Zarządzenie Nr 94/2019
Wójta Gminy Stara Dąbrowa
z dnia 06 sierpnia 2019 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Starej Dąbrowie

Na podstawie art. 24 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 (Dz. U.UE.L.2016.119.1) zarządzam co następuje:

§ 1. Wprowadzam Politykę Bezpieczeństwa Informacji Urzędu Gminy w Starej Dąbrowie, określoną w załączniku nr 1 do niniejszego zarządzenia.

§ 2. Wprowadzam Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Starej Dąbrowie, określoną w załączniku nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuje wszystkich pracowników Urzędu Gminy do przestrzegania zasad określonych dokumentach o których mowa w § 1 i 2

§ 4. Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Gminy.

§ 5. Traci moc zarządzenie Nr 86/2018 Wójta Gminy Stara Dąbrowa z dnia 05 listopada 2018 roku w sprawie wprowadzenia w Urzędzie Gminy Stara Dąbrowa Polityki Ochrony Danych Osobowych.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Sylwia Kalmus-Samsel

Załącznik nr 1 do Zarządzenia Nr 94/2019 Wójta Gminy Stara Dąbrowa
z dnia 06 sierpnia 2019 roku

POLITYKA BEZPIECZEŃSTWA INFORMACJI
W URZĘDZIE GMINY W STAREJ DĄBROWIE

Polityka bezpieczeństwa informacji jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych w Jednostce. Niniejszy dokument został wprowadzony Zarządzeniem Wójta Gminy oraz udostępniony każdej osobie mającej dostęp do danych osobowych przetwarzanych w Jednostce. Potwierdzeniem zapoznania się z postanowieniami niniejszego dokumentu jest złożenie pisemnego oświadczenia, którego wzór stanowi załącznik do polityki.

I. DEFINICJE

administrator danych osobowych- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

anonimizacja- zmiana danych osobowych, która oznacza utratę charakteru danych osobowych;

dane biometryczne- oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

dane dotyczące zdrowia- oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;

dane genetyczne- oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

dane osobowe- oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

incydent bezpieczeństwa danych- zdarzenie losowe zewnętrzne (pożar, zalanie wodą pomieszczenia, utrata zasilania), zdarzenie losowe wewnętrzne (awaria komputera lub serwera, pomyłka informatyka lub samego użytkownika, utrata lub zagubienie danych),

umyślne incydenty (kradzież danych lub sprzętu, wyciek informacji, świadome niszczenie dokumentów, działania wirusów i szkodliwego oprogramowania);

inspektor danych osobowych (IOD)- jeśli wyznaczono jest osobą, która została formalnie wybrana przez administratora danych osobowych do doradztwa i przekazywania informacji administratorowi, podmiotowi przetwarzającemu dane osobowe oraz pracownikom (w zakresie prawa dotyczącego ochrony danych osobowych. Do zadań IOD należy również kontrola i monitorowanie przestrzegania działań w zakresie polityki ochrony danych osobowych. Celem działania inspektora danych osobowych jest również kontakt między osobami przetwarzającymi dane, a organem nadzorczym;

naruszenie ochrony danych osobowych- oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

odbiorca- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

ograniczenie przetwarzania- oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

podatność bezpieczeństwa danych osobowych- niewłaściwe zabezpieczenie pomieszczeń, urządzeń i dokumentów; niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem lub kradzieżą danych osobowych; niestosowanie zasad ochrony danych przez pracowników (nieprzestrzeganie zasady czystego biurka, ochrony haseł, niezamykanie szafek i pomieszczeń);

podmiot przetwarzający (procesor)- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

profilowanie- oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

przetwarzanie danych osobowych- oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

pseudonimizacja- oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

RODO- rozporządzenie Parlamentu Europejskiego i Rady Europy nr 2016/679, które obejmuje sprawy ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych;

strona trzecia- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;

zbiór danych- oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

zgoda osoby, której dane dotyczą- oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

aktywa- zasoby materialne i niematerialne, które mają wpływ na przetwarzanie danych osobowych;

przypadek naruszenia ochrony danych osobowych (jednorazowe zdarzenie)- to naruszenie bezpieczeństwa ochrony danych osobowych, które prowadzi do zniszczenia, utracenia lub zmodyfikowania danych osobowych. Może także wiązać się z ujawnieniem lub nieuprawnionym dostępem do danych osobowych przez osoby trzecie,

ryzyko- prawdopodobieństwo wystąpienia zagrożenia, które może powodować straty lub zniszczenie zasobów zawierających dane osobowe,

skutki- efekty niepożądane incydentu (straty w wypadku wystąpienia zagrożenia),

zagrożenie-potencjalne naruszenie ochrony danych osobowych.

II. ANALIZA RYZYKA

Jeżeli dany rodzaj przetwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy wykonać ocenę skutków przetwarzania danych. Ocena ta ma służyć formalnej analizie ryzyka. Za jej wykonanie odpowiada Administrator, przy współudziale Inspektora Danych Osobowych.

1. Inwentaryzacja aktywów

W celu dokonania analizy, należy zidentyfikować dane osobowe, przetwarzane w zbiorach. Wykaz zbiorów danych osobowych stanowi **załącznik nr 1** do polityki. Opis zbiorów musi zawierać niezbędne informacje w postaci:

- nazwy zbioru,
- opisu celów przetwarzania,
- zakresu i charakteru danych osobowych,
- odbiorców danych osobowych,
- opisu operacji przetwarzania danych osobowych,
- aktywów, które są niezbędne do przetwarzania danych osobowych, np. programów, systemów operacyjnych, informacji, infrastruktury, pracowników,
- powiadomienia o konieczności wpisu do rejestru czynności przetwarzania oraz konieczności przeprowadzenie oceny skutków dla opisu kategorii osób.

Jeżeli jest to wymagane przepisami prawa, na podstawie wykazu zbiorów danych osobowych, sporządza się rejestr czynności przetwarzania danych (RCPD). Dopuszczalne jest, aby wykaz zbiorów danych osobowych oraz rejestr czynności przetwarzania danych stanowiły jeden plik.

2. Zgodność z przepisami RODO

Aby przeprowadzić analizę ryzyka Administrator powinien spełniać obowiązki prawne i formalne, poprzez gwarancję, że:

- dane będą legalnie przetwarzane,
- dane będą odpowiednie w stosunku do celu ich przetwarzania,
- dane będą przetwarzane przez określony czas,
- wobec osób, których dane osobowe będą przetwarzane, zostanie wykonany obowiązek informacyjny, którego celem jest wskazanie praw tych osób. Należy poinformować je, że mają prawo do dostępu do danych, do ich przenoszenia, sprostowania, usunięcia, bądź ograniczenia ich przetwarzania, a także do sprzeciwu przetwarzania danych oraz do odwołania zgody na przetwarzanie danych osobowych,
- zostały przygotowane klauzule informacyjne dla osób, których dane osobowe będą przetwarzane. Wzory klauzul informacyjnych stanowią **załącznik nr 2** do polityki,
- zostały przygotowane umowy powierzenia z podmiotami przetwarzającymi dane.

Wzór umowy powierzenia oraz rejestr umów powierzenia stanowią odpowiednio **załącznik nr 3 i 4** do polityki.

3. Analiza ryzyka

W celu zabezpieczenia danych osobowych należy przeprowadzić analizę ryzyka. Działanie to musi być odpowiednie do występujących zagrożeń, które mogą wynikać ze zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Analiza ryzyka dla poszczególnych aktywów stanowi **załącznik nr 5** do polityki.

Ocena ryzyka przeprowadzana jest dla każdego zidentyfikowanego podczas inwentaryzacji aktywa. W trakcie analizy ryzyka rozpatruje się prawdopodobieństwo

wystąpienia zagrożenia, podatność aktywów na zagrożenia oraz skutki potencjalnych zagrożeń. Ponadto, należy wziąć pod uwagę następstwa naruszenia lub utraty poufności, integralności i dostępności, które mogą nastąpić w wyniku działań umyślnych, przypadkowych oraz naturalnych.

Listę potencjalnych i realnych zagrożeń, wykaz aktywów i ich zabezpieczeń wykazano w **załączniku nr 5** do polityki. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa oraz skutków zdarzeń. Dodatkowo wprowadza się listę zabezpieczeń do wdrożenia, terminów ich realizacji i osób za to odpowiedzialnych, wszędzie tam, gdzie Administrator postanowi obniżyć ryzyko.

Ponowna analiza ryzyka jest realizowana cyklicznie oraz po wprowadzeniu ważnych zmian w przetwarzaniu danych osobowych. **Załącznik nr 5** w zakresie potencjalnych zagrożeń, wykazu aktywów i stosowanych zabezpieczeń, należy regularnie aktualizować. Administrator danych sprawuje nadzór i kontrolę nad wykazem zabezpieczeń, który ma na celu ochronę danych osobowych.

Instrukcja zarządzania systemem informatycznymi stanowi **załącznik nr 12** do polityki.

Dokumenty te opisują stosowane zabezpieczenia w jednostce i są aktualizowane po każdej analizie ryzyka i ocenie skutków.

III. UPOWAŻNIENIA

Za nadawanie i anulowanie upoważnień do przetwarzania danych osobowych w zbiorach (papierowych i informatycznych) odpowiada Administrator. Osoby upoważnione do przetwarzania danych osobowych dokonują tego wyłącznie na polecenie Administratora (lub na podstawie przepisu prawa). Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 6** do polityki. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi **załącznik nr 7** do polityki. Ewidencję prowadzi się w celu utrzymania kontroli nad dostępem poszczególnych osób do danych osobowych.

IV. INCYDENTY

Procedura ta opisuje sposób postępowania w przypadku wystąpienia incydentów zagrażających bezpieczeństwu danych osobowych. Ponadto, celem procedury jest ograniczenie ryzyka powstawania zagrożeń i występowania incydentów w przyszłości.

Osoby posiadające upoważnienia do przetwarzania danych osobowych są zobligowane do niezwłocznego poinformowania przełożonego lub IOD, o sytuacji, w której wystąpiło stwierdzenie incydentu.

W przypadku wystąpienia incydentu Administrator (lub IOD) winien przeprowadzić postępowanie wyjaśniające, które ustali przyczyny i zakres niepożądanego zdarzenia, oraz określi jego ewentualne skutki. Administrator (lub IOD) podejmuje działania dyscyplinarne i działa na rzecz przywrócenia sprawnego działania jednostki po wystąpieniu incydentu. Osoba

odpowiedzialna za przetwarzanie danych osobowych zaleca działania zapobiegawcze, które mają w przyszłości eliminować wystąpienie podobnych incydentów, lub zmierzają do zmniejszenia strat w momencie ich zaistnienia.

Wystąpienie incydentów powinno być udokumentowane przez Administratora, w tym wszystkie okoliczności, w których doszło do naruszenia ochrony danych osobowych, opisane skutki i podjęte działania zapobiegawcze. Formularz rejestracji incydentu oraz sposób jego oceny stanowi **załącznik nr 8** do polityki.

W przypadku utraty danych osobowych Administrator powinien zapewnić możliwość jak najszybszego przywrócenia dostępności tych danych, dzięki zastosowaniu procedur przywracania danych. Tworzone kopie zapasowe należy regularnie testować.

W przypadku wystąpienia incydentów skutkujących naruszeniem praw lub wolności osób fizycznych, Administrator powiadamia organ nadzorczy, nie później niż 72 godziny po wystąpieniu incydentu, oraz osoby, których dane dotyczyły.

W toku oceny naruszenia bierze się pod uwagę kontekst przetwarzania **(KP)**, łatwość identyfikacji **(I)** i okoliczności naruszenia **(ON)**. Poziom naruszenia **(PN)** praw i wolności ocenia się według wzoru **PN=KPxI+ON** na podstawie wytycznych Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA).

V. REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie niezbędnej wiedzy osobom, które przetwarzają dane osobowe w celu ich bezpiecznego przetwarzania. Obowiązki te dotyczą przede wszystkim pracowników, współpracowników, innych pracowników, którzy posiadają dostęp do przetwarzanych danych w formie papierowej oraz w systemach informatycznych. Każda osoba, która zapoznała się z Regulaminem zobowiązana jest do potwierdzenia znajomości tych zasad i deklaracji ich stosowania. Wzór oświadczenia o dochowaniu tajemnicy służbowej i o zaznajomieniu się z zasadami ochrony danych, oraz ewidencja oświadczeń stanowi odpowiednio **załącznik nr 9 i 10** do polityki.

Każdy pracownik, w tym nowo zatrudniony pracownik, zanim zostanie dopuszczony do pracy z danymi osobowymi, powinien zostać przeszkolony i zapoznany z przepisami RODO. Za przeprowadzenie szkolenia odpowiedzialny jest Administrator. Szkolenia pracowników należy udokumentować zakresem szkolenia i listą obecności. Szkolenia pracowników przeprowadza się nie rzadziej niż raz do roku.

1. Bezpieczne użytkowanie sprzętu IT

- osoba, która przetwarza dane osobowe i korzysta ze sprzętu IT (komputer stacjonarny, monitor, drukarka, skaner, ksero, laptop, tablet, smartfon) ma obowiązek zabezpieczenia go przed zniszczeniem lub uszkodzeniem,
- przypadki zgubienia, utraty lub zniszczenia powierzonego sprzętu IT powinny być zgłoszone. Zabrania się samowolnego instalowania sprzętu IT i dodatkowych urządzeń (twarde dyski, pamięć),
- zakazuje się podłączania niezatwierdzonych urządzeń do systemu informatycznego,

- należy uniemożliwić osobom niepowołanym wgląd do danych widocznych na ekranie monitora,
- czasowe opuszczenie miejsca pracy winno się wiązać z przywołaniem blokowanego hasłem wygaszacza ekranu (*WINDOWS+L*). Dozwolone jest całkowite wylogowanie się z systemu lub programu,
- po zakończeniu pracy należy wylogować się z systemu informatycznego, wyłączyć sprzęt komputerowy, zabezpieczyć stanowisko pracy (szczególnie nośniki, na których znajdują się dane osobowe),
- w trakcie wspólnego użytkowania komputera, użytkownicy zobowiązani są do usuwania plików, do których dostęp mają inni nieuprawnieni użytkownicy,
- osoby uprawnione do niszczenia nośników mają obowiązek trwale zniszczyć nośnik, lub trwale usunąć z niego dane.

2. Uprawnienia

- każdy użytkownik musi posiadać swój indywidualny identyfikator (*login*) i hasło. Zabrania się umożliwiania innym osobom pracy na swoim identyfikatorze,
- polecenie do utworzenia konta wraz z uprawnieniami wydaje przełożony. Czynności te wykonuje osoba wyznaczona, tj. informatyk, lub jeżeli wyznaczono- Administrator Sieci Informatycznej (ASI),
- użytkownik nie ma prawa do zmiany swoich uprawnień,
- użytkownik rozpoczyna pracę z użyciem identyfikatora (loginu) i hasła,
- jeśli system zasygnalizuje próby logowania się do systemu osoby nieupoważnionej, należy to niezwłocznie zgłosić informatykowi (ASI),
- w chwili zablokowania systemu podczas próby logowania, należy natychmiast powiadomić o tym informatyka (ASI),
- należy uniemożliwić osobom nieupoważnionym wgląd do danych zawartych na ekranach monitorów,
- w przypadku czasowego opuszczenia miejsca pracy system należy zablokować (*WINDOWS+L*). Dozwolone jest całkowite wylogowanie się z systemu lub programu,
- po upływie 10 minut system automatycznie aktywuje wygaszacz,
- nie można uruchamiać aplikacji, które nie zostały zweryfikowane przez informatyka (ASI), w szczególności dotyczy to programów przesyłanych pocztą elektroniczną,
- po zakończeniu pracy użytkownik musi wylogować się z wszelkich systemów informatycznych, wyłączyć sprzęt komputerowy oraz zabezpieczyć stanowisko pracy (w szczególności dokumentację i nośniki, na których znajdują dane osobowe).

3. Polityka haseł

- hasło musi zawierać określoną liczbę znaków, duże i małe litery oraz cyfrę (mogą też zawierać znaki specjalne). Hasło powinno być trudne do odgadnięcia. Nie może być powszechnie używanym słowem. Hasłem nie powinny być: imiona, daty urodzenia, nazwiska oraz typowe zestawy (1234..., qwerty),
- nie należy ujawniać haseł innym osobom, ani zapisywać ich na kartkach (w notesie, przy komputerze, na monitorze, pod klawiaturą); jeśli zaistnieje sytuacja ujawnienia hasła osobie trzeciej, należy je natychmiast zmienić,
- pracownicy obowiązani są do zachowania hasła w tajemnicy, nawet po utracie przez nie ważności,
- nie można używać takich samych haseł w serwisach internetowych, jak w systemie komputerowym w jednostce,
- jedno hasło nie może być używane jako zabezpieczenie do różnych systemów,
- zabronione jest generowanie haseł, w których jeden z członów zawsze pozostaje niezmienny, a drugi zmieniany jest według określonego wzorca (np. styczeń 2018, luty2018, marzec2018 itd.).

4. Zabezpieczenie dokumentacji papierowej

- każdy pracownik ma obowiązek stosować się do polityki czystego biurka. Pod pojęciem polityki czystego biurka rozumie się obowiązek zabezpieczenia dokumentów i nośników danych przed kradzieżą, lub przed dostępem osób nieupoważnionych. W miarę możliwości stosuje się zamykane szafy i biurka, a w przypadku ich braku zamykane na klucz pomieszczenie. Politykę czystego biurka należy stosować po godzinach pracy, a także podczas chwilowej nieobecności w pracy,
- dokumenty papierowe i wydruki obowiązkowo należy niszczyć w niszczarkach. Zakazuje się: wyrzucania niezniszczonych dokumentów na śmietnik, porzucania ich na zewnątrz lub zostawiania w niezabezpieczonym pomieszczeniu.

5. Wynoszenie nośników danych poza obszar przetwarzania

- pracownicy jednostki nie mogą wynosić na zewnątrz jednostki wymiennych nośników informacji zawierających dokumenty służbowe, w tym dane osobowe, bez zgody pracodawcy,
- w przypadku zgody pracodawcy dane osobowe, które zostają wyniesione poza jednostkę należy zaszyfrować,
- użytkownicy służbowego sprzętu mobilnego, tj. komputerów przenośnych, smartfonów, tabletów, dysków przenośnych i pendrive-ów wynoszonych za zgodą pracodawcy poza obszar organizacji, są zobowiązani do przestrzegania zasad bezpieczeństwa, tj. stosuje się szyfrowanie dysków oraz używa mechanizmów uwierzytelniania,
- sprzęt mobilny w miarę możliwości powinien być wyposażony w oprogramowanie umożliwiające jego zdalny nadzór, blokowanie dostępu oraz czyszczenie zawartości,

- przewożenie dokumentacji papierowej musi odbywać się w bezpieczny sposób, np. należy korzystać ze specjalnej torby (teczki) do tego celu, lub z zaufanych firm kurierskich,
- jeśli przewiezienie dokumentów zawierających dane osobowe zostało powierzone pracownikowi, musi on w należyty i staranny sposób zabezpieczyć dokumenty przed kradzieżą lub zagubieniem,
- jeśli chcemy przekazać nośniki zawierające dane osobowe poza obszar przetwarzania należy zastosować odpowiednie środki bezpieczeństwa: powiadomić adresata o przesyłce, zaszyfrować dane, a hasło do ich odczytania przekazać inną drogą, lub zastosować koperty depozytowe oraz nadać przesyłkę przez kuriera.

6. Korzystanie ze służbowej poczty elektronicznej

- Przesyłanie danych osobowych mailem poza jednostkę odbywa się tylko przez upoważnione do tego osoby. W celu wysłania danych osobowych pocztą elektroniczną należy plik spakować, zaszyfrować oraz opatrzyć hasłem zgodnym z polityką haseł. Hasło należy przekazać odbiorcy inną drogą (telefonicznie lub smsem),
- należy dołożyć wszelkiej staranności przy wysyłce dokumentów z danymi osobowymi, poprzez kilkukrotne sprawdzenie poprawności adresu odbiorcy oraz stosowanie potwierdzenie odbioru,
- ZABRANIA SIĘ: otwierania podejrzanych załączników w mailach (.zip, .xlsm, .pdf, .exe) oraz klikania w hiperlinki, ponieważ wiąże się to z bardzo wysokim ryzykiem infekcji komputera i utraty danych. Podejrzane wiadomości e-mail należy zgłaszać informatykowi (ASI),
- poczty służbowej nie należy używać do spraw prywatnych. Obowiązuje zakaz wysyłania wiadomości e-mail z poczty służbowej na prywatne adresy pocztowe pracowników lub innych osób. Poczty służbowej nie należy łączyć lub przekierowywać na prywatną skrzynkę,
- wysyłając wiadomość do wielu adresatów używa się pola UDW – ukryte do wiadomości,
- służbowej poczty mailowej nie można używać w celu rozpowszechniania treści o charakterze obraźliwym lub niemoralnym,
- użytkownik nie ma prawa bez zgody pracodawcy wysyłać za pośrednictwem poczty mailowej wiadomości, które zawierają dane osobowe dotyczące: pracodawcy, jego pracowników, klientów, kontrahentów,
- każdy użytkownik zobowiązany jest do skanowania programem antywirusowym plików, które wprowadza z dysków zewnętrznych. Obowiązuje zakaz wyłączania systemu antywirusowego, podczas gdy przetwarzamy dane osobowe w systemie informatycznym. Podczas stwierdzenia zainfekowania systemu należy natychmiast poinformować o tym fakcie informatyka.

7. Korzystanie z Internetu

- Internetu należy używać tylko w sprawach służbowych;
- każdy, kto korzysta z Internetu ponosi odpowiedzialność za szkody, które powoduje oprogramowanie instalowane z Internetu;
- zabronione jest zgrywanie na dysk twardy komputera i korzystanie z nielegalnych programów,
- zabrania się korzystania ze stron, które mają charakter hackerski, lub zawierają treści niedozwolone (np. hazardowe lub pornograficzne). Strony te często są zainfekowane i mają automatycznie zainstalowane szkodliwe oprogramowanie, które może zniszczyć zasoby znajdujące się w komputerze użytkownika,
- nie należy używać w przeglądarce opcji autouzupełniania formularzy zapamiętywania haseł,
- gdy używamy szyfrowanego połączenia w przeglądarce, każdorazowo należy sprawdzić, czy pojawia się ikona "kłódki", a adres rozpoczyna się od „https",
- szczególną uwagę należy zwrócić, gdy pojawia się podejrzane żądanie lub prośba logowania na stronę (bank, portal społecznościowy, e-sklep, poczta mailowa). Podejrzane powinno wydać się również, gdy strona wymaga podania loginu, hasła, PIN-u, numeru karty płatniczej przez Internet. Podawanie takich informacji jest zabronione zwłaszcza, gdy dokonujemy płatności przez stronę internetową banku.

8. Incydenty związane z ochroną danych osobowych

- niezwłocznie i natychmiastowo należy powiadomić o zdarzeniu pracodawcę (nawet w przypadku, gdy istnieje tylko podejrzenie naruszenia ochrony danych osobowych). W szczególności, gdy zauważono nieprawidłowe: zabezpieczenie pomieszczeń, dokumentów i urządzeń, sprzętu IT i oprogramowania; lub gdy nie zostały zachowane zasady bezpieczeństwa wyszczególnione w niniejszej polityce,
- incydenty i zdarzenia, o których należy powiadamiać to: zewnętrzne zdarzenia losowe (pożary, kradzieże, zalania, utrata łączności), wewnętrzne zdarzenia losowe (awarie sprzętu IT, pomyłki informatyków lub samych użytkowników, zgubienie danych) i umyślnie spowodowane incydenty (kradzież lub wyciek danych osobowych, ujawnienie informacji osobom nieupoważnionym, świadome niszczenie danych lub dokumentów oraz działanie wirusów i szkodliwego oprogramowania),
- w szczególności należy reagować, gdy:
  - ✓ zauważymy ślady na drzwiach wskazujące na próbę włamania i kradzieży,
  - ✓ niszczona jest dokumentacja zawierająca dane osobowe bez użycia niszczarki,
  - ✓ w jednostce znajdują się osoby zachowujące się w podejrzany sposób,
  - ✓ otwarte pozostają drzwi do szaf i pomieszczeń z danymi osobowymi,
  - ✓ ustawienia monitorów wskazują na możliwość wglądu osób nieupoważnionych,

- ✓ dane osobowe są wynoszone na zewnątrz jednostki (w wersji papierowej i elektronicznej),
- ✓ udostępniane są dane osobowe osobom nieupoważnionych,
- ✓ odbywają się próby wyłudzenia danych osobowych przez telefon,
- ✓ dochodzi do kradzieży lub zagubienia komputerów i innego typu sprzętu, który zawiera dane osobowe,
- ✓ otrzymujemy maila z próbą wyłudzenia hasła i loginu,
- ✓ zauważymy działania wirusa w komputerze,
- ✓ zaobserwujemy zapisane hasła w pobliżu komputera.

9. Poufność

- osoba przetwarzająca dane osobowe jest zobowiązana do przetwarzania danych osobowych tylko w zakresie i celu, który został przewidziany w drodze powierzenia jej przez pracodawcę zadań. Użytkownik przetwarzający dane musi zachować tajemnicę danych osobowych do których ma wgląd i dostęp, w związku z obowiązkami, jakie nałożył na niego pracodawca. Dane osobowe nie mogą być wykorzystywane w celach niezgodnych z zakresem powierzonych zadań przez pracodawcę. W tajemnicy należy zachować sposób zabezpieczenia danych osobowych oraz chronić dane przed zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem i dostępem i przetwarzaniem przez osoby do tego nieupoważnione,
- należy przeszkolić pracowników z zasad ochrony danych osobowym. Pracownicy, którzy przeszli szkolenie i zapoznali się z Regulaminem ochrony danych osobowych w jednostce zobowiązani są podpisać oświadczenie o dochowaniu tajemnicy,
- kategorycznie zabrania się przekazywania bezpośrednio lub drogą telefoniczną danych osobowych osobom nieupoważnionym, lub osobom, których tożsamość pozostaje trudna do zweryfikowania, lub gdy osoby nieupoważnione podszywają się pod kogoś innego. Instytucjom i osobom, które nie mogą wykazać jasnej podstawy prawnej do dostępu do danych osobowych, również nie należy przekazywać i ujawniać danych osobowych.

10. Odpowiedzialność pracownika, czynności dyscyplinarne

W sytuacji, gdy nastąpi nieuzasadnione zaniedbanie obowiązków wynikających z regulaminu ochrony danych osobowych w jednostce, będzie to traktowane jako ciężkie naruszenie obowiązków pracowniczych i zasad współpracy. Sprzeczne działania z zobowiązaniami zawartymi w tym dokumencie może zostać uznane przez pracodawcę jako naruszenie przepisów karnych zawartych w Rozporządzeniu o ochronie danych UE z dnia 27.04.2016 r.

VI. AUDYTY

Zgodnie z RODO- do zadań Administratora należy regularne mierzenie, testowanie i ocena skuteczności środków technicznych i organizacyjnych, które mają zapewnić ochronę i bezpieczeństwo przetwarzania danych osobowych. W tym celu należy przeprowadzać regularne audyty w zakresie bezpieczeństwa informacji i ochrony danych osobowych. Za regularne przeprowadzenie audytu odpowiedzialny jest Administrator. W przypadku wyznaczenia w jednostce Inspektora Ochrony Danych (IOD), audyt w imieniu Administratora wykonuje Inspektor Ochrony Danych.

Celem audytu jest uzyskanie potwierdzenia, że wewnętrzne uregulowania oraz funkcjonujący system zabezpieczeń gwarantują odpowiedni poziom bezpieczeństwa danych osobowych i informacji. Celem drugorzędnym jest dostarczenie kierownictwu obiektywnych analiz i ocen w badanym obszarze.

Audyt w zakresie bezpieczeństwa informacji i ochrony danych osobowych przeprowadza się co najmniej z roczną częstotliwością.

VII. Wykaz załączników:

1. wykaz zbiorów danych osobowych + (RCPD),
2. wzory klauzul informacyjnych,
3. wzór umowy powierzenia,
4. ewidencja umów powierzenia,
5. arkusz analizy ryzyka, lista aktywów, wykaz zagrożeń, wykaz zabezpieczeń,
6. wzór upoważnienia do przetwarzania danych osobowych,
7. ewidencja osób upoważnionych do przetwarzania danych osobowych,
8. formularz rejestracji incydentu,
9. wzór oświadczenia o dochowaniu poufności,
10. ewidencja oświadczeń o dochowaniu poufności,

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH	
Nazwa i dane kontaktowe przetwarzającego	
Nazwa	**Urząd Gminy w Starej Dąbowie**
Adres	**Stara Dąbrowa 20** **73-112 Stara Dąbrowa**
Email	ug@staradabrowa.pl
Telefon	(+48) 91 573 98 20
Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	Bartosz Kaniuk
Adres	-
Email	bkaniuk@proinspektor.pl
Telefon	579 979 237

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji, Rejestr czynności przetwarzania danych osobowych

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
L.P.	Nazwisko i Imię pracownika	Zajmowane stanowisko	Numer pokoju	Nazwa przetwarzanego zbioru danych (kategorii osób, których dane dotyczą)	Symbol klasyfikacyjny z Jednolitego Rzeczowego Wykazu Akt	Podstawa prawna przetwarzania zbioru	Cel przetwarzania	Kategorie oraz opis przetwarzanych danych (wymienić)	Kategorie odbiorców którym udostępniono dane lub zamierza się udostępnić (w tym państw trzecich)	Planowane usunięcie poszczególnych danych (instrukcja kancelaryjna)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (wymienić)	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
													Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
1.														
2.														
3.														
4.														
5.														

6.														

Załącznik nr do Polityki Bezpieczeństwa Informacji -Rejestr czynności przetwarzania danych osobowych

Lista pracowników Urzędu Gminy w Stara Dąbrowa			
L.P.	Nazwisko	Imię	Stanowisko
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

Załącznik nr 2a do Polityki Bezpieczeństwa Informacji
– Klauzula ogólna

INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH

Administrator danych osobowych

Administratorem Państwa danych osobowych jest Wójt Gminy Stara Dąbrowa z siedzibą w Urzędzie Gminy, Stara Dąbrowa 20, 73-112 Stara Dąbrowa. Kontakt jest możliwy za pomocą telefonu: (+48) 91 573 98 20, adresu e-mail: ug@staradabrowa.pl

Inspektor Ochrony Danych

Inspektorem Ochrony Danych jest Bartosz Kaniuk, z którym w sprawach ochrony swoich danych osobowych możecie się Państwo kontaktować przez telefon: +48 579 979 237; adres e-mail: bkaniuk@proinspektor.pl lub pisemnie na adres Gminy.

Cel i podstawa przetwarzania

Państwa dane osobowe przetwarzane będą na podstawie:

a) wypełnianie obowiązku prawnego w związku z realizowaniem zadań przez Gminę,

b) wykonywanie zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,

c) wyrażonej zgody na przetwarzanie swoich danych osobowych w jednym lub w większej liczbie określonych celów,

d) umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

Odbiorcy danych osobowych

Odbiorcami do których mogą być przekazane Państwa dane osobowe będą strony i uczestnicy postępowań, lub organy właściwe do załatwienia wniosku na mocy przepisów prawa, którym Wójt Starej Dąbrowy Państwa wniosek przekazał.

Odrębną kategorią odbiorców, którym mogą być ujawnione Państwa dane są podmioty, które przetwarzają dane osobowe w imieniu i na zlecenie Administratora, na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (np. usługa serwisowa systemów informatycznych).

Okres przechowywania danych

Państwa dane osobowe będą przetwarzane przez okres niezbędny do realizacji wskazanego w pkt. 3 celu przetwarzania, w tym również obowiązku archiwizacyjnego wynikającego z przepisów prawa.

Prawa osób, których dane dotyczą

Przysługuje Państwu prawo do:

a) dostępu do treści danych oraz ich sprostowania,

b) usunięcia danych, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa, lub w ramach sprawowania władzy publicznej,

c) ograniczenia przetwarzania danych lub wniesienia sprzeciwu wobec ich przetwarzania,

d) cofnięcia zgody, w przypadku, w którym przetwarzanie Państwa danych odbywa się na podstawie udzielonej zgody,

e) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych narusza przepisy prawa.

STOPKA E-MAIL:

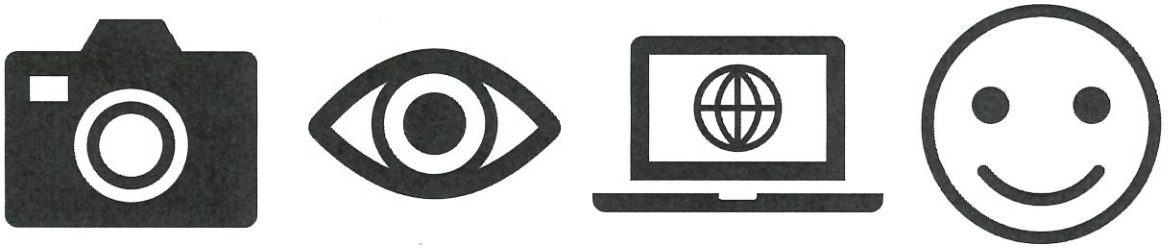
Administratorem Państwa danych osobowych jest Wójt Gminy Stara Dąbrowa. Wszelkie informacje w zakresie ochrony danych osobowych dostępne są na stronie http://bip.staradabrowa.pl/strony/menu/2.dhtml.

Załącznik nr 2b do Polityki Bezpieczeństwa Informacji
– Klauzula ogólna, stopka e-mail

STOPKA E-MAIL:

Administratorem Państwa danych osobowych jest Wójt Gminy Stara Dąbrowa.
Wszelkie informacje w zakresie ochrony danych osobowych dostępne są na stronie www.staradabrwa.pl (https://www.staradabrowa.pl/strony/menu/192.dhtml).

Załącznik nr 2c do Polityki Bezpieczeństwa Informacji
– Klauzula impreza otwarta



UWAGA

SZANOWNI PAŃSTWO, NA IMPREZIE/WYDARZENIU/SPOTKANIU* BĘDĄ ROBIONE ZDJĘCIA. IMPREZĄ CHCEMY SIĘ POCHWALIĆ, DLATEGO ZDJĘCIA UMIEŚCIMY NA NASZEJ STRONIE INTERNETOWEJ. JEŻELI SIĘ NA TO NIE ZGADZASZ, POINFORMUJ NAS O TYM.

Administratorem danych jest **Urząd Gminy w Starej Dąbowie, Stara Dąbrowa 20, 73-112 Stara Dąbrowa**. Udzieloną zgodę możesz wycofać w każdym momencie. Pełna treść informacji związanych z ochroną danych osobowych dostępna jest na naszej stronie internetowej www.staradabrowa.pl (*https://www.staradabrowa.pl/strony/menu/192.dhtml*) oraz w sekretariacie Urzędu Gminy.

Załącznik nr 2d do Polityki Bezpieczeństwa Informacji
– Klauzula informacyjna, rekrutacja

KLAUZULA INFORMACYJNA - REKRUTACJA

Przekazywane przez Panią/Pana dane osobowe są administrowane przez **Urząd Gminy w Starej Dąbrowie, 73-112 Stara Dąbrowa 20.**
Pani/Pana dane osobowe zamieszczone w CV oraz liście motywacyjnym będą przetwarzane w celu przeprowadzenia i rozstrzygnięcia rekrutacji na stanowisko, którego dotyczy ogłoszenie, jak również w celu przeprowadzenia i rozstrzygnięcia przyszłych rekrutacji, jeżeli udzielą Państwo na to stosownej zgody.

Inspektorem ochrony danych w **Urzędzie Gminy w Starej Dąbrowie** jest Bartosz Kaniuk, z którym kontaktować się można pod adresem e-mail: bkaniuk@proinspektor.pl.
Pani/Pana dane osobowe będą przechowywane, aż do czasu zakończenia procesu rekrutacji (za wyjątkiem CV wybranego kandydata), chyba że udzielili Państwo zgody na przetwarzanie danych również na potrzeby przyszłych rekrutacji, wówczas Państwa dane osobowe będą przechowywane, przez okres 3 miesięcy od dnia przesłania CV.

Przysługuje Pani/Panu prawo żądania dostępu do danych osobowych dotyczących Pani/Pana osoby, ich sprostowania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec ich przetwarzania oraz cofnięcia wyrażonej zgody w dowolnym momencie.
Przysługuje Pani/Panu prawo do złożenia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
Podanie przez Panią/Pana danych osobowych jest dobrowolne, przy czym niezbędne do wzięcia udziału w procesie rekrutacji.
Decyzje dotyczące przeprowadzenia oraz rozstrzygnięcia procesu rekrutacji nie będą podejmowane w sposób zautomatyzowany.

Dodatek do CV

Prosimy o zawarcie w ramach CV kandydatów do pracy następujące treści klauzul:

*„Wyrażam zgodę na przetwarzanie przez **Urząd Gminy w Starej Dąbrowie** moich danych osobowych w zakresie zawartym w niniejszym CV/liście motywacyjnym w celu przeprowadzenia i rozstrzygnięcia rekrutacji. Oświadczam, że zapoznałem się z informacją w zakresie ochrony danych osobowych".*

Brak takiej klauzuli spowoduje, że Państwa CV nie zostanie rozpatrzone i zostanie usunięte.

Jeśli wyrażają Państwo wolę, aby złożone przez Państwa CV/listy motywacyjne były wykorzystywane przez administratora w kolejnych rekrutacjach, prosimy o zawarcie klauzuli o treści:

„Wyrażam zgodę na przetwarzanie moich danych osobowych przez ***Urząd Gminy w Starej Dąbrowie*** w zakresie wskazanym w niniejszym CV/liście motywacyjnym przez okres 3 miesięcy w celu przeprowadzenia i rozstrzygnięcia kolejnych rekrutacji prowadzonych przez tego pracodawcę. *Oświadczam, że zapoznałem się z informacją w zakresie ochrony danych osobowych*".

Załącznik nr 2e do Polityki Bezpieczeństwa Informacji – Klauzula informacyjna, ewidencja 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	Administratorami są: 1. **Wójt Gminy Stara Dąbrowa, Stara Dąbrowa 20, 73-112 Stara Dąbrowa, tel. (+48) 91 573 98 20, ug@staradabrowa.pl** – w zakresie rejestracji danych w rejestrze PESEL oraz prowadzenia i przetwarzania danych w rejestrze mieszkańców oraz przechowywanej przez Wójta 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	Z administratorem – **Wójtem** można się skontaktować pisemnie na adres siedziby administratora Z administratorem – Ministrem Cyfryzacji można się skontaktować poprzez adres email iod@mc.gov.pl, formularz kontaktowy pod adresem https://www.gov.pl/cyfryzacja/kontakt, lub pisemnie na adres siedziby administratora. Z administratorem – Ministrem Spraw Wewnętrznych i Administracji można się skontaktować poprzez adres mail iod@mswia.gov.pl, formularz kontaktowy pod adresem https://www.gov.pl/web/mswia/formularz-kontaktowy lub pisemnie na adres siedziby administratora.
DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH	Administrator – **Wójt** wyznaczył inspektora ochrony danych, z którym może się Pani / Pan skontaktować poprzez adres mailowy **bkaniuk@proinspektor.pl** Administrator – Minister Cyfryzacji wyznaczył inspektora ochrony danych, z którym może się Pani / Pan skontaktować poprzez email iod@mc.gov.pl, lub pisemnie na adres siedziby administratora. Administrator – Minister Spraw Wewnętrznych i Administracji wyznaczył inspektora ochrony danych, z którym może się Pani / Pan skontaktować poprzez email iod@mswia.gov.pl lub pisemnie na adres siedziby administratora. Z każdym z wymienionych inspektorów 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 przepisem szczególnym ustawy; • przez Wójta/Burmistrza/Prezydenta miasta - w celu wprowadzenia

Załącznik nr 2e do Polityki Bezpieczeństwa Informacji – Klauzula informacyjna, ewidencja 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)

	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 administracyjnoprawny 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**-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.

Załącznik nr 2e do Polityki Bezpieczeństwa Informacji – Klauzula informacyjna, ewidencja 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)

	Pani/Pana dane **Wójt** 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 Pani/Pana danych oraz prawo żądania ich sprostowania, a także danych osób, nad którymi sprawowana jest prawna opieka, np. danych dzieci.
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 Telefon: 22 531 03 00
ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH	Pani / Pana dane do rejestru PESEL wprowadzane są przez następujące organy: – kierownik urzędu stanu cywilnego sporządzający akt urodzenia, małżeństwa i zgonu oraz wprowadzający do tych aktów zmiany, a także wydający decyzję o zmianie imienia lub nazwiska, – organ gminy dokonujący rejestracji obowiązku meldunkowego, – organ gminy wydający lub unieważniający dowód osobisty, – wojewoda lub konsul RP wydający lub unieważniający paszport, – wojewoda lub minister właściwy do spraw wewnętrznych dokonujący zmian w zakresie nabycia lub utraty obywatelstwa polskiego. Rejestr mieszkańców zasilany jest danymi z rejestru PESEL.
INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH	Obowiązek podania danych osobowych wynika z ustawy o ewidencji ludności (art. 8 i 10 ustawy). W przypadku działania na wniosek odmowa podania danych przez ich posiadacza skutkuje nie zrealizowaniem żądania nadania lub zmiany numeru PESEL, zameldowania, wymeldowania, rejestracji wyjazdu, powrotu lub udostępnienia danych. Nie wykonanie obowiązku meldunkowego przez cudzoziemców nie będących obywatelami państwa członkowskiego UE lub członkami ich rodzin zagrożone jest karą grzywny.

Załącznik nr 2 f do Polityki Bezpieczeństwa Informacji
– Klauzula informacyjna, ZFŚS

INFORMACJA WARSTWOWA

Poniższy akapit należy wkleić do wniosku (oświadczenia), który jest podpisany przez osobę składającą.

Administratorem danych osobowych jest **Urząd Gminy w Starej Dąbowie, Stara Dąbrowa 20 73-112 Stara Dąbrowa ,tel. +48 91 573 98 20.** Dane przetwarzane są w celu realizacji świadczeń socjalnych przysługujących z Zakładowego Funduszu Świadczeń Socjalnych. Pełna treść informacji w zakresie ochrony danych osobowych dostępna jest na stronie internetowej: www.staradabrowa.pl. (https://www.staradabrowa.pl/strony/menu/192.dhtml).

Oświadczam, że mi i członkom mojej rodziny znane są informacje wynikające z art. 13 i 14 RODO w zakresie ochrony danych osobowych oraz Regulaminu Zakładowego Funduszu Świadczeń Socjalnych.

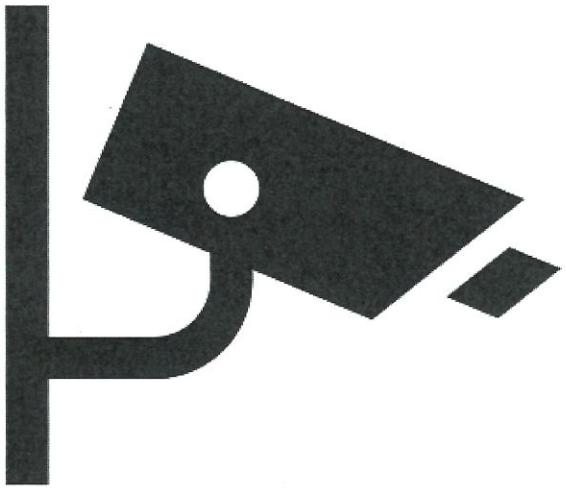
Poniższa pełna treść klauzuli informacyjnej powinna zostać umieszczona we wskazanym miejscu.

Zgodnie z art. 13 ogólnego 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 – dalej w skrócie zwane RODO oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. Poz. 1000) informuję:

1. Administratorem Pani/Pana danych osobowych **Urząd Gminy w Starej Dąbowie, Stara Dąbrowa 20, 73-112 Stara Dąbrowa.** Z Administratorem można kontaktować się pisemnie, za pomocą poczty tradycyjnej pod wskazanym adresem lub telefonicznie pod numerem **telefonu +48 91 573 98 20.**
2. Kontakt z Inspektorem Danych Osobowych – e-mail: bkaniuk@proinspektor.pl, telefon: 579 979 237.
3. Dane osobowe przetwarzane są w celu realizacji zadań Administratora związanych z pomocą socjalną. Podstawa prawna: ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (Dz. U. Dz.U. 1994 nr 43 poz. 163 z późn. zm.), oraz Regulamin gospodarowania środkami zakładowego funduszu świadczeń socjalnych wprowadzony Zarządzeniem Nr 38/2019 Wójta Gminy Stara Dąbrowa z dnia 05 kwietnia 2019 roku.
4. Odbiorcami Pani/Pana danych osobowych będą wyłącznie upoważnieni pracownicy oraz podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa.
5. Dane osobowe są przechowywane przez okres nie dłuższy niż jest to niezbędne w celu przyznania świadczeń oraz ustalenia ich wysokości, a także przez okres dochodzenia do nich praw lub roszczeń.
6. Posiada Pani/Pan prawo do dostępu do treści Pani/Pana danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawa do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych osobowych, prawo do cofnięcia zgody.
7. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa, w pozostałym zakresie jest dobrowolne.

Załącznik nr 2 g do Polityki Bezpieczeństwa Informacji
– Klauzula informacyjna, monitoring

OBSZAR MONITOROWANY



Monitoring stosowany jest przez **Urząd Gminy w Starej Dąbowie, Stara Dąbrowa 20, 73-112 Stara Dąbrowa** w celu ochrony mienia i osób. Monitoring swoim zasięgiem obejmuje pomieszczenia budynku oraz teren wokół budynku. Nagrania monitoringu przechowywane są przez ….. dni. Pełna treść informacji związanych z ochroną danych osobowych dostępna jest https://www.staradabrowa.pl/strony/menu/192.dhtml.

Załącznik nr 2 g do Polityki Bezpieczeństwa Informacji
– Klauzula informacyjna, monitoring

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego Rozporządzenia PE i Rady (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 oraz uchylenia dyrektywy 95/46/WE (dalej) RODO informuję, że:

1. Administratorem danych osobowych jest Urząd Gminy w Starej Dąbowie z siedzibą w Starej Dąbrowie 20, 73-112 Stara Dąbrowa, który reprezentuje Wójt. Kontakt jest możliwy pod numerem telefonu (+48) 91 573 98 20
2. W przypadku pytań lub wątpliwości kontaktuj się z Inspektorem Ochrony Danych pod adresem e-mail: bkaniuk@proinspektor.pl lub numerem telefonu +48 579 979 237.
3. Dane osobowe w postaci wizerunku zarejestrowanego przez monitoring przetwarzane będą w celu zapewnienia bezpieczeństwa osób i mienia na podstawie przepisów prawa.
4. Nagrania z monitoringu nie będą nikomu udostępniane, chyba że zajedzie taka potrzeba, wynikająca z przepisów prawa, np. wniosek policji.
5. Nagrania monitoringu będą przechowywane przez ..... dni.
6. Posiadasz prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem - w granicach określonych w przepisach prawa.
7. Posiadasz prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, jeżeli uznasz, że przetwarzanie danych osobowych narusza przepisy RODO.
8. Dane będą przetwarzane w sposób zautomatyzowany – kamery monitoringu nagrywają obraz w sposób ciągły, po upływie ..... dni zapis jest automatycznie nadpisywany.

Instrukcja:

- Pierwsza warstwa – obiekt monitorowany – umieszczona przed wejściem w obszar monitorowany,
- Druga warstwa – klauzula informacyjna – dostępna w wyznaczonym miejscu.

Załącznik nr 2 h do Polityki Bezpieczeństwa Informacji
– Klauzula informacyjna, podatki

KLAUZULA INFORMACYJNA
PODATKI I OPŁATY

Zgodnie z art. 13 rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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), zwanego dalej „ogólnym rozporządzeniem o ochronie danych osobowych", informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Wójt Gminy Stara Dąbrowa z siedzibą w Starej Dąbrowie 20, 73-112 Stara Dąbrowa.

2. Dane kontaktowe Inspektora ochrony Danych – e-mail: bkaniuk@proinspektor.pl, tel.:608 442 652

3. Pani/Pana dane osobowe będą przetwarzane celach podatkowych na podstawie art. 6 ust 1 lit. a, b i c ogólnego rozporządzenia o ochronie danych osobowych.

4. Odbiorcami Pani/Pana danych osobowych będzie organ podatkowy.

5. Pani/Pana dane osobowe będą przechowywane przez okres 10 lat.

6. Posiada Pani/Pan prawo do: żądania od Administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia praw.

7. Ma Pani/Pan prawo do wniesienia skargi do organu nadzorczego.

9. Podanie danych osobowych jest obligatoryjne na mocy przepisu prawa, jednakże niepodanie danych w zakresie wymaganym przez administratora może skutkować odmową podjęcia współpracy przez Administratora.

Załącznik nr 2 i do Polityki Bezpieczeństwa Informacji – Klauzula informacyjna, Sesja Rady Gminy

UWAGA

ZGODNIE Z OBOWIĄZUJĄCYMI PRZEPISAMI PRAWA, OBRADY RADY GMINY SĄ TRANSMITOWANE I UTRWALANE ZA POMOCĄ URZĄDZEŃ REJESTRUJĄCYCH OBRAZ I DŹWIĘK. NAGRANIA OBRAD SĄ UDOSTĘPNIANE W BIULETYNIE INFORMACJI PUBLICZNEJ I NA STRONIE INTERNETOWEJ GMINY ORAZ W INNY SPOSÓB ZWYCZAJOWO PRZYJĘTY.

Administratorem danych jest Gmina Stara Dąbrowa, z siedzibą w Starej Dąbrowie 20, 73-112 Stara Dąbrowa. Podstawą przetwarzania danych jest Art. 6 ust 1, lit. c i e 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) (Tekst mający znaczenie dla EOG). Pełna treść informacji związanych z ochroną danych osobowych dostępna jest na stronie internetowej gminy www.staradabrowa.pl.

Załącznik nr 2 j do Polityki Bezpieczeństwa Informacji
– Klauzula zgody

..... Miejscowość ,.....

Imię i nazwisko pracownika data

KLAUZULA ZGODY

Zgodnie z art. 6 ust.1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. wyrażam zgodę na przetwarzanie moich danych osobowych:

- do celów kontaktowych,
- w celu budowania pozytywnego wizerunku Administratora poprzez publikowanie mojego wizerunku na stronie internetowej gminy: www.staradabrowa.pl
- w celu ochrony mienia i osób poprzez monitoring wizyjny zainstalowany w jednostce.

Oświadczam również, że zostały mi przekazane wszelkie informacje dotyczące administratora danych, wynikające z art. 13 RODO.

(data i podpis pracownika)

Załącznik nr 3a do Polityki Bezpieczeństwa Informacji
Umowa powierzenia przetwarzania danych osobowych – wzór uproszczony

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w/we ..... w dniu ..... r. pomiędzy:
..... z siedzibą w ....., zarejestrowaną/
ym w ..... pod numerem KRS .....,
posiadającą/ym numer NIP ..... oraz numer REGON .....,
reprezentowaną/ym przez: .....,
zwaną/ym dalej Zleceniodawcą, a

..... z siedzibą w ....., zarejestrowaną/
ym w ..... pod numerem KRS .....,
posiadającą/ym numer NIP ..... oraz numer REGON .....,
reprezentowaną/ym przez: .....,
zwaną/ym dalej Zleceniobiorcą.

§ 1
Oświadczenia stron

1. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w zakresie i celu objętym niniejszą umową.

2. Zleceniodawca oświadcza, że jest administratorem danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1662, dalej zwana ustawą), które przetwarza zgodnie z obowiązującymi przepisami prawa. Zleceniodawca oświadcza ponadto, że zawiera niniejszą umowę w celu bezpośrednio związanym z jego działalnością gospodarczą lub zawodową.

3. Zleceniobiorca oświadcza, iż dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami ustawy oraz 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. Nr 100, poz. 1024, dalej zwane rozporządzeniem).

§ 2
Zakres i cel przetwarzania danych osobowych

1. Zleceniobiorca może przetwarzać dane osobowe przekazane przez Zleceniodawcę wyłącznie w zakresie i w celu określonych w niniejszej umowie.
2. Dane osobowe będą przetwarzane przez Zleceniobiorcę tylko i wyłącznie w celu *[wskazać cel przetwarzania]*.
3. Zakres przetwarzania obejmuje następujące dane osobowe *[wskazać zakres przetwarzania]*
4. Poprzez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

§ 3

Zobowiązania podmiotu, któremu powierzono przetwarzanie danych osobowych

1. Zleceniobiorca zobowiązuje się przed przystąpieniem do przetwarzania powierzonych przez Zleceniodawcę danych wdrożyć i utrzymywać przez czas przetwarzania wszelkie środki i zabezpieczenia związane z przetwarzaniem danych, zgodnie z wymaganiami ustawy oraz rozporządzenia.

2. Zleceniobiorca może powierzać przetwarzanie powierzonych przez Zleceniodawcę danych osobowych innym podmiotom, takim jak: *[wskazać określone podmioty]*.

3. Zleceniobiorca odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez Zleceniobiorcę powierzonych danych osobowych.

4. Zleceniobiorca nie jest odpowiedzialny za udostępnienie powierzonych danych osobowych osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem tych danych osobowych w przypadku, gdy przyczyną powyższego jest działanie bądź zaniechanie Zleceniodawcy

§ 4

Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy ustawy oraz powiązanych z nią aktów wykonawczych, a także rozporządzenia i kodeksu cywilnego.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

UMOWA POWIERZENIA
PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w ..... dnia ..... pomiędzy:

.....
reprezentowaną przez:

.....

dalej jako **"Administrator"**,

a

.....

reprezentowaną przez:

.....

dalej jako **"Podmiot Przetwarzający"**.

Administrator oraz Podmiot Przetwarzający dalej łącznie jako "**Strony**", a indywidualnie jako "**Strona**".

ZWAŻYWSZY, ŻE:

(A) Administrator jest podmiotem, który decyduje o celach i środkach przetwarzania danych osobowych w rozumieniu przepisu art. 4 pkt 7 Rozporządzenia, a Podmiot Przetwarzający podmiotem, który przetwarza dane osobowe w rozumieniu przepisu art. 4 pkt 8 Rozporządzenia;

(B) Na mocy zawartej przez Strony Umowy Głównej, Administrator zlecił Podmiotowi Przetwarzającemu świadczenie usług, w celu wykonania których Podmiot Przetwarzający będzie w imieniu Administratora dokonywał określonych w niniejszej umowie operacji na danych osobowych;

(C) Stosownie do art. 28 ust. 3 Rozporządzenia, przetwarzanie danych osobowych przez Podmiot Przetwarzający w imieniu Administratora, odbywa się na podstawie umowy, która wiąże Podmiot Przetwarzający i Administratora, określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa Administratora.

Strony postanowiły, co następuje:

1. DEFINICJE

W niniejszej Umowie, następujące terminy mają znaczenie zdefiniowane poniżej:

1.1. „**Umowa**" – oznacza niniejszą umowę powierzenia przetwarzania danych osobowych;

1.2. „**Umowa Główna**" – oznacza umowę brokerską zawartą dnia 08.09.2016r.

1.3. „**Rozporządzenie**" – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

2. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

2.1. Administrator, na podstawie art. 28 ust. 3 Rozporządzenia, powierza Podmiotowi Przetwarzającemu dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2.2. Podmiot Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, z przepisami prawa Unii Europejskiej (w szczególności z przepisami Rozporządzenia) oraz krajowymi przepisami prawa.

3. ZAKRES I CEL PRZETWARZANIA

Strony postanawiają następująco określić zakres i cel przetwarzania danych osobowych przez Podmiot Przetwarzający:

Przedmiot przetwarzania	Dane osobowe powierzone do przetwarzania Podmiotowi Przetwarzającemu, w związku ze świadczeniem usług na rzecz Administratora, na podstawie zawartej przez Strony Umowy Głównej
Czas przetwarzania	Okres obowiązywania Umowy Głównej
Charakter przetwarzania	Przetwarzanie danych w systemach IT i w formie papierowej obejmujące następujące operacje: utrwalanie, organizowanie, porządkowanie, przechowywanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, dopasowywanie lub łączenie, ograniczanie, niszczenie.
Cel przetwarzania	Realizacja postanowień Umowy Głównej, w szczególności obejmującej wykonywanie czynności brokerskich na rzecz Administratora, takimi jak analizę aktualnego stanu ochrony ubezpieczeniowej, przygotowywanie i przedstawianie ofert ubezpieczeniowych na rzecz Administratora, wsparcie w procesie likwidacji szkód na rzecz Administratora, przygotowywanie dokumentacji ubezpieczeniowej,
Rodzaj danych osobowych	Imię i nazwisko, miejsce pracy, NIP, Regon, nr PESEL, nr dowodu osobistego, nr prawa jazdy, adres zamieszkania, informacje o stanie zdrowia, informacje o wysokości wynagrodzenia, adres e-mail, nr telefonu, posiadane ubezpieczenie, stan cywilny, dane opiekuna prawnego osoby niepełnoletniej,
Kategorie osób, których dane dotyczą	klienci Administratora, osoby trzecie zgłaszające roszczenia do Administratora, pracownicy klientów Administratora, osoby ubezpieczone, pracownicy Administratora

4. PRAWA I OBOWIĄZKI ADMINISTRATORA

4.1. Administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania przez niego danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami prawa, w tym wymogami Rozporządzenia.

4.2. Administrator, zgodnie z art. 28 ust. 3 lit. h Rozporządzenia, ma prawo przeprowadzania u Podmiotu Przetwarzającego audytów i kontroli, w celu weryfikacji, czy środki zastosowane przez

niego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, spełniają postanowienia niniejszej Umowy, zgodnie z postanowieniami pkt 7 Umowy.

4.3. Administrator ma prawo żądania niezwłocznego, to jest w terminie 7 dni/dnia udostępnienia przez Podmiot Przetwarzający aktualnego rejestru kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w pkt. 6.1 niniejszej Umowy.

5. BEZPIECZEŃSTWO PRZETWARZANIA

5.1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Podmiot Przetwarzający zobowiązuje się wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

5.2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, Podmiot Przetwarzający zobowiązany jest uwzględnić w szczególności ryzyko wiążące się z przetwarzaniem, w tym wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

6. OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO

6.1. Podmiot Przetwarzający prowadzi w formie pisemnej oraz elektronicznej rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, stosownie do postanowień przepisu art. 30 ust. 2 Rozporządzenia.

6.2. Podmiot Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.

6.3. Podmiot Przetwarzający zobowiązuje się zapewnić zachowanie tajemnicy powierzonych danych, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, przez osoby, które upoważnia do przetwarzania danych osobowych, zarówno w trakcie ich zatrudnienia w Podmiocie Przetwarzającym, jak i po jego ustaniu.

6.4. Wraz z zawarciem niniejszej umowy Administrator poleca Podmiotowi Powierzającemu przetwarzanie danych osobowych w celu wskazanym w niniejszej umowie, w odniesieniu do czynności i kategorii danych wskazanych w niniejszej umowie.

6.5. Z zastrzeżeniem pkt 6.6 Umowy, Podmiot Przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy również przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

6.6. Podmiot Przetwarzający może również przetwarzać dane osobowe w zakresie, w jakim obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

6.7. Podmiot Przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.

6.8. Podmiot Przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia.

6.9. Podmiot Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych, zobowiązany jest zgłosić je Administratorowi bez zbędnej zwłoki, nie później jednak niż w ciągu 36 h od stwierdzenia naruszenia. Zgłoszenie powinno uwzględniać co najmniej charakter naruszenia

ochrony danych, w tym miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie.

6.10. Podmiot Przetwarzający, po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Nie dotyczy to sytuacji gdy Podmiot Przetwarzający ma prawo do przetwarzania danych osobowych uzyskanych od Administratora jako odrębny administrator danych, w szczególności w przypadku konieczności ustalenia, dochodzenia lub obrony roszczeń.

7. PRAWO KONTROLI

7.1. Podmiot Przetwarzający umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. W tym celu Administrator może zażądać od Podmiotu Przetwarzającego niezbędnych dokumentów oraz informacji, a także dokonać inspekcji siedziby Podmiotu Przetwarzającego, w godzinach jego działalności.

7.2. Administrator zobowiązany jest poinformować Podmiot Przetwarzający o terminie i zakresie planowanej kontroli, co najmniej na 7 dni przed jej rozpoczęciem.

7.3. W ramach kontroli Podmiot Przetwarzający zobowiązany jest:

a. umożliwić osobom przeprowadzającym kontrolę dostęp do miejsc, w których przetwarza powierzone na podstawie niniejszej umowy dane osobowe,

b. udzielić Administratorowi, wszelkich informacji lub złożyć pisemne wyjaśnienia dotyczące przetwarzania powierzonych danych osobowych, co może obejmować przedstawienie sposobu działania systemów IT oraz przekazanie innych danych niezbędnych do sprawdzenia sposobu i zakresu ochrony danych osobowych przez Podmiot Przetwarzający.

7.4. Kontrolę kończy raport pokontrolny sporządzony na piśmie, podpisany przez upoważnionych przedstawicieli obu Stron.

8. ZASADY PODPOWIERZENIA

8.1. Wraz z zawarciem niniejszej umowy Administrator udziela na rzecz Podmiotu Przetwarzającego ogólnej zgody na dalsze powierzanie przetwarzania danych osobowych. W przypadku gdy Podmiot Przetwarzający dokonuje zmian dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających, informuje o tym Administratora. Administrator ma prawo do wyrażenia sprzeciwu w tym zakresie w terminie 7 dni od dnia poinformowania go przez Podmiot Przetwarzający. Poinformowanie przez Podmiot Przetwarzający może nastąpić poprzez wiadomość elektroniczną wysłaną na adres Administratora: .....

8.2. Podmiot, któremu Podmiot Przetwarzający powierzył przetwarzanie danych osobowych powinien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot Przetwarzający w niniejszej Umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.

8.3. Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązywanie się przez podwykonawcę ze spoczywających na nim obowiązków ochrony danych.

9. ODPOWIEDZIALNOŚĆ PODMIOTU PRZETWARZAJĄCEGO

9.1. Podmiot Przetwarzający odpowiada za szkody spowodowane przetwarzaniem powierzonych mu danych osobowych w przypadku gdy:
   a. nie dopełnił obowiązków, które Rozporządzenia nakłada bezpośrednio na podmioty przetwarzające lub gdy
   b. działał wbrew zobowiązaniom wynikającym z niniejszej Umowy.

9.2. Podmiot Przetwarzający zostanie zwolniony z odpowiedzialności wynikającej z pkt 9.1 Umowy, jeżeli udowodni, że nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

10. CZAS TRWANIA I ROZWIĄZANIE UMOWY

10.1. Niniejsza Umowa zostaje zawarta na czas trwania Umowy Głównej i ulega rozwiązaniu z chwilą rozwiązania Umowy Głównej.

10.2. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot Przetwarzający przetwarza powierzone mu dane osobowe w sposób rażąco sprzeczny z treścią przepisów Rozporządzenia lub niniejszej umowy i nie zaprzestał takiego przetwarzania pomimo pisemnego upomnienia przez Administratora.

11. POUFNOŚĆ

11.1. Strony zobowiązują się zachować w poufności informacje lub materiały dotyczące innej Strony lub działalności przez nią prowadzonej, które znajdą się w ich posiadaniu, w związku z zawarciem lub wykonywaniem Umowy.

11.2. Postanowienie zawarte w pkt 11.1. Umowy nie dotyczy informacji i materiałów, które:
   a. są jawne,
   b. zostały legalnie uzyskane przez Stronę od podmiotów innych niż druga Strona Umowy lub
   c. Strona przekazująca informacje lub materiały wyraziła zgodę na ich ujawnienie osobom trzecim.

12. POSTANOWIENIA KOŃCOWE

12.1. Strony postanawiają, że postanowienia niniejszej umowy zastępują dotychczas wiążące strony postanowienia dotyczące ochrony danych osobowych, w tym w szczególności zawarte w treści Umowy Głównej oraz pełnomocnictwa brokerskiego z dnia 11.09.2015r.

12.2. Niniejsza Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

12.3. Wszelkie zmiany treści niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.

12.4. Jakiekolwiek spory wynikłe w związku z niniejszą Umową oraz jej wykonywaniem będą rozstrzygane przez sąd powszechny właściwy dla siedziby Pozwanego.

12.5. Umowa wchodzi w życie z dnie jej zawarcia i z tą datą zastępuje wszelkie wcześniejsze umowy lub porozumienia Stron dotyczące powierzenia przetwarzania danych osobowych.

Administrator	**Podmiot Przetwarzający**
_____	_____

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji *Ewidencja umów powierzenia*	Sporządził: Data: Strona:

L .p.	Administrator Danych Osobowych (ADO)	Kategoria osób, których dane dotyczą, kategoria danych osobowych, zakres przetwarzanych danych	Numer umowy powierzenia	Data zawarcia / wygaśnięcia umowy	Zakres czynności przetwarzania
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					

ANALIZA RYZYKA	
NAZWA I DANE KONTAKTOWE ADMINISTRATORA	
Nazwa	Urząd Gminy w Starej Dąbrowie
Adres	Stara Dąbrowa 20
E-mail	ug@staradabrowa.pl
Telefon	(+48) 91 573 98 20
INSPEKTOR OCHRONY DANYCH	
Nazwa	Bartosz Kaniuk
E-mail	bkaniuk@proinspektor.pl
Telefon	579 979 237

Ocena ryzyka przeprowadzana jest dla każdego zidentyfikowanego podczas inwentaryzacji aktywa, rozpatruje dwa obszary:
⇧ prawdopodobieństwo wystąpienia zagrożenia i podatność aktywów na zagrożenia;
⇧ skutków potencjalnych zagrożeń;

biorąc pod uwagę następstwa naruszenia lub utraty:
⇧ poufności,
⇧ integralności,
⇧ dostępności,

które mogą nastąpić w wyniku działań:
⇧ umyślnych,
⇧ przypadkowych,
⇧ naturalnych.

Listę potencjalnych i realnych dla Jednostki zagrożeń umieszczono w kolejnej zakładce. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa oraz skutków zdarzeń.

SKALA	PRAWDOPODOBIEŃSTWO / PODATNOŚĆ
1	niskie, odległe, mało realne szanse na zdarzenie - aktywa bardzo dobrze zabezpieczone.
2	może się zdarzyć lub zdarza się sporadycznie - aktywa dostatecznie zabezpieczone.
3	bardzo realne szanse wystąpienia - aktywa słabo lub nie zabezpieczone

SKALA	SKUTEK
1	utrata danych nie spowoduje utrudnień w pracy jednostki lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu.
2	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku jednostki , odtworzenie danych jest możliwe ale pracochłonne.
3	utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne, odtworzenie danych i reputacji będzie trudne i kosztowne.

WARTOŚĆ (R = P x S)	RYZYKO
od 1 do 2	akceptowalne - podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące.

od 3 do 6	opcjonalne - należy zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne.
od 7 do 9	nieakceptowalne - należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc aktywa w bezpieczniejsze miejsce.

Zagrożenie	Opis zagrożenia	
Ataki zewnętrzne	socjotechniczne	
	na infrastrukturę	
	dla sprzętu	

Zagrożenia danych		
Błędy ludzkie		

Załącznik nr 5d do Polityki Bezpieczeństwa Informacji , Analiza Ryzyka- Aktywa

Inwentarz (aktywa)	Grupy (podaktywa)	Uwagi
Infrastruktura		
Pracownicy i współpracownicy		
Zlecenie wykonania usług na zewnątrz		
	Sieć	

Infrastruktura IT		
	Sprzęt komputerowy	
	Nośniki danych	
	Oprogramowanie	
	Telekomunikacja	

Informacje	Informacje	

Jednostka:		Urząd Gminy w Starej Dąbrowie			
Komórka organizacyjna:					
Imiona i Nazwiska zespołu wykonującego analizę:					
Imię i Nazwisko Inspektora Ochrony Danych:		Bartosz Kaniuk			
Utworzono:		28.05.2019 r.			
Aktualizacja:					
Zagrożenie	**Zagrożone aktywa**	**Prawdopodobieństwo (P)**	**Skutek (S)**	**Ryzyko (R)**	***Opis podjętych działań minimalizujących (zabezpieczenia)***
1	2	3	4	5	6
Zalanie					
Powódź					
Pożar (wewnątrz budynku)					
Pożar (na zewnątrz budynku)					
Zagrożenie terrorystyczne					
Katastrofa budowlana					
Brak dostawy prądu					
Brak dostępu do Internetu					
Awaria klimatyzacji					
Awaria systemu ppoż					
Sabotaż wewnętrzny					
Kradzież dokumentów przez osoby upoważnione					
Kradzież dokumentów przez osoby nieupoważnione					
Odejście pracownika do konkurencji					
Kradzież dokumentów przez osoby z zewnątrz					
Kradzież z włamaniem					
Atak hakerski					
Awaria nośników danych					
Brak backupu danych					
Niepowodzenie w odzyskaniu danych z backupu					
Przerwa w dostarczaniu usługi kluczowej					
Awaria u dostawcy usług zewnętrznych (poczta, hosting itd.)					
Bankructwo zewnętrznego dostawcy usług lub towarów					
Niedyspozycyjność osób kluczowych dla działalności					
Kradzież telefonu komórkowego					
Awaria sprzętu sieciowego					
Awaria serwerów					
Awaria oprogramowania					

Kradzież laptopa					
Infekcja złośliwym oprogramowaniem					
Atak socjotechniczny (phishing, telefon)					
nieuprawniony dostęp					
kradzież tożsamości					
Nieuprawniona modyfikacja / usunięcie					
Nieuprawnione kopiowanie danych					
kradzież danych lub nośników					
utrata / kradzież danych dostępowych (hasła, klucze, certyfikaty)					
błąd / awaria oprogramowania					
brak / błędy w wykonywaniu kopii bezpieczeństwa					
udostępnienie danych osobom nieupoważnionym					
fałszowanie danych					
nieprawidlowe / brak procedur niszczenia nośników z danymi					
nieprawidłowe / brak procedur napraw w serwisach zewnętrznych					
nieprzestrzeganie procedur					
pomyłki					
brak świadomości / wiedzy					
błędy projektowe / konfiguracyjne					
brak aktualnej dokumentacji					
nieprawidłowe / brak umowy o współpracy					
nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego					
upadek firmy outsourcingowej lub dostawczej					
awaria łączy telekomunikacyjnych					

Załącznik nr 5f do Polityki Bezpieczeństwa Informacji , Wykaz zabezpieczeń

Typ zabezpieczenia	Zabezpieczenie	Uwagi
Zabezpieczenia zewnętrzne		
Zabezpieczenia informatyczne		
Zabezpieczenia techniczne		
Zabezpieczenia organizacyjne		

Zabezpieczenia fizyczne		

Załącznik nr 5g do Polityki Bezpieczeństwa Informacji , Zalecenia

Zagrożenie do obniżenia	Zabezpieczenie do wdrożenia (nowe zabezpieczenia dodajemy do wykazu zabezpieczeń)	Osoba odpowiedzialna	Ocena wykonania

Załącznik nr 6 do Polityki Bezpieczeństwa Informacji,
Wzór upoważnienia do przetwarzania danych osobowych

....

Imię i Nazwisko Miejscowość, data

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniam Panią/Pana do przetwarzania danych osobowych:

a) w zbiorach papierowych:

1.

2.

3.

4.

5.

...

w zakresie niezbędnym do wykonywania obowiązków pracowniczych w tym: wprowadzania danych, modyfikacji, usuwania, archiwizacji, udostępniania innym upoważnionym podmiotom, wglądu itp..

b) w systemach informatycznych:

....

Pieczęć i podpis pracownika Pieczęć i podpis Administratora

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji , Ewidencja osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych	Sporządził:
	Data:

L .p.	Imię i Nazwisko pracownika	Zajmowane stanowisko	Data udzielonego upoważnienia	Zakres upoważnienia	Data wycofania upoważnienia	Data modyfikacji upoważnienia	Uwagi
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							
13.							
14.							
15.							

16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26.

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW BEZPIECZEŃSTWA DANYCH

Etap I Podejrzenie naruszenia
Po otrzymaniu informacji wiarygodnej informacji o zdarzeniu, Administrator ocenia czy doszło do naruszenia ochrony danych osobowych.

Etap II Stwierdzenie naruszenia
W przypadku stwierdzenia naruszenia, Administrator ocenia czy doszło do:
- Przypadkowego zniszczenia, utraty lub modyfikacji danych,
- Niezgodnego z prawem zniszczenia, utraty lub modyfikacji danych,
- Nieuprawnionego ujawnienia lub dostępu do danych.

W celu dokonania oceny naruszenia, Administrator zbiera informacje dotyczące:
- Kategorii podmiotów danych,
- Zakresu danych,
- Liczby wpisów,
- Źródła naruszenia,
- Okoliczności naruszenia (w tym daty i skutków),
- Opisu czynności zaradczych (w tym terminu ich wdrożenia i osobę odpowiedzialną).

Etap III – Ocena naruszenia

(KP) KONTEKST PRZETWARZANIA - zwiększ lub obniż wyjściową wartość w zależności od okoliczności:
- Dane zwykłe, np. imię i nazwisko, adres (1)
- Dane behawioralne, np. lokalizacja, preferencje (2)
- Dane finansowe, np. numer rachunku bankowego (3)
- Dane wrażliwe, np. o zdrowiu (4)

(I) ŁATWOŚĆ IDENTYFIKACJI - przyjmij najbardziej adekwatną z czterech poniższych wartości:
- Poziom nisko (0,25)- identyfikacja za pomocą danych objętych naruszeniem jest bardzo trudna
- Poziom ograniczony (0,5) - identyfikacja za pomocą danych objętych naruszeniem jest trudna
- Poziom znaczny (0,75)- identyfikacja za pomocą objętych danych jest łatwa
- Poziom wysoki (1)- identyfikacja jest bardzo łatwa, natychmiastowa

(ON) OKOLICZNOŚCI NARUSZENIA – zsumuj uzyskane wartości:
- Naruszenie poufności (0/0,25/0,5)
- Naruszenie integralności (0/0,25/0,5)
- Naruszenie dostępności (0/0,25/0,5)
- Działanie zamierzone lub przypadkowe (0/0,5)

(PN) POZIOM NARUSZENIA – oblicz wg wzoru: PN=KP x I + ON
- **PN <2** – poziom niski
- **2 ≤ PN <3** – poziom średni
- **3 ≤ PN <4** – poziom wysoki,
- **4 ≤ PN** – poziom bardzo wysoki,

Etap IV- Podjęcie niezbędnych działań

Określenie poziomu ryzyka naruszenia praw wolności podmiotów danych		
Małe prawdopodobieństwo	**Występuje ryzyko dla praw i**	**Występuje wysokie ryzyko dla praw i**

ryzyka dla praw i wolności	wolności	wolności
✓ Wpis do rejestru naruszeń ✓ Wdrożenie środków zaradczych	✓ Wpis do rejestru naruszeń ✓ Wdrożenie środków zaradczych ✓ Powiadomienie organu nadzorczego *<u>zawiadomienie uzupełniające-</u> w razie stwierdzenia nowych istotnych okoliczności dotyczących naruszenia lub uzyskania brakujących wcześniej informacji	✓ Wpis do rejestru naruszeń ✓ Wdrożenie środków zaradczych ✓ Powiadomienie organu nadzorczego - powinno zawierać następujące informacje (art. 33 ust.3 RODO): - charakter naruszenia, w tym kategorie i przybliżona liczba osób dotkniętych naruszeniem - imię i nazwisko, dane kontaktowe IOD/ osoby kontaktowej dla organu nadzorczego - możliwe konsekwencje naruszenia - wdrożone lub planowane środki bezpieczeństwa ✓ Powiadomienie podmiotów danych- obowiązek powiadomienia jest wyłączony, gdy (art. 34 ust. 3 RODO): -administrator wdrożył odpowiednie środk bezpieczeństwa i uniemożliwił dostęp do danych objętych naruszeniem osobom nieupoważnionym, - administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia, - powiadomienie wymagałoby niewspółmiernie dużego wysiłku i administrator wydał publiczny komunikat o naruszeniu lub zastosował inne podobne rozwiązania <u>* zawiadomienie uzupełniające</u> - w razie stwierdzenia nowych istotnych okoliczności dotyczących naruszenia lub uzyskania brakujących wcześniej informacji

Etap II/ Etap III/ Etap IV – 72 godziny na powiadomienie PUODO

Załącznik nr 9a do Polityki Bezpieczeństwa Informacji ,
Wzór oświadczenia pracownika

....

Imię i Nazwisko Miejscowość, data

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz znana mi jest treść przyjętej w jednostce dokumentacji ochrony danych osobowych, wobec czego zobowiązuję się do:

1. stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
2. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
3. należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nie upoważnionym,
4. zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą,
5. zachowania w tajemnicy danych do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy,
6. zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu.

W zakresie systemu informatycznego zobowiązuję się:

1. nie ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
2. nie ujawniać szczegółów technologicznych w używanych systemach oraz oprogramowaniu,
3. nie udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
4. nie kopiować lub nie przetwarzać danych w sposób inny niż dopuszczony obowiązującą Dokumentacją.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora Danych Osobowych za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....

(podpis)

Załącznik nr 9b do Polityki Bezpieczeństwa Informacji
Wzór oświadczenia dla pracownika gospodarczego

....

Imię i Nazwisko Miejscowość, data

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz znana mi jest treść dokumentacji ochrony danych osobowych przyjętej w jednostce, wobec czego zobowiązuję się do:

- stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
- zachowania w tajemnicy danych do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę, oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy,
- należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nie upoważnionym,
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora Danych Osobowych za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

.....

(podpis)

Załącznik nr 10 do Polityki Bezpieczeństwa Informacji , Ewidencja oświadczeń pracowników			
Ewidencja oświadczeń pracowników			Sporządził:
			Data:

L .p.	Imię i Nazwisko pracownika	Zajmowane stanowisko	Data złożonego oświadczenia
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			