w zbiorach danych wynikających z realizacji praw osób, których dane dotyczą, ADM zobowiązany jest poinformować bez zbędnej zwłoki odbiorców, którym je udostępnił (przekazanie do wiadomości odpowiedzi kierowanej do adresata).

§ 10

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych na podstawie przepisów prawa,
   2) na podstawie umowy powierzenia zawartej z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych osobowych.
2. Dane osobowe udostępnia się na pisemny umotywowany wniosek, chyba że istnieją przepisy stanowiące inaczej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§11.

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach i pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane, osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność IODO i Administratorowi.
4. IODO i Administrator podejmują wszelkie niezbędne środki techniczne organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§ 12.

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

§ 13.

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   a) nieautoryzowany dostęp do danych,
   b) nieautoryzowane modyfikacje lub zniszczenie danych,
   c) udostępnienie danych nieautoryzowanym podmiotom,
   d) nielegalne ujawnienie danych,
   e) pozyskiwanie danych z nielegalnych źródeł.

3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych lub podejrzewa, że taka sytuacja miała miejsce, ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
4. W przypadku podejrzenia lub stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub innej osób upoważnionych przez Administratora.
5. Wobec osoby, która naruszyła zasady ochrony danych osobowych lub w przypadku stwierdzonego naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby, zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne, porządkowe lub karne. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby dokonującej naruszenia lub uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W przypadku podejrzenia lub stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IODO i Administratora.
7. W przypadku opisanym w ust. 1 przeprowadza się sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.
8. Przy dokonywaniu sprawdzenia IODO oraz osobom wyznaczonym do współpracy z nim przez Administratora przysługują uprawnienia wskazane w rozporządzeniu ministra administracji i cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych, w szczególności prawo do:
   a) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
   b) odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
   c) sporządzeniu kopii otrzymanego dokumentu;
   d) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.
9. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając Raport według wzoru (Załącznik nr 9).
10. Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze, w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych osobowych i prowadzi Wykaz naruszeń według wzoru (Załącznik nr 10).
11. Jeżeli IODO jest długotrwale nieobecny Administrator w przypadku, o którym mowa w ust. 1 obowiązany jest przeprowadzić postępowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad

bezpieczeństwa i sposobów zabezpieczenia, w sposób odpowiadający czynnościom podejmowanym przez IODO w przypadku sprawdzenia doraźnego.

§ 14
POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. IODO podejmuje decyzje o wprowadzeniu zmian w środkach zabezpieczeń fizycznych oraz w systemie organizacji pracy, stosownie do mogących ponownie wystąpić naruszeń bezpieczeństwa danych osobowych.
2. ASI podejmuje decyzje odnośnie zmian w sposobie zabezpieczenia systemu informatycznego.
3. Administrator podejmuje decyzje o wyciągnięciu konsekwencji wobec osoby odpowiedzialnej za naruszenie zasad bezpieczeństwa.
4. IODO przekazuje do PUODO w terminie do 72 godzin, zgłoszenie zawierające informacje o stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:
    a) w przypadku przekroczenia 72 godzinnego terminu dodatkowo do zgłoszenia dołącza wyjaśnienia,
    b) w przypadku gdy informacji nie może udzielić w tym samym czasie, udziela ją sukcesywnie bez zbędnej zwłoki.
5. IODO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Poinformowanie bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Należy przekazywać informację osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z PUODO, z poszanowaniem wskazówek przekazanych przez PUODO lub inne odpowiednie organy, takie jak organy ścigania. Zawiadomienie powinno przekazywać informację w jasnym i prostym języku a zawierać:
    a) opis charakteru naruszenia ochrony danych osobowych,
    b) zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków.
7. Poinformowanie, o którym mowa w pkt. 6 nie jest wymagane jeśli PUODO stwierdzi, że spełniony został jeden z poniższych warunków:
    a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
    b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    c) wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają

poinformowane w równie skuteczny sposób.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRWANIEŃ W SYSTEMIE INFORMATYCZNYM
§ 15.

Użytkownikowi systemu informatycznego zostaje nadany dostęp na podstawie „Karty dostępu (zmiany) do przetwarzania danych w systemie informatycznym", stanowiącej załącznik nr 11 do niniejszej Polityki, po uprzednim:

1. Zapoznaniu z przepisami dotyczącymi ochrony danych osobowych.
2. Podpisaniu oświadczenia o zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych.
3. Podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych.
4. Otrzymaniu upoważnienia do przetwarzania danych osobowych.

POLITYKA HASEŁ
§ 16.

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora Systemu Informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznego Administratora jest obowiązany do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego;
   4) poinformowania Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   6) stosowania haseł nie posiadających w swojej strukturze części loginu;
   7) stosowania haseł nie będących zbliżone do poprzednich (np.Tomasz$2013 - Tomasz$2014);
   8) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.
5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
6. Zabronione jest:

1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
4) udostępnianie haseł innym użytkownikom;
5) przeprowadzanie prób łamania haseł;
6) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);
7) po trzykrotnym, błędnym wprowadzeniu hasła użytkownik jest zobowiązany zgłosić ten fakt do Administratora Systemu Informatycznego, w celu zresetowania hasła dostępowego.

POLITYKA KLUCZY
§ 17.

I. Postanowienia ogólne

1. Polityka obowiązuje wszystkich pracowników Urzędu Gminy w Chrzypsku Wielkim.
2. Wykaz pomieszczeń w budynku/ach* Urzędu Gminy stanowi *Załącznik Nr 1 do Polityki kluczy* i dotyczy wszystkich budynków i pomieszczeń będących w dyspozycji Urzędu Gminy w Chrzypsku Wielkim z siedzibą przy ulicy Głównej 15, 64-412 Chrzypsko Wielkie.
3. Za nadzór nad przestrzeganiem niniejszej procedury odpowiadają Kierownik Jednostki oraz Pracownicy zajmujący samodzielne stanowiska.
4. Utrzymanie skutecznego zabezpieczenia budynku Urzędu, tj. zamknięć, krat, zamków, kluczy, sytemu alarmowego i monitoringu wizyjnego należy do zadań Jednostki.
5. Za przyznanie i odebranie prawa do pobierania kluczy do konkretnego pomieszczenia odpowiedzialny jest w Kierownik Jednostki.
6. Z uwagi na publiczny charakter Urzędu, w czasie jego pracy nie obowiązuje system przepustek, ani też inny system określający uprawnienia do wejścia, przebywania i wyjścia z budynku Urzędu.
7. Zobowiązuje się pracowników Urzędu do:
   a) zwracania uwagi na zachowanie osób wchodzących i wychodzących z budynku Urzędu;
   b) reagowania na wejście do budynku i przebywanie w nim osób będących pod wpływem alkoholu lub innych środków odurzających;
   c) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku Urzędu;
   d) reagowania na próby wnoszenia do budynku przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie itp.;
   e) natychmiastowego reagowania poprzez powiadomienie odpowiednich służb (Straż Miejska, Policja, Straż Pożarna, Pogotowie Ratunkowe) o zaobserwowanych próbach
   f) stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia

mienia.

8. Klucze do pomieszczeń biurowych, jak również do pomieszczeń szczególnie chronionych (serwerownia) zdawane i wydawane są w sekretariacie Urzędu. Wzór upoważnienia do zarządzania kluczami i/albo kodem cyfrowym do systemu alarmowego stanowi *Załącznik nr 2 o Polityki kluczy*.
9. Pracownicy przed rozpoczęciem pracy podpisują listę obecności znajdującą się w pomieszczeniu dyżurki oraz pobierają klucze do swoich pomieszczeń biurowych.
10. Od momentu pobrania kluczy do momentu ich zdania na pracownikach urzędujących w tych pomieszczeniach spoczywa pełna odpowiedzialność za ich należyte zabezpieczenie.
11. Pracownikom zabrania się:
    a) wynoszenia kluczy poza Urząd,
    b) samodzielnego dorabiania kluczy do pomieszczeń i budynku Urzędu,
    c) pozostawiania kluczy w zamkach od strony korytarza podczas obecności i nieobecności pracownika w pomieszczeniu,
    d) udostępniania kluczy osobom nieupoważnionym.
12. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu. Po zakończonej pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
13. Po zakończeniu pracy, pracownicy zobowiązani są do uporządkowania swoich

a) stanowisk pracy oraz wykonania czynności zabezpieczających, w szczególności do:
    b) zabezpieczenia dokumentacji i pieczęci urzędowych;
    c) zabezpieczenia komputerów i nośników informacji;
    d) wyłączenia wszystkich urządzeń zasilanych energią elektryczną (czajniki, wentylatory zgodnie z zasadami bhp;
    e) zamknięcia okien i drzwi;
    f) pozostawienia kluczy od pomieszczeń biurowych w dyżurce, po zakwitowaniu.

14. Klucze zapasowe do wszystkich pomieszczeń Urzędu są zabezpieczone i przechowywane w zamkniętej szafie zlokalizowanej w bezpiecznym miejscu Urzędu. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do sekretariatu.
15. Wydawanie kluczy zapasowych pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w przypadkach awaryjnych. Rejestr wydawania i zdawania kluczy zapasowych stanowi *Załącznik Nr 3 do Polityki kluczy*.
16. Otwarcie Urzędu w soboty, niedziele oraz święta możliwe jest wyłącznie w uzasadnionych przypadkach za wiedzą i zgodą Administratora – Wójta Gminy oraz w związku z przeprowadzeniem ceremonii zawarcia małżeństwa.
17. Do otwierania pomieszczeń dla potrzeb wykonania czynności związanych ze sprzątaniem wykorzystywane są klucze powierzone do tego celu pracownikom obsługi. Klucze po wykonanych czynnościach osoby sprzątające zamykają w szafce zlokalizowanej w bezpiecznym miejscu. Osobą odpowiedzialną za zorganizowanie pracy pracowników obsługi (sprzątaczek) poza godzinami pracy Wójt.
18. Komplet kluczy wejściowych do budynku Urzędu posiadają następujące osoby:

.....
.....
.....

II. Bezpieczeństwo serwerowni

1. Zabezpieczenia serwerowni można podzielić na:
   a) fizyczne (drzwi, ściany, stropy itp.),
   b) techniczne (elektroniczne systemy zabezpieczeń),
   c) środowiskowe (zapewnienie optymalnej pracy urządzeń i ochrona przeciwpożarowa),
   d) personalne (pracownicy ochrony, świadomy personel),
   e) organizacyjne (obowiązujące regulaminy, polityki itp.).
2. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa komputerowych nośników danych może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego.
3. Strefy bezpieczeństwa są chronione systemem sygnalizacji włamania i napadu.
4. W uzasadnionych przypadkach, zarówno strefy administracyjne jak i strefy bezpieczeństwa, mogą być poddane monitoringowi wizyjnemu.
5. Strefy bezpieczeństwa nie posiadają oznakowania wewnątrz lub na zewnątrz, które, wskazywałyby na to, że znajdują się w nich szczególnie chronione zasoby.
6. Klucze do strefy bezpieczeństwa przechowywane są u .....w kasie pancernej zamykanej na klucz. Kluczem w godzinach pracy dysponują pracownicy obsługi, a po godzinach pracy pracownik dyżurki lub pracownik wyznaczony przez Kierownika Jednostki.
7. Klucze od biurek stanowiskowych i szaf biurowych znajdujących się w strefie bezpieczeństwa są w posiadaniu upoważnionych pracowników którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
8. Gospodarka kluczami zapasowymi do strefy bezpieczeństwa podlega przepisom opisanym w polityce kluczy.
9. Strefa bezpieczeństwa sprzątana jest wyłącznie w godzinach pracy urzędu w obecności zatrudnionych tam pracowników.
10. Utrzymanie skutecznego zabezpieczenia technicznego strefy administracyjnej, stosownie do obowiązujących wymogów w tym zakresie (zamknięcia, systemy zamknięcia elektronicznego, kraty) podlega nadzorowi Kierownika Jednostki.

Załącznik Nr 1

Wykaz pomieszczeń z ich numeracją oraz osobą odpowiedzialną za klucz

L.p.	Lokalizacja pomieszczenia	Nr pomieszczenia	Osoba odpowiedzialna za klucz

Załącznik Nr 2

Upoważnienie do zarządzania kluczami oraz kodem cyfrowym do system alarmowego Urzędu Gminy w Chrzypsku Wielkim

Na podstawie obowiązującej w Urzędzie Gminy w Chrzypsku Wielkim Polityki kluczy, obowiązującej od dnia ..... 2020 r. powierzam
Pani(u)*

.....

zatrudnionej(mu) na stanowisku .....

komplet kluczy do strefy administracyjnej.

W skład kompletu do pomieszczeń biurowych wchodzą następujące klucze:

1 – od pomieszczenia Nr .....
2 – od pomieszczenia Nr .....
3 – od pomieszczenia Nr .....
4 – od pomieszczenia Nr .....
5 – od pomieszczenia Nr .....
6 – od pomieszczenia Nr .....

Ponadto, przydzielam Pani(u) kod cyfrowy do systemu alarmowego, który należy zachować w ścisłej tajemnicy i wykorzystywać zgodnie z postanowieniami Polityki kluczy.

.....
Kierownik jednostki

Oświadczenie pracownika

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze /kod cyfrowy* do systemu alarmowego i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem.

.....

(data i podpis pracownika)

*niepotrzebne skreślić

Załącznik Nr 3

Rejestr wydawania kluczy zapasowych

Lp.	Data	Nr pokoju	Przyczyna pobrania klucza	Godzina pobrania	Imię i nazwisko pracownika pobierającego klucz	Podpis

Lp.	Data	Nr pokoju	Przyczyna zdania kluczy	Godzina zdania	Imię i nazwisko pracownika zdającego klucz	Podpis

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI
§ 18.

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych Administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy bezzwłocznie powiadomić Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.
5. Dane osobowe wrażliwe lub informacje poufne Administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu Informatycznego oraz Inspektorowi Ochrony Danych.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

§ 19.

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić wIODOk wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty danych.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:
   a) Wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
   b) Niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§ 20.

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością Administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.

5. Użytkownicy mają prawo korzystać z systemu poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
6. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych lub umownych, a także na wydajność systemu poczty elektronicznej.
7. Zabronione jest:
   1) wysyłanie bez zgody Administratora materiałów służbowych zawierających chronione dane na konta prywatne (np. celem pracy nad dokumentami poza miejscem pracy);
   2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
   3) odbieranie przesyłek z nieznanych źródeł;
   4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych bez zgody Administratora;
   6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
   7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
   8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;
   9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
   10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)
§ 21.

1. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
2. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Wprowadza się całkowity zakaz w dostępie do treści niezgodnych z prawem lub niestosownych, a w szczególności pornograficznych, rasistowskich, traktujących o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§ 22.

Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:

1) Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
2) Komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości maskować je;
3) Użytkownik wykonując czynności zawodowe lub umowne poza stałym miejscem wykonywania obowiązków powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
4) Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
5) Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością UG Chrzypsko Wielkie;
6) W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Ochrony Danych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;
7) Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§ 23.

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartphony,
   5) drukarki,
   6) modemy,
   7) monitory,
   8) routery,
   9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.

3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, administrator systemu informatycznego informuje o powyższym Inspektora Ochrony Danych.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować, usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ
§ 24.

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne Administratora jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM
§ 25.

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z administratorem systemu informatycznego.

POSTANOWIENIA KOŃCOWE
§ 26.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
3. Polityka jest dostępna w sieci Intranet Administratora.

Załączniki:

Załącznik nr 1 ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH
Załącznik nr UPOWAŻNIENIE NR do przetwarzania danych osobowych, OŚWIADCZENIE PRACOWNIKA
Załącznik nr 3 UPOWAŻNIENIE NR do przebywania w obszarze przetwarzania, OŚWIADCZENIE PRACOWNIKA
Załącznik nr 4 ODWOŁANIE UPOWAŻNIENIA do przetwarzania danych osobowych
Załącznik nr 5 Informacja w Sekretariacie i na stronie internetowej
Załącznik nr 5a Klauzula informacyjna dot. przetwarzania danych osobowych w związku z ustawą z dnia 24 września 2010 r. o ewidencji ludności)
Załącznik nr 5b Klauzula informacyjna dot. przetwarzania danych osobowych w związku z ustawą z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa)
Załącznik nr 5c Klauzula informacyjna dot. przetwarzania danych osobowych w związku z wydaniem zaświadczenia o wyłączeniu gruntów z produkcji rolnej
Załącznik nr 5d Klauzula informacyjna dot. przetwarzania danych osobowych w związku z wycinką drzew i krzewów
Załącznik nr 5e Klauzula informacyjna dot. przetwarzania danych osobowych na podstawie ustawy z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego
Załącznik nr 5f Klauzula dot. usuwania folii rolniczych i innych odpadów pochodzących z działalności rolniczej
Załącznik nr 5g Klauzula dot. utrzymania czystości i porządku w gminach
Załącznik nr 6 Klauzula informacyjna KANDYDACI DO PRACY
Załącznik nr 7 Klauzula informacyjna ZATRUDNIENI
Załącznik nr 8 Klauzula informacyjna ZAMÓWIENIA PUBLICZNE i ZAOPATRZENIE
Załącznik nr 9 WZÓR Raport
Załącznik nr 10 WYKAZ INCYDENTÓW POWODUJĄCYCH NARUSZENIE OCHRONY DANYCH OSOBOWYCH
Załącznik nr 11 Wzór karty

Załącznik nr 1

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Ja, niżej podpisana/y ....., **legitymujący się dowodem osobistym/paszportem/kartą pobytu serii** ..... **o numerze** .....

wyrażam zgodę na*:

- ○ przetwarzanie moich danych osobowych przez Urząd Gminy Chrzypsko Wielkie (dalej: UG Chrzypsko Wielkie) do celów realizacji zadań ustawowych i statutowych,
- ○ przetwarzanie moich danych osobowych przez w UG Chrzypsko Wielkie do celów promocyjnych,
- ○ przetwarzanie moich danych osobowych przez UG Chrzypsko Wielkie w związku ze zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, w tym przekazywaniem danych osobowych do państwa trzeciego.

UG Chrzypsko Wielkie przetwarza dane osobowe na następującym/ch **portalu/ach społecznościowym/ch:** ....., co oznacza **automatyczne przetwarzanie danych** oraz ich profilowanie przez właściciela portalu oraz przekazywanie danych osobowych tj. np. wizerunek - udostępnionych na tym portalu/ach - do Państw Trzecich (poza obszar UE).

proszę zaznaczyć zakres zgody

Rozumiem, że moje dane osobowe mogą być przetwarzane z pominięciem mojej zgody w następujących sytuacjach:

a) przetwarzanie jest niezbędne do wykonania umowy lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Zgodnie z art. 4 ust. pkt. 7 RODO **Administratorem** Pani/Pana danych osobowych jest **Wójt.**

Podanie danych osobowych jest dobrowolne lub wynika z obowiązku podania danych na podstawie przepisów obowiązującego prawa lub przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania. Dokumenty zawierające Pani/Pana dane osobowe będą przetwarzane przez okres określony przepisami prawa. Przetwarzane dane osobowe mogą być udostępniane innym podmiotom zwłaszcza, gdy obowiązek taki wynika z powszechnie obowiązujących przepisów prawa lub na podstawie niniejszej - wyrażonej przez Panią/Pana - zgody. **Ma Pani/Pan prawo wycofać zgodę w każdym momencie, w formie ustnej lub pisemnej.**

.....

Data, miejsce i podpis osoby wyrażającej zgodę*

Załącznik nr 2

UPOWAŻNIENIE NR .....
do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady Europy (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Poz. 1000) upoważniam:

Panią/Pana: .....

wykonującą/wykonującego obowiązki .....

w Urzędzie Gminy w Chrzypsku Wielkim

.....

.....

.....

(pieczęć instytucji)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem zadań wynikających z zakresu obowiązków i czynności w systemach kartotekowych oraz informatycznych* (dostęp do modułów oraz danych zgodnie z prawem dostępu nadanym przez administratora), w kategoriach:

- danych osobowych interesantów z podzbiorami w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*
- danych pracowniczych z podzbiorami w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*
- danych administracyjnych z podzbiorami w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*
- danych doraźnych w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*

w okresie: na czas stażu/praktyki/ zatrudnienia/ wolontariatu *

.....

Pieczęć i podpis Administratora Danych lub upoważnionego przedstawiciela

....., dnia .....

***niepotrzebne skreślić**

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisany/na oświadczam, iż zostałem/zostałam* przeszkolony/przeszkolona* w zakresie ochrony danych osobowych i znana jest mi treść **Polityki Ochrony Danych Osobowych** wraz z załącznikami i zobowiązuję się:

- do przestrzegania i stosowania zasad zawartych w wyżej wymienionych dokumentach,
- zachować w tajemnicy dane w tym dane osobowe, z którymi zetknąłem/zetknęłam* się w trakcie wykonywania swoich zadań, zarówno w czasie trwania umowy jak i po jej zakończeniu,
- chronić dane w tym dane osobowe przed dostępem osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem polityki bezpieczeństwa i ustawy oraz zmianą, utratą, ujawnieniem, uszkodzeniem lub zniszczeniem.

.....

Czytelny podpis pracownika

.....

Podpis Inspektora Ochrony Danych

* niewłaściwe skreślić lub wpisać właściwe

Załącznik nr 3

UPOWAŻNIENIE NR .....

do przebywania w obszarze przetwarzania

WAŻNOŚĆ:

Od* .....
Do* .....
Na czas trwania stosunku pracy*

UPOWAŻNIENIE
DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie pkt 1.2 załącznika do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., NR 100, poz. 1024 ze zm.) UPOWAŻNIAM Panią/Pana*:

.....
(imię i nazwisko pracownika)

.....
(stanowisko)

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe, w czasie niezbędnym do wykonywania obowiązków służbowych.

.....
Podpis Wójta

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisany/na oświadczam, iż zostałem/zostałam* przeszkolony/przeszkolona* w zakresie ochrony danych osobowych i znana jest mi treść **Polityki Ochrony Danych Osobowych** wraz z załącznikami i zobowiązuję się:

- do przestrzegania i stosowania zasad zawartych w wyżej wymienionych dokumentach,
- zachować w tajemnicy dane w tym dane osobowe, z którymi zetknąłem/zetknęłam* się w trakcie wykonywania swoich zadań, zarówno w czasie trwania umowy jak i po jej zakończeniu,
- chronić dane w tym dane osobowe przed dostępem osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem polityki bezpieczeństwa i ustawy oraz zmianą, utratą, ujawnieniem, uszkodzeniem lub zniszczeniem.

.....
Czytelny podpis pracownika

.....
Podpis Inspektora Ochrony Danych

Załącznik nr 4
ODWOŁANIE UPOWAŻNIENIA
do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady Europy (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 (RODO), odwołuję z dniem ..... upoważnienie nr ....., z dnia ..... do przetwarzania danych osobowych /przebywania w obszarze przetwarzania* wydane Pani/Panu:

.....

(imię i nazwisko pracownika)

na stanowisku:

.....

.....

Podpis Wójta

*Niepotrzebne skreślić

Klauzula informacyjna dot. przetwarzania danych osobowych na podstawie obowiązku prawnego ciążącego na Administratorze

TOŻSAMOŚĆ ADMINISTRATORA i WSPÓŁADMINISTRATORA	Administratorem danych osobowych jest **Wójt Gminy Chrzypsko Wielkie z siedzibą Urzędu Gminy,** ul. Główna 15, 64-412 Chrzypsko Wielkie, tel.: 61 29 51 011, fax: 61 62 10 890, e-mail: urzad@chrzypsko.pl w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej.
DANE KONTAKTOWE ADMINISTRATORA, WSPÓŁADMINISTRATORA I DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH	**Z administratorem - Wójtem Gminy Chrzypsko Wielkie** można się skontaktować pisemnie na adres jego siedziby **Z administratorem – Wójtem Gminy Chrzypsko Wielkie** można się skontaktować pisemnie na adres jego siedziby tj. **Urząd Gminy,** ul. Główna 15, 64-412 Chrzypsko Wielkie, tel.: 61 29 51 011, fax: 61 62 10 890, e-mail: urzad@chrzypsko.pl lub z wyznaczonym przez niego inspektorem ochrony danych pod adresem: kontakt@smart-standards.com albo pod numerem tel. +48 602 24 12 39 Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, które pozostają w jego zakresie działania.
CELE PRZETWARZANIA I PODSTAWA PRAWNA	Pani/Pana dane oraz/lub dane Pani/Pana dziecka lub podopiecznego będą przetwarzane na podstawie art. 6 ust. 1 lit. c w związku z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, z późn. zm.) (dalej: RODO) w celach **realizacji zadań określonych w ustawie o samorządzie gminnym** (Dz.U.2019.0.506 t.j. - Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym)
ODBIORCY DANYCH	Odbiorcami danych są podmioty przetwarzające te dane. Pani/Pana dane osobowe oraz/lub dane osobowe Pani/Pana dziecka/podopiecznego mogą być udostępnione podmiotom: • służbom; organom administracji publicznej; sądom i prokuraturze; komornikom sądowym; państwowym i samorządowym jednostkom organizacyjnym oraz innym podmiotom – w zakresie niezbędnym do realizacji zadań publicznych; • osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes prawny; • osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes faktyczny w otrzymaniu danych, pod warunkiem uzyskania zgody Pani /Pana zgody; • jednostkom organizacyjnym, w celach badawczych, statystycznych, badania opinii publicznej, jeżeli po wykorzystaniu dane te zostaną poddane takiej modyfikacji, która nie pozwoli ustalić tożsamości osób, których dane dotyczą; przez: • **Wójta Gminy Chrzypsko Wielkie** - podmiotom uprawnionym w trybie indywidualnych zapytań; Pani/Pana dane oraz dane Pani/Pana dziecka lub podopiecznego mogą być

	udostępnione stronom postępowań administracyjnych prowadzonych na podstawie Kodeksu postępowania administracyjnego, których jest Pan/Pani i/lub Pana/Pani podopieczny stroną/stronami lub uczestnikiem/ uczestnikami w trybie udostępnienia akt tych postępowań.
OKRES PRZECHOWYWANIA DANYCH	Dane zgromadzone w formie pisemnej są przetwarzane zgodnie z klasyfikacją wynikająca z jednolitego rzeczowego wykazu akt organów gminy i związków międzygminnych oraz urzędów obsługujących te organy i związki na podstawie przepisów rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011r. Dz.U. Nr 14, poz. 67).
PRAWA PODMIOTÓW DANYCH	Przysługuje Pani/Panu prawo dostępu do Pani/Pana danych oraz prawo żądania ich sprostowania.
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych, Biuro Prezesa Urzędu Ochrony Danych Osobowych Adres: Stawki 2, 00-193 Warszawa, Tel. 22 531 03 00
INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH	Obowiązek podania danych osobowych wynika z przepisów prawa, w szczególności dyrektywy RODO oraz ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U.2019.0.506 z późn. zm.)

Załącznik nr 5a
Klauzula informacyjna dot. przetwarzania danych osobowych
w związku z ustawą z dnia 24 września 2010 r. o ewidencji ludności

Klauzula informacyjna dot. przetwarzania danych osobowych na podstawie obowiązku prawnego ciążącego na administratorze (przetwarzanie w związku z ustawą z dnia 24 września 2010 r. o ewidencji ludności)	
TOŻSAMOŚĆ ADMINISTRATORA i WSPÓŁADMINISTRATORA	**Administratorami są:** 1. **Wójt Gminy Chrzypsko Wielkie z siedzibą Urzędu Gminy,** ul. Główna 15, 64-412 Chrzypsko Wielkie, tel.: 61 29 51 011, fax: 61 62 10 890, e-mail: urzad@chrzypsko.pl w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej.; 2. **Minister Cyfryzacji,** mający siedzibę w Warszawie (00-060) przy ul. Królewskiej 27 – odpowiada za nadawanie numeru PESEL oraz utrzymanie i rozwój rejestru PESEL 3. **Minister Spraw Wewnętrznych i Administracji**, mający siedzibę w Warszawie (02-591) przy ul Stefana Batorego 5 – odpowiada za kształtowanie jednolitych zasad postępowania w kraju w zakresie ewidencji ludności oraz zapewnia funkcjonowanie wydzielonej sieci umożliwiającej dostęp do rejestru PESEL.
DANE KONTAKTOWE ADMINISTRATORA, WSPÓŁADMINISTRATORA I DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH	1. **Z administratorem – Wójtem Gminy Chrzypsko Wielkie** można się skontaktować pisemnie na adres siedziby administratora ul. Główna 15, 64-412 Chrzypsko Wielkie, tel.: 61 29 51 011, fax: 61 62 10 890, elektronicznie na adres e-mail urzad@chrzypsko.pl 2. **Z administratorem – Ministrem Cyfryzacji** można się skontaktować poprzez adres email IODO@mc.gov.pl, formularz kontaktowy pod adresem https:// www.gov.pl /cyfryzacja/kontakt lub pisemnie na adres siedziby administratora. 3. **Z administratorem – Ministrem Spraw Wewnętrznych i Administracji** można się skontaktować poprzez adres mail IODO@mswia.gov.pl, formularz kontaktory pod adresem https://www.gov.pl/web/mswia/formularz-kontaktowy lub pisemnie na adres siedziby administratora. **Administrator – Wójt Gminy Chrzypsko Wielkie** wyznaczył inspektora ochrony danych – Panią Joannę Mrowicką, z którym może się Pani / Pan skontaktować telefonicznie pod numerem 602 24 12 39 lub elektronicznie na adres e-mail: kontakt@smart-standards.com lub pisemnie na adres siedziby administratora. Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, które pozostają w jego zakresie działania.
CELE PRZETWARZANIA I PODSTAWA PRAWNA	Pani / Pana dane będą przetwarzane na podstawie art. 6 ust. 1 lit. c Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) (dalej: RODO) w związku z przepisami szczególnymi ustawy z dnia 24 września 2010 r. o ewidencji ludności (tj. Dz. U. z 2019 r., poz. 1397) to znaczy: • przez Wójta Gminy Chrzypsko Wielkie - w celu wprowadzenia

	Pani/Pana danych do rejestru PESEL, udostępniania z niego Pani/Pana danych oraz prowadzenia rejestru mieszkańców – na podstawie art. 6a, art. 10, art. 11 oraz art. 50 ust. 1 pkt 2 ustawy o ewidencji ludności, • przez Ministra Cyfryzacji i Ministra Spraw Wewnętrznych i Administracji – w celu prowadzenia ewidencji ludności na terenie Rzeczypospolitej Polskiej na podstawie danych identyfikujących tożsamość oraz status administracyjno-prawny osób fizycznych wprowadzanych do rejestru PESEL – na podstawie art. 2, art. 5 ust. 3 i 4 oraz art. 6 ust. 2 ustawy o ewidencji ludności.
ODBIORCY DANYCH	Odbiorcami danych są podmioty przetwarzające dane: • Centrum Personalizacji Dokumentów – w zakresie udostępniania danych z rejestru PESEL w imieniu Ministra Spraw Wewnętrznych i Administracji w zakresie wniosków o udostępnienie danych złożonych przed 1 lipca 2019 r. • Centralny Ośrodek Informatyki – w zakresie technicznego utrzymania rejestru PESEL i jego rozwoju w imieniu Ministra Cyfryzacji • podmiot świadczący usługi w zakresie utrzymania i serwisu systemu obsługującego rejestr mieszkańców (dane podmiotu do uzupełnienia przez organ gminy). Pani/Pana dane osobowe udostępnia się podmiotom: • służbom; organom administracji publicznej; sądom i prokuraturze; komornikom sądowym; państwowym i samorządowym jednostkom organizacyjnym oraz innym podmiotom – w zakresie niezbędnym do realizacji zadań publicznych; • osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes prawny; • osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes faktyczny w otrzymaniu danych, pod warunkiem uzyskania zgody Pani /Pana zgody; • jednostkom organizacyjnym, w celach badawczych, statystycznych, badania opinii publicznej, jeżeli po wykorzystaniu dane te zostaną poddane takiej modyfikacji, która nie pozwoli ustalić tożsamości osób, których dane dotyczą; przez: • Wójta Gminy Chrzypsko Wielkie – z rejestru mieszkańców w trybie indywidualnych zapytań oraz zapewnienia do danych dostępu online - podmiotom wskazanym powyżej w pkt 1-4, z rejestru PESEL w trybie indywidualnych zapytań podmiotom wskazanym w pkt 1-3; • Ministra Cyfryzacji – z rejestru PESEL w trybie zapewnienia do danych dostępu online - podmiotom wskazanym powyżej w pkt 1 oraz w trybie indywidualnych zapytań podmiotom wskazanym w pkt 4; • Ministra Spraw Wewnętrznych i Administracji - z rejestru PESEL, w zakresie wniosków o udostepnienie danych złożonych przed 1 lipca 2019 r., w imieniu Ministra dane udostępnia podmiotom wskazanym powyżej w pkt 1-3 w trybie indywidualnych zapytań Centrum Personalizacji Dokumentów. Pani/Pana dane Wójt Gminy udostępnia także stronom postępowań administracyjnych prowadzonych na podstawie ustawy o ewidencji ludności i Kodeksu postępowania administracyjnego, których jest Pan/Pani stroną lub

	uczestnikiem w trybie udostępnienia akt tych postępowań.
OKRES PRZECHOWYWANIA DANYCH	Zgodnie z art. 12a ustawy o ewidencji ludności dane osobowe zgromadzone w rejestrze mieszkańców oraz w rejestrze PESEL przetwarzane są bezterminowo. Dane zgromadzone w formie pisemnej są przetwarzane zgodnie z klasyfikacją wynikająca z jednolitego rzeczowego wykazu akt organów gminy i związków międzygminnych oraz urzędów obsługujących te organy i związki (rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011r. Dz.U. Nr 14, poz. 67): • dokumentacja spraw z zakresu ewidencji ludności po 50 latach jest oceniana pod kątem możliwości zniszczenia natomiast dotycząca aktualizacji danych w ewidencji ludności niszczona jest po 5 latach; • dokumentacja spraw meldunkowych niszczona jest po 10 latach; • dokumentacja spraw związanych z udostępnianiem danych i wydawaniem zaświadczeń z ewidencji ludności niszczona jest po 5 latach.
PRAWA PODMIOTÓW DANYCH	Przysługuje Pani/Panu prawo dostępu do wyżej wymienionych danych oraz prawo żądania ich sprostowania.
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych, Biuro Prezesa Urzędu Ochrony Danych Osobowych Adres: Stawki 2, 00-193 Warszawa, Tel. 22 531 03 00.
INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH	Obowiązek podania danych osobowych wynika z przepisów prawa, w szczególności dyrektywy RODO oraz ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U.2019.0.506 z późn. zm.)

Załącznik nr 5b
Klauzula informacyjna dot. przetwarzania danych osobowych w związku z ustawą z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa)

Klauzula informacyjna dot. przetwarzania danych osobowych na podstawie obowiązku prawnego ciążącego na administratorze (przetwarzanie w związku z ustawą z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa)	
TOŻSAMOŚĆ ADMINISTRATORA i WSPÓŁADMINISTRATORA	1. **Wójt Gminy Chrzypsko Wielkie z siedzibą Urzędu Gminy,** ul. Główna 15, 64-412 Chrzypsko Wielkie, tel.: 61 29 51 011, fax: 61 62 10 890, e-mail: urzad@chrzypsko.pl – w zakresie rejestracji danych w rejestrze podatników praz prowadzenia i przetwarzania danych w tym rejestrze oraz przechowywanej dokumentacji pisemnej; 2. **Współadministratorem danych osobowych jest Naczelnik Urzędu Skarbowego w Międzychodzie** na adres: **Urząd Skarbowy w Międzychodzie** ul. Piłsudskiego 2, 64-400 Międzychód, **Numery telefonów:** Centrala Telefoniczna: 95 74 82 008, **E-mail:** us.miedzychod@mf.gov.pl lub naczelnik urzędu skarbowego właściwego dla miejsca rejestracji podatnika w zakresie rejestracji danych w rejestrze podatników praz prowadzenia i przetwarzania danych w tym rejestrze oraz przechowywanej dokumentacji pisemnej.
DANE KONTAKTOWE ADMINISTRATORA, WSPÓŁADMINISTRATORA I DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH	1. **Z administratorem – Wójtem Gminy Chrzypsko Wielkie można się skontaktować na adres siedziby Urzędu Gminy,** ul. Główna 15, 64-412 Chrzypsko Wielkie, tel.: 61 29 51 011, fax: 61 62 10 890, e-mail: urzad@chrzypsko.pl,; w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej. 2. **Ze współadministratorem – Naczelnikiem Urzędu Skarbowego w Międzychodzie** można się skontaktować pisemnie na adres jego siedziby tj. ul. **Urząd Skarbowy w Międzychodzie** ul. Piłsudskiego 2, 64-400 Międzychód, **Numery telefonów:** Centrala Telefoniczna: 95 74 82 008, **E-mail:** us.miedzychod@mf.gov.pl, na skrzynkę e-Puap: https://epuap.gov.pl/wps/portal/strefa-klienta/katalog-spraw/profil-urzedu/7wxbec315m lub z naczelnikiem urzędu skarbowego właściwego dla miejsca rejestracji podatnika według właściwości miejscowej
CELE PRZETWARZANIA I PODSTAWA PRAWNA	Pani / Pana dane będą przetwarzane na podstawie art. 6 ust. 1 lit. c Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) (dalej: RODO) w związku z przepisami szczególnymi **ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa** (t.j. Dz. U. z 2019 r. poz. 900, 924, 1018), **ustawy z dnia z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz. U. z 2019 r. poz. 1438, 1501, 1553, 1579, 1655, 1798) oraz Kodeksu postępowania administracyjnego oraz przepisów wykonawczych do w/w aktów prawnych w celach realizacji** zobowiązań podatkowych; pozyskania informacji podatkowych; prowadzenia postępowań podatkowych oraz kontroli podatkowej i czynności sprawdzających przez Wójta Gminy Chrzypsko Wielkie i/lub Naczelnika

	Urzędu Skarbowego w Międzychodzie i/lub z naczelnika urzędu skarbowego właściwego dla miejsca rejestracji podatnika według właściwości miejscowej. Pani / Pana dane wprowadzane są przez organ gminy do następujących rejestrów: 1) Rejestr zaświadczeń o wielkości gospodarstwa i o niezaleganiu w podatkach 2) Rejestr wymiarowy podatników podatku od nieruchomości 3) Rejestr wymiarowy podatników podatku rolnego 4) Rejestr wymiarowy podatników podatku leśnego 5) Rejestr wymiarowy podatników podatku od środków transportowych 6) Rejestr udzielonych umorzeń, odroczeń, rozłożenia na raty, ulg 7) Rejestr zaświadczeń o niezaleganiu w podatkach 8) Rejestr tytułów wykonawczych
ODBIORCY DANYCH	Odbiorcami danych są podmioty przetwarzające dane: • podmiot świadczący usługi w zakresie utrzymania i serwisu systemu obsługującego rejestr podatników na poziomie gminy, • podmiot świadczący usługi w zakresie utrzymania i serwisu systemu POLTAX, obsługującego rejestr podatników na poziomie kraju. Pani/Pana dane osobowe udostępnia się podmiotom: 1) służbom; organom administracji publicznej; sądom i prokuraturze; komornikom sądowym; państwowym i samorządowym jednostkom organizacyjnym oraz innym podmiotom – w zakresie niezbędnym do realizacji zadań publicznych; 2) osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes prawny; 3) osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes faktyczny w otrzymaniu danych, pod warunkiem uzyskania zgody Pani /Pana zgody; 4) jednostkom organizacyjnym, w celach badawczych, statystycznych, badania opinii publicznej, jeżeli po wykorzystaniu dane te zostaną poddane takiej modyfikacji, która nie pozwoli ustalić tożsamości osób, których dane dotyczą; przez Wójta Gminy Chrzypsko Wielkie – z rejestru podatników w trybie indywidualnych zapytań oraz zapewnienia do danych dostępu online - podmiotom wskazanym powyżej w pkt 1-4. Pani/Pana dane Wójt Gminy udostępnia także stronom postępowań administracyjnych prowadzonych na podstawie Kodeksu postępowania administracyjnego, których jest Pan/Pani stroną lub uczestnikiem w trybie udostępnienia akt tych postępowań.
OKRES PRZECHOWYWANIA DANYCH	Dane zgromadzone w formie pisemnej są przetwarzane zgodnie z klasyfikacją wynikająca z jednolitego rzeczowego wykazu akt organów gminy i związków międzygminnych oraz urzędów obsługujących te organy i związki (rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011r. Dz.U. Nr 14, poz. 67); dokumentacja spraw finansowo-podatkowych niszczona jest po 10 latach.
PRAWA PODMIOTÓW DANYCH	Przysługuje Pani/Panu prawo dostępu do Pani/Pana danych oraz prawo żądania ich sprostowania, a także prawo dostępu do danych osób, nad którymi sprawowana jest przez Panią/Pana opieka, np. danych dzieci oraz prawo żądania ich sprostowania.
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	**Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych** Biuro Prezesa Urzędu Ochrony Danych Osobowych Adres: Stawki 2, 00-193 Warszawa