Zarządzenie nr 37/18
Wójta Gminy Żołynia
z dnia 10.08.2018 r.

w sprawie wdrożenia „Polityki ochrony danych osobowych w Urzędzie Gminy Żołynia"

Na podstawie art. 30 ust. 1 i art. 3 ust. 33 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2018 r., poz. 994 ze zm.) oraz art. 24 ust. 1 i ust. 2 rozporządzenia z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (Dz. U. UE. L.2016.119.1) 2016/679 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) zarządzam, co następuje:

§1. Ustalam „Politykę ochrony danych osobowych przetwarzanych w Urzędzie Gminy Żołynia" w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§2. Zobowiązuję wszystkich pracowników Urzędu Gminy Żołynia do stosowania i przestrzegania ustaleń zawartych w dokumencie, o którym mowa w §1.

§3. Traci moc Zarządzenie Nr 33/13 Kierownika Urzędu Gminy w Żołyni z dnia 21 sierpnia 2013 r. w sprawie wprowadzenia w Urzędzie Gminy Żołynia „Polityki bezpieczeństwa danych osobowych" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

§4. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Andrzej Benedyk

Załącznik
do Zarządzenia Nr 37/18
Wójta Gminy Żołynia
z dnia 10.08.2018 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

w Urzędzie Gminy Żołynia

Żołynia, 2018 r.

SPIS TREŚCI

ROZDZIAŁ I. POSTANOWIENIA OGÓLNE

ROZDZIAŁ II. DEFINICJE UŻYTE W POLITYCE OCHRONY DANYCH OSOBOWYCH

ROZDZIAŁ III. ZAKRESY ODPOWIEDZIALNOŚCI ZA PRZETWARZANIE I OCHRONĘ DANYCH OSOBOWYCH

ROZDZIAŁ IV. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ V. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

ROZDZIAŁ VI. UPOWAŻANIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ VII. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

ROZDZIAŁ VIII. ZASADY MINIMALIZACJI PRZETWARZANYCH DANYCH

ROZDZIAŁ IX. PROFILOWANIE

ROZDZIAŁ X. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ XI. UDOSTĘPNIANIE DANYCH OSOBOWYCH

ROZDZIAŁ XII. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ XIII. REALIZOWANIE PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE W URZĘDZIE

ROZDZIAŁ XIV. INSPEKTOR OCHRONY DANYCH

ROZDZIAŁ XV. NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

ROZDZIAŁ XVI. POSTANOWIENIA KOŃCOWE

ROZDZIAŁ XVII. SPIS ZAŁĄCZNIKÓW

ROZDZIAŁ I. POSTANOWIENIA OGÓLNE

W dążeniu do zapewnienia wysokiego poziomu ochrony danych osobowych przetwarzanych w Urzędzie Gminy Żołynia, zwanym dalej „Urzędem" w tym: zabezpieczenia danych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do przechowywanych lub przesyłanych danych określa się Politykę ochrony danych osobowych, zwanej dalej „Polityką".

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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;
- Przepisy krajowe w zakresie ochrony danych osobowych, głównie Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

Niniejsza polityka ochrony obowiązuje każde stanowisko pracy, wszystkie procesy i czynności przetwarzania danych w Urzędzie i reguluje zarządzanie ochroną danych osobowych przetwarzanych zarówno w formie papierowej jak i elektronicznej w Urzędzie.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Urząd przed różnego rodzaju zagrożeniami, zarówno wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi oraz określenie reguł i procedur zapewniających bezpieczeństwo tych danych.

Zastosowane zabezpieczenia organizacyjne i techniczne mają służyć osiągnięciu warunków, które:

- gwarantują przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa (legalność przetwarzania danych);
- gwarantują odpowiedni poziom ochrony przetwarzanych danych oraz ochronę prywatności osób, których dane osobowe są przetwarzane (bezpieczeństwo danych);
- zapewniają przejrzysty sposób przetwarzania danych osobowych oraz jasny sposób informowania o tych procesach osób, których dane dotyczą (transparentność procesów przetwarzania);
- dają możliwość realizacji przez osoby, których dane są przetwarzane, swoich praw zgodnie z obowiązującymi przepisami prawa (ochrona prywatności osób fizycznych);
- pozwalają na dokumentowanie realizowanych czynności w celu wykazania i potwierdzania ich zgodności z obowiązującymi przepisami prawa (rozliczalność procesów przetwarzania);
- zezwalają na gromadzenie danych wyłącznie w zakresie niezbędnym do załatwiania sprawy bądź realizacji zadań wynikających z przepisów prawa (minimalizacja i adekwatność danych);

- zapewniają przetwarzanie danych wyłącznie w okresie czasu, który jest niezbędny do załatwienia sprawy bądź zrealizowania zadań wynikających z przepisów prawa (ograniczenie w czasie przetwarzania danych).

ROZDZIAŁ II. DEFINICJE UŻYTE W POLITYCE

Ilekroć Polityce jest mowa o:

Administratorze Danych Osobowych (ADO) – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, (Urząd Gminy Żołynia), decydujące o celach i środkach przetwarzania danych osobowych.

Danych dzieci - rozumie się przez to dane osób poniżej 16-tego roku życia.

Danych osobowych – rozumie się przez nie wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Danych sensytywnych (wrażliwych) – rozumie się przez to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Pracowniku komórki organizacyjnej – rozumie się przez to pracownika komórki organizacyjnej odzwierciedlonej w Regulaminie Organizacyjnym Urzędu Gminy Żołynia.

Podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarzana dane osobowe w imieniu i na rzecz Administratora Danych Osobowych.

Powierzeniu przetwarzania danych – rozumie się przez to zlecenie wykonania czynności przetwarzania danych innemu podmiotowi w drodze odrębnej umowy zawartej na piśmie lub stosownego pisemnego zapisu do umowy wyłącznie w zakresie i celu w nich przewidzianym.

Profilowanie - rozumie się przez to dobrowolną 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, zachowania lub przemieszczania się.

Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, kopiowanie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

RODO - rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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;

Udostępnianiu danych – rozumienie się przez to w szczególności takie czynności na danych jak ich przekazywanie, rozpowszechnianie lub ujawnienie odbiorcy danych lub podmiotowi danych osobowych, w sposób tradycyjny lub poprzez teletransmisję poza struktury organizacyjne Urzędu Gminy Żołynia.

UODO – rozumie się przez to Urząd Ochrony Danych Osobowych.

Zgodzie osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych, tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

ROZDZIAŁ III. ZAKRESY ODPOWIEDZIALNOŚCI ZA PRZETWARZANIE I OCHRONĘ DANYCH OSOBOWYCH

1. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z przepisami RODO i z krajowymi przepisami w zakresie ochrony danych osobowych odpowiada Wójt Gminy Żołynia jako Administrator Danych, który jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną.
2. Wójt Gminy może być ponadto identyfikowany w procesach przetwarzania danych osobowych w Urzędzie jako:

- współadministrator danych osobowych, w przypadku określenia wspólnego celu przetwarzania danych wraz z innymi podmiotami,
- podmiot przetwarzający (procesor), w przypadku przetwarzania danych osobowych w imieniu i na rzecz innych administratorów danych na podstawie umowy powierzenia danych osobowych.

3. W zakresie ochrony danych osobowych Wójt wykonuje nałożone przez przepisy obowiązki m.in. przez:

- Inspektora Ochrony Danych,
- pracownika pełniącego funkcję informatyka w Urzędzie, który administruje aplikacjami i systemami teleinformatycznymi,
- pracowników, którzy realizują zadania określone w ich zakresach czynności i w przyznanych upoważnieniach;
- podmioty przetwarzające dane na podstawie umowy powierzenia.

4. Każdy pracownik jest odpowiedzialny za zapewnienie prawidłowego przetwarzania danych osobowych, z którymi pracuje.
5. Każdy pracownik ma obowiązek realizować obowiązki informacyjne określone w rozdziale III RODO, w tym w szczególności podejmować określone środki, aby w sposób zrozumiały, zwięzły, jasnym i prostym językiem udzielić osobie wyczerpujących informacji nt. jego danych osobowych.

ROZDZIAŁ IV. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

Za bezpieczeństwo przetwarzania danych osobowych indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy jak i poza nim w sposób wykraczający poza czynności związane z ich przetwarzaniem związanym z zakresem obowiązków służbowych w ramach udzielonego upoważnienia do przetwarzania danych.

Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. Dane osobowe w formie papierowej muszą być przechowywane, co najmniej w meblach biurowych zamykanych na klucz. Klucze należy przechowywać w sposób bezpieczny bez możliwości dostępu do nich osób nieuprawnionych.

W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka", która oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.

Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku drzwi.

Nie można udzielać informacji dotyczących danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego za wyjątkiem spraw związanych ze zwykłymi czynnościami dnia codziennego związanymi z wykonywaniem obowiązków służbowych.

Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania za wyjątkiem konieczności wykonywania określonych czynności służbowych.

Zasady obowiązujące przy kopiowaniu danych osobowych w ramach obszaru przetwarzania

Kopiowanie danych osobowych w ramach komórki organizacyjnej może odbywać się wyłącznie przez osobę w ramach posiadanego upoważnienia do przetwarzania danych i może być dokonywane wyłącznie na potrzeby związane z realizacją zadań komórki organizacyjnej wynikających z regulacji wewnętrznych Urzędu lub w celu realizacji umów zawieranych przez Urząd w zakresie udostępnienia danych i powierzenia przetwarzania danych, w których realizację dana komórka organizacyjna jest zaangażowana.

Kopia danych osobowych podlega zniszczeniu niezwłocznie po realizacji celu, dla którego kopia została wykonana chyba, że co innego wynika z postanowień umów, regulacji wewnętrznych Urzędu Gminy Żołynia lub powszechnie obowiązujących przepisów prawa.

ROZDZIAŁ V. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH W SYSTMACH INFORMATYCZNYCH

Dostęp do systemów i programów komputerowych

1. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na przekazaniu dostępu w postaci identyfikatora, hasła oraz ustalenie zakresu dostępnych danych.
2. Za wygenerowanie identyfikatora i hasła użytkownikowi odpowiada administrator danych przy współpracy z informatykiem obsługującym działanie systemu informatycznego w Urzędzie.

Stosowane metody i środki uwierzytelniania użytkownika oraz procedury z ich zarządzaniem i użytkowaniem

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym użytkownik otrzymuje po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.
3. Użytkownik dostaje swoje hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznym. Hasło przydzielone do użytkownika musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego.
4. Hasło jest zmieniane przez użytkownika po upływie 30 dni od ostatniej zmiany.
5. Hasło składa się z co najmniej 6 znaków i powinno zawierać co najmniej jedną dużą literę i jeden znak specjalny.
6. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy.
7. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie użytkownik nie może udostępniać swojego stanowiska pracy osobom nieupoważnionym. Niedopuszczalne jest by dwóch lub większa liczba użytkowników wykorzystywała wspólnie jedno konto użytkownika.
8. W przypadku gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło oraz powiadomić o tym administratora danych osobowych.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik zobowiązany jest do zwrócenia uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.
2. Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego.
3. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.

4. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, powinny być ustawione w taki sposób, aby uniemożliwiały tym osobom wgląd w dane.
6. W sytuacji opuszczenia stanowiska pracy przez użytkownika na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu.
7. Przed opuszczeniem stanowiska pracy użytkownik zobowiązany jest wywołać wygaszacz ekranu bądź wylogować się z systemu informatycznego.
8. Kończąc pracę użytkownik obowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy.
9. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafkach zamykanych na klucz.

Procedury tworzenia kopii zapasowych

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych odpowiedzialny jest każdy użytkownik systemu informatycznego.
3. Kopie zapasowe zbiorów danych są tworzone co najmniej dwa razy w roku, w szczególnych przypadkach – przed aktualizacją lub zmianą w systemie.
4. Nośniki kopii zapasowych, które zostały wycofane z użycia należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych; w przeciwnym wypadku podlegają fizycznemu zniszczeniu w sposób uniemożliwiający odczytanie zapisanych na nich danych.
5. Kopie zapasowe przechowywane są w serwerowni, do której dostęp ma wyłącznie osoba pracująca na stanowisku informatyka urzędu lub osoba upoważniona przez Administratora Danych.

Sposób, miejsce i okres przechowywania wydruków elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z budynku Urzędu wydruków, nośników z danymi osobowymi bez zgody administratora danych osobowych.
2. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich osobom nieupoważnionym.
3. Kopie zapasowe na nośnikach optycznych i magnetycznych przechowywane są w szafce na klucze, do którego ma dostęp wyłącznie osoba zatrudniona na stanowisku Informatyka Urzędu.
4. Za bezpieczeństwo danych zapisanych w komputerze odpowiada użytkownik komputera.
5. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
6. Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, zawierające dane osobowe pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy

nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie.
7. Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii.

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskania dostępu do systemu informatycznego

1. W celu przeciwdziałania zagrożeniom systemów informatycznych, oprócz odpowiedniego poziomu komplikacji haseł dostępu stosuje się ochronę antywirusową na stacjach roboczych komputerów wykorzystywanych do przetwarzania danych osobowych.
2. System antywirusowy zainstalowany jest w każdym komputerze.
3. Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów.
5. Do ochrony antywirusowej stosuje się najnowszą dostępną wersję programu antywirusowego.
6. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym osobę zatrudnioną na stanowisku Informatyka Urzędu.
7. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
8. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów antywirusowych.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora danych osobowych.
3. Prace serwisowe na terenie Urzędu prowadzone w zakresie przeglądów i konserwacji systemów informatycznych mogą być wykonywane wyłącznie przez pracowników jednostki lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników Urzędu.
4. Przed rozpoczęciem prac serwisowych przez osoby spoza Urzędu konieczne jest potwierdzenie tożsamości serwisantów.

Urządzenie, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe przeznaczone do likwidacji bądź naprawy, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych osobowych.

ROZDZIAŁ VI. UPOWAŻNIENIA DO PRZETARZANIA DANYCH OSOBOWYCH

1. Wójt jako Administrator odpowiada za nadawanie/ zmianę/ anulowanie upoważnień do przetwarzania danych w Urzędzie.
2. Każda osoba upoważniona może przetwarzać dane wyłącznie na podstawie przepisu prawa lub na polecenie Administratora.
3. Każda osoba, przed dopuszczeniem do przetwarzania danych osobowych i uzyskaniem upoważnienia przechodzi szkolenie podstawowe z zakresu ochrony danych osobowych. Szkolenie prowadzone jest przez Inspektora Ochrony Danych. Szkolenie polega na zapoznaniu osoby z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z Polityką Ochrony Danych wprowadzoną w Urzędzie. Fakt zapoznania z ww. dokumentami i przyjęcie na siebie obowiązku ich stosowania pracownik potwierdza poprzez złożenie oświadczenia stanowiącego ***załącznik nr 1*** do niniejszej Polityki.
4. Dostęp do danych osobowych, na podstawie upoważnienia uzyskują:
   a) osoby zatrudnione w Urzędzie, które przetwarzają dane osobowe w ramach swoich obowiązków służbowych, a także stażyści i praktykanci;
   b) osoby świadczące usługi na podstawie umów cywilnoprawnych.
5. Upoważnienie do przetwarzania danych osobowych udzielane jest pracownikowi po podpisaniu przez osobę oświadczenia o zachowaniu w tajemnicy przetwarzanych informacji czyli tzw. oświadczenia o poufności, którego wzór stanowi ***załącznik nr 2*** do niniejszej Polityki
6. Każdy pracownik mający dostęp do danych osobowych musi posiadać pisemne upoważnienie do przetwarzania tych danych nadane przez Administratora Danych Osobowych, którego wzór stanowi ***załącznik nr 3*** do niniejszej Polityki. Upoważnienie jest napisane w trzech egzemplarzach, gdzie jeden zostaje wręczony pracownikowi, drugi Inspektorowi Ochrony Danych Osobowych, zaś trzeci odkładany jest do akt osobowych pracownika. W upoważnieniu wskazywany jest również system informatyczny, jaki może obsługiwać pracownik otrzymujący upoważnienie.
7. Na podstawie nadanych upoważnień prowadzona jest w Urzędzie „Ewidencja osób upoważnionych do przetwarzania danych osobowych", której wzór stanowi ***załącznik nr 4*** do niniejszej Polityki.

ROZDZIAŁ VII. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Zidentyfikowane czynności przetwarzania zawierające dane osobowe w wersji papierowej i elektronicznej są przetwarzane i przechowywane w Urzędzie i znajdują się w jednym budynku.

Szczegółowy wykaz pomieszczeń obszaru, w którym przetwarzane są dane osobowe w Urzędzie zawiera ***załącznik nr 5*** do niniejszej Polityki.

ROZDZIAŁ VIII. ZASADY MINIMALIZACJI PRZETWARZANYCH DANYCH

1. W Urzędzie zapewnione są warunki aby przetwarzanie danych było ograniczone do niezbędnego minimum.
2. Niezbędne minimum ustalane jest na etapie wprowadzania nowych usług lub systemów teleinformatycznych i wynika z analizy możliwości wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby w momencie uruchamiania nowych usług przetwarzane były wyłącznie te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.
3. Minimalizacja przetwarzania danych odnosi się do:
   a) zakresu danych czyli ilości potrzebnych danych oraz zakresu przetwarzania;
   b) dostępu do danych;
   c) czasu przechowywania danych.
4. Minimalizacja zakresu polega na tym, że w Urzędzie na bieżąco weryfikowany jest zakres pozyskiwanych danych oraz prowadzony jest przegląd ilości przetwarzanych danych i zakresu ich przetwarzania zgodnie z zasadą ochrony danych w fazie projektowania (privacy by design) i zasadą domyślnej ochrony danych (privacy by default).
5. Minimalizacja dostępu polega na tym, że w Urzędzie stosuje się ograniczenia dostępu do danych osobowych (prawne tj. zobowiązania do poufności, zakresy upoważnień), fizyczne (zamykane pomieszczenia) oraz logiczne (hasła na komputery itp.);.
6. Minimalizacja czasu polega na tym, że w Urzędzie:
   - przetwarza się dane osobowe do czasu osiągnięcia celu,
   - terminy przetwarzania danych określone zostały na podstawie przepisów prawa lub wynikają z przeprowadzonej analizy ich przydatności,
   - dane, których zakres przydatności ulega ograniczeniu są archiwizowane oraz przechowywane w archiwum zakładowym przez okres określony w obowiązujących przepisach prawa w zakresie archiwizacji.

ROZDZIAŁ IX. PROFILOWANIE

W Urzędzie nie identyfikuje się przypadków, w których dokonywane jest profilowanie przetwarzanych danych. W przypadku zastosowania profilowania zostaną wdrożone odpowiednie mechanizmy zapewniające zgodność tego procesu z przepisami prawa, a osoby, których dane będą w takim przypadku przetwarzane zostaną o tym poinformowane.

ROZDZIAŁ X. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie przetwarzania danych osobowych może się odbyć tylko na podstawie pisemnej umowy, w której wyraźnie zostanie określony charakter i cel przetwarzania, przedmiot i czas trwania przetwarzania, rodzaj danych osobowych, a także obowiązki podmiotu przetwarzającego.
2. Dane mogą zostać powierzone wyłączenie podmiotom, które gwarantują odpowiednie środki techniczne i organizacyjne do skutecznej ochrony praw osób, których dane dotyczą.
3. Przykładowa umowa powierzenia przetwarzania danych stanowi ***załącznik nr 6*** do niniejszej Polityki.
4. Należy prowadzić ewidencję zawartych umów powierzania danych, której wzór stanowi ***załącznik nr 7*** do niniejszej Polityki.

ROZDZIAŁ XI. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia Administratora może mieć miejsce wyłącznie w przypadku działań osób i podmiotów uprawnionych na mocy odpowiednich przepisów prawa.
2. Dane osobowe mogą być udostępniane:

a) stronom postępowań administracyjnych prowadzonych w Urzędzie, na zasadach określonych w Kodeksie Postępowania Administracyjnego lub odrębnych przepisów,

b) podmiotom i organom publicznym działającym w granicach przyznanym im uprawnień po okazaniu dokumentów potwierdzających te uprawnienia.

3. Udostępnianie danych osobowych podmiotom i osobom, które wykażą interes prawny lub faktyczny musi być ewidencjonowany.
4. Odmowa udostępnienia może nastąpić w sytuacji, gdy spowodowałoby to:
   - ujawnienie wiadomości zawierających informacje niejawne,
   - zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
   - istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

ROZDZIAŁ XII. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. W Urzędzie prowadzony jest „Rejestr czynności przetwarzania danych osobowych". Rejestr ten powinien być na bieżąco aktualizowany.
2. Rejestr czynności przetwarzania służy do inwentaryzacji, usystematyzowania i monitorowania sposobu, w jaki przetwarzane są dane osobowe w Urzędzie.
3. Rejestr czynności przetwarzania danych osobowych zawierać powinien następujące informacje:
   - nazwę czynności przetwarzania,
   - cel przetwarzania,
   - referat, stanowisko pracy,
   - opis kategorii osób, których dane dotyczą,
   - opis kategorii danych osobowych,
   - podstawę prawną przetwarzania danych,
   - źródło danych, z którego dane zostały pozyskane,
   - planowany termin usunięcia kategorii danych,
   - nazwę współadministratora i jego dane kontaktowe,
   - nazwę podmiotu przetwarzającego i jego dane kontaktowe,
   - kategorie odbiorców,
   - nazwa systemu lub oprogramowania,
   - ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
   - ocena skutków dla ochrony danych (DPIA),
   - transfer do kraju trzeciego lub organizacji międzynarodowej i dokumentacja odpowiednich zabezpieczeń, jeżeli dotyczy.
4. Rejestr czynności przetwarzania ma charakter dokumentu wewnętrznego i z uwagi na zawarte w nim informacje (np. o zabezpieczeniach ochrony danych osobowych) nie może być udostępniony osobom nieuprawnionym.
5. Rejestr czynności przetwarzania składa się ze strony tytułowej oraz ponumerowanych kart czynności przetwarzania i spisu kart.
6. Wzór Rejestru czynności przetwarzania danych osobowych stanowi ***załącznik nr 8*** do niniejszej Polityki.

ROZDZIAŁ XIII. REALIZOWANIE PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE W URZĘDZIE

1. W Urzędzie respektuje się prawa osób, których dane są przetwarzane, a w szczególności:

a) zapewnienia osobom, których dane dotyczą wyrażenia zgody na przetwarzanie danych osobowych (gdy brak innej podstawy do przetwarzania danych);
b) informowania osób, których dane dotyczą o zbieraniu i przetwarzaniu tych danych;
c) prawa dostępu osobom, których dane dotyczą;
d) prawa sprostowania swoich danych;
e) prawa do usunięcia swoich danych (prawo do bycia zapomnianym);
f) prawa do przeniesienia swoich danych;
g) prawa do ograniczenia przetwarzania swoich danych.

2. Jedną z przesłanek przetwarzania danych osobowych w Urzędzie może być udzielona na piśmie zgoda, której przykładowy wzór stanowi ***załącznik nr 9***.
3. Obowiązek informacyjny względem osób, których dane są przetwarzane odbywa się poprzez:

a) przekazanie osobom (klientom) informacji wymaganych prawem – informację należy przekazać w sposób zwięzły, przejrzysty, w zrozumiałej formie, jasnym i prostym językiem. Informacji tej udziela się na piśmie bądź ustnie, w zależności od sytuacji.
b) realizacja zgłaszanych przez klientów żądań, w tym np. dostęp, usunięcie lub ograniczenie przetwarzania danych osobowych musi być zgodne z przepisami prawa, na podstawie których odbywa się przetwarzanie oraz na podstawie przepisów prawa określających zasady przetwarzania dokumentacji archiwalnej.

4. Realizacja obowiązku informacyjnego określonego w art. 13 RODO polega na przekazaniu osobom, których dane dotyczą, następujących informacji:

- identyfikujących administratora danych osobowych (Urząd Gminy Żołynia, ul. Rynek 22, 37-110 Żołynia);
- umożliwiających kontakt z Inspektorem Ochrony Danych w Urzędzie (np. telefon, e-mail),
- wskazujących w jakim celu przetwarzane będą dane oraz jaka jest podstawa prawna przetwarzania,
- o odbiorcach danych,
- o okresie przetwarzania danych osobowych,
- o przysługującym prawie do żądania dostępu do danych osobowych, prawie ich sprostowania, a po ustaniu okresu ich przechowywania prawie do ich usunięcia lub ograniczenia przetwarzania, w myśl obowiązujących przepisów prawa,
- o przysługującym prawie do wniesienia sprzeciwu wobec przetwarzania danych osobowych,
- o przysługującym prawie do przenoszenia swoich danych,
- o przysługującym prawie do wniesienia skargi do organu nadzorczego,
- o obowiązku podania danych osobowych oraz skutków ich nieprzekazania,

5. W celu skutecznego informowania osób, których dane osobowe są przetwarzane można stosować następujące sposoby:

a) -umieszczanie informacji na stronie internetowej Urzędu, w szczególności w Biuletynie Informacji Publicznej;
b) umieszczenie informacji w postaci tabliczki przy stanowiskach pracy pracowników Urzędu;

c) umieszczenie informacji w odrębnym dokumencie, na którym klient może potwierdzić fakt zapoznania się z nimi,
d) ustne przekazywanie informacji obsługiwanym klientom,
e) umieszczenie informacji w korespondencji przesyłanej do klientów Urzędu.

6. Wybór sposobu uzależniony jest do charakteru prowadzonych działań i specyfiki sprawy.
7. Przykładowa propozycja ogólnej klauzuli informacyjnej dla klientów Urzędu stanowi ***załącznik nr 10*** do niniejszej Polityki.

ROZDZIAŁ XIV. INSPEKTOR OCHRONY DANYCH

1. W celu jak najlepszej ochrony danych osobowych oraz w celu realizacji zapisów rozporządzenia powołany został Inspektor ochrony danych.

Inspektor ochrony danych:

a) informuje administratora i pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich w zakresie ochrony danych osobowych,
b) monitoruje, w miarę sowich możliwości i kompetencji przestrzegania zapisów niniejszej polityki,
c) udziela ustnych i pisemnych informacji klientom Urzędu w zakresie zagadnień dotyczących przetwarzania danych osobowych,
d) przyjmuje zgłoszenia o wystąpieniu naruszenia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie,
e) zawiadamia osoby, których dane dotyczą o naruszeniu ochrony danych osobowych,
f) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych,
g) pełni nadzór nad prowadzeniem rejestru czynności przetwarzania danych osobowych,
h) pełni nadzór nad bieżącą aktualizacją „Ewidencji osób upoważnionych do przetwarzania danych osobowych".

2. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

ROZDZIAŁ XV. NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Każda osoba zatrudniona w Urzędzie lub wykonująca prace na rzecz Urzędu (stażysta, praktykant, przedstawiciel firmy zewnętrznej współpracujący z Urzędem itp.) jest zobowiązana do natychmiastowego powiadamiania inspektora ochrony danych i administratora, jeśli stwierdzi lub ma podejrzenie, że doszło do naruszenia ochrony danych osobowych.
2. Z uwagi na wymogi RODO, w tym krótki okres na zgłoszenie naruszenia bezpieczeństwa danych osobowych (72 godziny od stwierdzenia wykrycia naruszenia) informacje w tym zakresie muszą być przekazywane natychmiastowo, bez zbędnej zwłoki.
3. W przypadku naruszenia ochrony danych osobowych sporządza się raport o naruszeniu, którego wzór stanowi ***załącznik nr 11*** do niniejszej Polityki.
4. Typowe sytuacje zagrożeń bezpieczeństwa danych osobowych

Zagrożenia dla poufności danych	Zagrożenia dla dostępności i integralności danych	Zagrożenia dla rozliczalności danych
✓ przebywanie nieuprawnionych osób w obszarze przetwarzania danych osobowych, ✓ nieuwaga, lekkomyślność osób przetwarzających dane osobowe, ✓ przetwarzanie danych osobowych przez osoby nie posiadające upoważnień, ✓ zbieranie danych osobowych przez osobę nieuprawnioną, ✓ wynoszenie danych osobowych poza obszar ich przetwarzania, ✓ wysyłanie plików zawierających dane osobowe za pomocą poczty elektronicznej, ✓ brak kontroli i ewidencjonowania elektronicznych nośników zawierających dane osobowe, ✓ kompromitacja kluczy szyfrujących odpowiedzialnych za bezpieczną komunikację,	✓ przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych, ✓ awaria sprzętu sieciowego odpowiedzialnego za komunikację w sieci lokalnej, ✓ przypadkowe lub celowe uszkodzenie, utrata, zniszczenie, modyfikacja danych osobowych, ✓ ataki pochodzące z sieci publicznej, ✓ działanie szkodliwego oprogramowania, ✓ klęski żywiołowe, ✓ wandalizm, ✓ ataki terrorystyczne, ✓ trwała lub czasowa utrata dostępu do zasobów informatycznych, ✓ przeciążenie lub awarie sprzętu sieciowego, ✓ uszkodzenie lub nieautoryzowana modyfikacja danych osobowych, ✓ uszkodzenie, celowe lub przypadkowe ✓ brak oprogramowania aplikacyjnego lub	✓ nieprzydzielenie użytkownikom systemu informatycznego unikalnego identyfikatora w jego obrębie, ✓ brak adekwatnych do wymagań prawa mechanizmów kontroli dostępu do danych, ✓ niewłaściwa administracja systemem informatycznym, ✓ niewłaściwa konfiguracja systemu informatycznego, ✓ zbyt duże uprawnienia użytkowników systemu informatycznego, ✓ zniszczenie lub sfałszowanie logów systemowych.

✓ istnienie luki w oprogramowaniu pozwalającej na przechwycenie komunikacji w trybie nienadzorowanym	użytkowego służącego do przetwarzania danych osobowych, ✓ brak możliwości uruchomienia łącza zapasowego w przypadku uszkodzenia łącza podstawowego, ✓ niedostosowanie przepustowości łącza do aktualnej liczby użytkowników systemu	

5. Najczęstsze sytuacje, o których pracownik powinien powiadomić Administratora Danych Osobowych oraz inspektora ochrony danych:
- ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
- zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki,
- fizyczna obecność w budynku lub pomieszczeniu osób zachowujących się podejrzanie,
- otwarte drzwi do pomieszczeń szaf, w których przechowywane są dane osobowe,
- ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz firmy bez upoważnienia inspektora ochrony danych,
- udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież komputerów lub CD, twardych dysków, pendriv`e z danymi osobowymi,
- e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
- przechowywanie haseł do systemów w pobliżu komputera.

6. Zawiadomienie organu nadzorczego o sytuacji naruszenia bezpieczeństwa danych osobowych

a) Jeżeli jest chociażby podejrzenie, że zaistniałe naruszenie może skutkować ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana do Urzędu Ochrony Danych Osobowych.

b) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonywane jest w sposób określony przez organ nadzorczy nie później niż 72 godziny od wykrycia zdarzenia.

c) Zgłoszenia naruszenia bezpieczeństwa danych osobowych dokonuje Inspektor Ochrony Danych Osobowych wyznaczony w Urzędzie lub osoba działająca w jego zastępstwie.

7. Zawiadomienie osoby, której dane dotyczą o sytuacji naruszenia bezpieczeństwa jej danych osobowych

a) Jeżeli naruszenie bezpieczeństwa danych osobowych skutkuje ryzykiem naruszenia praw i wolności osób, informacja o tym zdarzeniu jest kierowana bez zbędnej zwłoki do osób, których dane dotyczą.

b) Zawiadomienie o naruszeniu powinno zawierać opis zdarzenia oraz możliwe do zastosowania środki zalecane w celu poradzenia sobie z naruszeniem i zminimalizowania jego negatywnych skutków.
c) Zawiadomienie o naruszeniu powinno zostać przekazane osobom, których ono dotyczy listownie, telefonicznie lub na adres e-mail.
d) Zawiadomienie o naruszeniu nie jest wymagane jeżeli wprowadzone zostały rozwiązania uniemożliwiające odczyt osobom nieuprawnionym dostępu do tych danych bądź zostały wprowadzone środki eliminujące prawdopodobieństwo ryzyka naruszenia praw i wolności osób.
e) Bezpośrednie zawiadomienie nie jest również wymagane jeśli powodowałoby to poniesienie niewspółmiernie dużych nakładów pracy i środków finansowych ze strony Urzędu. Można wówczas wydać publiczny komunikat na stronie Urzędu.

8. Wzór zawiadomienia o naruszeniu danych osobowych stanowi ***załącznik nr 12*** do niniejszej Polityki.

ROZDZIAŁ XVI. POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

3. Niniejszy dokument wchodzi w życie z dniem podpisania.

WÓJT
mgr Andrzej Benedyk

.....

Podpis Wójta Gminy

ROZDZIAŁ XVII. SPIS ZAŁĄCZNIKÓW

Załącznik nr 1 - Oświadczenie o zapoznaniu się z przepisami w zakresie ochrony danych osobowych

Załącznik nr 2 – Zobowiązanie do zachowania poufności

Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 4 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 5 – Wykaz pomieszczeń, w którym przetwarzane są dane osobowe w Urzędzie Gminy Żołynia

Załącznik nr 6 – Wzór umowy powierzenia przetwarzania danych osobowych

Załącznik nr 7 – Wykaz zawartych umów powierzania danych osobowych

Załącznik nr 8 – Wzór rejestru czynności przetwarzania danych osobowych dla Urzędu Gminy Żołynia

Załącznik nr 9 – Wzór przykładowej klauzuli zgody na przetwarzanie danych osobowych

Załącznik nr 10 – Wzór ogólnej klauzuli informacyjnej dla klientów Urzędu

Załącznik nr 11 – Wzór raportu o naruszeniu ochrony danych osobowych

Załącznik nr 12 – Wzór zawiadomienia o naruszeniu danych osobowych

WÓJT
mgr Andrzej Benedyk

Załącznik nr 1
do Polityki ochrony
danych osobowych w Urzędzie Gminy Żołynia

OŚWIADCZENIE

Ja, niżej podpisany (a) oświadczam, iż zostałam/zostałem* zapoznana/zapoznany* i przedszkolna/przeszkolony z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 100) oraz 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 oraz wprowadzonej i wdrożonej do stosowania przez Administratora Danych „Polityki ochrony danych osobowych" w Urzędzie Gminy Żołynia

Jednocześnie zobowiązuję się do:

- nie ujawniania danych osobowych nieuprawnionym osobom lub instytucjom w jakiejkolwiek formie bez zgody Administratora Danych Osobowych;
- przestrzegania obowiązujących aktów prawnych w zakresie ochrony danych osobowych,
- korzystania z oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy,
- nie podejmowania prób samodzielnego instalowania oprogramowania pochodzącego z innych źródeł,
- wnoszenia, wynoszenia i użytkowania komputerów przenośnych bądź innych nośników danych wyłącznie za wiedzą i zgodą Administratora Danych Osobowych,
- należytej dbałości o powierzony sprzęt i oprogramowanie,
- korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem, wyłącznie za zgodą Administratora Danych Osobowych,
- zachowania w tajemnicy wszelkich danych osobowych, które uzyskałem/uzyskałam w związku z zatrudnieniem w Urzędzie Gminy Żołynia. Wymogu tego dochowam również po ustaniu zatrudnienia w urzędzie.

Naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, będzie stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych w zakresie stosowania kary porządkowej zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r. poz. 917 z późn. zm.).

WÓJT
mgr Andrzej Benedy

.....
(data i czytelny podpis pracownika)

Załącznik nr 2
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

ZOBOWIĄZANIE
DO ZACHOWANIA POUFNOŚCI

Ja, niżej podpisany (a) zobowiązuję się do bezwzględnego zachowania w poufności zarówno w trakcie trwania stosunku pracy (stażu, praktyki, umowy zlecenia) w Urzędzie Gminy Żołynia jak i po jego ustaniu, wszelkich informacji uzyskanych w związku z wykonywaną pracą w urzędzie.

Przyjmuję do wiadomości, że przez obowiązek bezwzględnego zachowania w poufności rozumie się w szczególności zakaz:
1. zapoznawania się z wszelkimi dokumentami w formie papierowej, zawartością dysków twardych i innych nośników informatycznych nie związanych z ustalonym zakresem czynności, kopiowania, przegrywania dokumentów i danych bez zgody bezpośredniego przełożonego, a zwłaszcza udostępniania ich osobom trzecim,
2. informowania osób trzecich o zakresie spraw objętych nakazem poufności.

Przyjmuje również do wiadomości, że naruszenie zasady poufności obowiązującej w Urzędzie Gminy Żołynia spowoduje wobec mnie odpowiedzialność dyscyplinarną i karną.

WÓJT
mgr Andrzej Bernadyk

.....
(data i czytelny podpis pracownika)

Załącznik nr 3
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 oraz art. 32 ust. 4 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 upoważniam Panią/Pana:

.....
Imię i nazwisko

.....
stanowisko służbowe

do przetwarzania następujących czynności przetwarzania

.....
nazwa czynności przetwarzania

w formie papierowej i w następujących systemach informatycznych:

- .....

w zakresie zbierania, wprowadzania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania, rozpowszechniania lub innego rodzaju udostępniania oraz ich usuwania lub niszczenia po osiągnięciu celu przetwarzania danych*

Upoważnienie udzielane jest na czas trwania zatrudnienia na danym stanowisku pracy/ praktyki/ stażu/ współpracy* w Urzędzie Gminy Żołynia.

WÓJT
mgr Andrzej Benedyk
.....
data, i podpis Administratora Danych Osobowych

Otrzymują:
Egz. nr 1. Pracownik uzyskujący upoważnienie;
Egz. nr 2. Inspektor Ochrony Danych Osobowych;
Egz. nr 3. Akta osobowe pracownika.

*niepotrzebne usunąć

Załącznik Nr 4
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia do przetwarzania danych osobowych – nazwa czynności przetwarzania	Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym

WÓJT
mgr Andrzej Benedyk

Załącznik nr 5
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

Wykaz pomieszczeń, w którym przetwarzane są dane osobowe w Urzędzie Gminy Żołynia

L.p.	Adres/lokalizacja	Pomieszczenie/nazwa/nr pomieszczenia	Uwagi

WÓJT
mgr Andrzej Benedyk

Załącznik nr 6
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

UMOWA POWIERZENIA PRZETWARZANIA
DANYCH OSOBOWYCH

W dniu ..... pomiędzy:
Urzędem Gminy Żołynia, z siedzibą ul. Rynek 22, 37-110 Żołynia
reprezentowanym/ą przez ..... – Wójta Gminy Żołynia
zwanym/ą dalej „Powierzającym",
a
....., z siedzibą .....
zwanym dalej „Przetwarzającym",
wspólnie zwanymi dalej „Stronami",

w związku z zawarciem pomiędzy Stronami umowy dotyczącej
.....
.....
w celu wykonania postanowień powyższej umowy, Strony zawierają niniejszą umowę, zwaną dalej Umową.

§ 1.

Użyte w Umowie określenia oznaczają:

1) RODO - 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 (Dz. Urz. UE z 2016 r. L 119/1);
2) dane osobowe - dane osobowe dotyczące osób fizycznych;
3) przetwarzanie danych osobowych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, o których mowa w RODO.

§ 2.

Powierzający oświadcza, że jest administratorem danych w rozumieniu art. 4 pkt. 7 RODO o nazwie:
.....
.....

§ 3.

Przetwarzający powierzone dane osobowe będzie przetwarzał w okresie niezbędnym do realizacji umowy. Umowa ulega rozwiązaniu z dniem wygaśnięcia bądź rozwiązania umowy.

§ 4.

1. Powierzający, na podstawie art. 28 ust. 3 RODO, w celu realizacji postanowień Umowy, powierza Przetwarzającemu przetwarzanie danych osobowych zawartych w zbiorze, o którym mowa w § 2 w imieniu i na rzecz Powierzającego, na warunkach opisanych w Umowie.
2. Przekazane przez Powierzającego Przetwarzającemu do przetwarzania dane osobowe zawarte w zbiorze, o którym mowa w § 2 mogą być przetwarzane wyłącznie w celu realizacji Umowy, w szczególności do .....

§ 5.

Zakres danych osobowych powierzonych Przetwarzającemu do przetwarzania obejmuje:

1) .....,
2) .....
3) .....
4) .....

§ 6.

1. Przetwarzający zapewnia, że do przetwarzania danych osobowych będą dopuszczone jedynie osoby, które:
   1) posiadają imienne upoważnienie do przetwarzania danych osobowych,
   2) zobowiążą się, przed rozpoczęciem przetwarzania danych, do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczenia, także po ustaniu zatrudnienia u Przetwarzającego.

§ 7.

1. Powierzający wyraża zgodę/ nie wyraża zgody* na powierzenie przez Przetwarzającego przetwarzania zbioru danych osobowych, o którym mowa w § 2 innym podmiotom, z którymi

Przetwarzający zawrze odpowiednie umowy powierzenia przetwarzania tych danych, w celu, o którym mowa w § 4 ust. 2 oraz zakresie, o którym mowa w § 5.

2. Na podmiot przetwarzający, na podstawie umowy, o której mowa w ust. 2 będą nałożone te same obowiązki ochrony danych w szczególności wdrożenia odpowiednich środków technicznych i organizacyjnych jak w Umowie by przetwarzanie odpowiadało wymogom RODO.

§ 8.

1. Powierzający lub upoważniony przez niego audytor zewnętrzny ma prawo do przeprowadzenia audytu przestrzegania przez Przetwarzającego zasad przetwarzania danych osobowych, o których mowa w niniejszej umowie oraz w obowiązujących przepisach prawa, w szczególności poprzez żądanie udzielenia informacji dotyczących przetwarzania przez Przetwarzającego powierzonych danych osobowych, stosowanych środków technicznych i organizacyjnych, lub dokonywania audytu w miejscach, w których są przetwarzane powierzone dane osobowe.

§ 9.

1. Przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych w zgodzie z przepisami RODO oraz postanowieniami zawartymi w Umowie oraz wyłącznie na udokumentowane polecenie Powierzającego.
2. Przetwarzający będzie niezwłocznie informować Powierzającego, jeżeli zdaniem Przetwarzającego wydane mu polecenie lub zalecenie stanowi naruszenie RODO lub innych przepisów dotyczących ochrony danych.
3. Przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie powierzonych danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w tym środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania, o których mowa w art. 32 RODO. W związku z powyższym będzie w szczególności:
   1) stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, zapewniające ich poufność, integralność, dostępność i odporność systemów informatycznych służących do ich przetwarzania oraz usług przetwarzania danych osobowych,
   2) przetwarzać powierzone dane osobowe w taki sposób, aby zabezpieczyć je przed udostępnianiem ich osobom nieupoważnionym do ich przetwarzania, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów RODO oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem,
   3) oceniać regularnie skuteczność zastosowanych środków technicznych i organizacyjnych zapewniających bezpieczeństwo powierzonych danych osobowych,

4) zachowywać w poufności wszystkie powierzone dane osobowe, a także zachowywać w poufności informacji o stosowanych sposobach zabezpieczenia danych osobowych, również po rozwiązaniu Umowy lub zakończeniu jej realizacji.

§ 10.

1. Przetwarzający niezwłocznie poinformuje Powierzającego o:
   1) wszelkich przypadkach naruszenia obowiązków dotyczących ochrony powierzonych do przetwarzania danych osobowych, naruszenia tajemnicy tych danych osobowych lub ich niewłaściwego wykorzystania;
   2) wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony powierzonych do przetwarzania danych osobowych prowadzonych w szczególności przez organ właściwy ds. ochrony danych osobowych, policję lub sąd.
2. Przetwarzający zobowiązuje się do udzielenia Powierzającemu, na każde jego żądanie, informacji na temat przetwarzania powierzonych do przetwarzania danych osobowych.
3. Przetwarzający biorąc pod uwagę charakter przetwarzania, będzie pomagać Powierzającemu, poprzez odpowiednie środki techniczne i organizacyjne w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO.
4. Przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomagać będzie Powierzającemu w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO; w szczególności, Przetwarzający zgłasza Powierzającemu, bez zbędnej zwłoki, naruszenie ochrony powierzonych danych osobowych zgodnie z art. 33 ust. 2 oraz przekazuje informacje niezbędne Powierzającemu do zgłoszenia naruszenia ochrony danych organowi nadzorczemu, o którym mowa w art. 33 ust. 3 RODO.

§ 11.

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. Umowa zaczyna obowiązywać z dniem jej podpisania przez prawidłowo umocowanych przedstawicieli Stron, na okres .....
3. W związku z rozwiązaniem lub wygaśnięciem Umowy, Przetwarzający zobowiązuje się do zaprzestania wszelkich czynności przetwarzania powierzonych danych osobowych oraz usunięcia tych danych z nośników Przetwarzającego w sposób uniemożliwiający ich odczytanie lub wykorzystanie
4. Strony przystąpią do wykonania umowy niezwłocznie po jej zawarciu.
5. W sprawach nieuregulowanych Umową zastosowanie mają przepisy Kodeksu cywilnego, RODO i innych właściwych przepisów prawa.

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

Powierzający	**Przetwarzający**
.....	.....

W Ó J T
mgr Andrzej Benedyk

UWAGA: Treść zapisów umowy powierzenia nie ma charakteru zamkniętego i może być w każdym przypadku odpowiednio modyfikowana na potrzeby zawieranej umowy na realizację usług/ wykonanie prac.

*niepotrzebne przekreślić

Załącznik nr 7
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

WYKAZ ZAWARTYCH UMÓW POWIERZENIA

L.p.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Nr umowy powierzenia	Zakres powierzonych danych – nazwa czynności przetwarzania

WÓJT
mgr Andrzej Benedyk

Załącznik nr 8
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH DLA URZĘDU GMINY ŻOŁYNIA

		Dane kontaktowe
Nazwa administratora	**Urząd Gminy Żołynia**	**ul. Rynek 22, 37-110 Żołynia**
Imię i nazwisko inspektora danych	**Anna Podgórska - Kielar**	**apodgorska@zolynia.pl, tel. 17 224 30 18**

Rejestr opracowano zgodnie z art. 37 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).

SPIS KART W REJESTRZE CZYNNOŚCI PRZETWARZANIA

NR KARTY	NAZWA CZYNNOŚCI PRZETWARZANIA

KARTA NR 1

Nazwa czynności przetwarzania	
Referat, stanowisko pracy	
Cel przetwarzania	
Kategorie osób	
Kategorie danych	
Podstawa prawna	
Źródło danych	
Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	
Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy)	
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	
Kategorie odbiorców (innych niż podmiot przetwarzający)	
Nazwa systemu lub oprogramowania	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	
DPIA (jeśli tak, lokalizacja raportu)	
Transfer do kraju trzeciego lub organizacji międzynarodowej i dokumentacja odpowiednich zabezpieczeń	

WÓJT
mgr Andrzej Benedyk

Załącznik nr 9
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

Klauzula zgody na przetwarzanie danych osobowych

Zgadzam się na przetwarzanie moich danych osobowych przez pracowników Urzędu Gminy Żołynia w celu .....

Wiem, że podanie danych jest dobrowolne a podstawą ich przetwarzania moja zgoda.

Zostałem poinformowany, że:

1. Administratorem moich danych osobowych jest Gmina Żołynia z siedzibą ul. Rynek 22, 37-110 Żołynia, zwana dalej administratorem; administrator prowadzi operacje przetwarzania Pani/Pana danych osobowych.
2. Inspektorem ochrony danych osobowych u administratora jest Pani Anna Podgórska – Kielar, e-mail: apodgorska@zolynia.pl.
3. Przysługuje mi prawo dostępu do treści danych oraz ich sprostowania, usunięcia lub ograniczonego przetwarzania, a także prawo sprzeciwu, zażądania zaprzestania przetwarzania i przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie oraz prawo do wniesienia skargi do organu nadzorczego tj. do Prezesa Urzędu Ochrony Danych Osobowych.
4. Podanie danych jest dobrowolne lecz niezbędne do realizacji .....
5. Dane udostępnione przez mnie nie będą podlegały udostępnieniu do państw trzecich lub organizacji międzynarodowych. Odbiorcami danych mogą być tylko instytucje upoważnione z mocy prawa.
6. Dane udostępnione przeze mnie nie będą podlegały profilowaniu (forma zautomatyzowanego przetwarzania danych osobowych).
7. Dane osobowe podane przeze mnie będą przechowywane przez okres .....

W przypadku jakichkolwiek wątpliwości czy pytań w zakresie przetwarzania danych osobowych mogę skontaktować się z Inspektorem Ochrony Danych w Urzędzie Gminy:

a) listownie na adres Urzędu Gminy w Żołyni;
b) telefonicznie 17 224 30 18;
c) e-mailowo apodgorska@zolynia.pl.

WÓJT
mgr Andrzej Beneuyk

.....

(podpis osoby udzielającej zgody)

Załącznik nr 10
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

Informacja o przetwarzaniu danych osobowych (klauzula informacyjna dotycząca przetwarzania danych osobowych)

Informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Gmina Żołynia z siedzibą ul. Rynek 22, 37-110 Żołynia, zwana dalej administratorem; administrator prowadzi operacje przetwarzania Pani/Pana danych osobowych.
2. Inspektorem ochrony danych osobowych u administratora jest Pani Anna Podgórska – Kielar, e-mail: apodgorska@zolynia.pl.
3. Celem zbierania danych jest realizacja ustawowych zadań Wójta Gminy Żołynia.
4. Przysługuje Pani/Panu prawo dostępu do treści danych oraz ich sprostowania, usunięcia lub ograniczonego przetwarzania, a także prawo sprzeciwu, zażądania zaprzestania przetwarzania i przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie oraz prawo do wniesienia skargi do organu nadzorczego tj. do Prezesa Urzędu Ochrony Danych Osobowych.
5. Podanie danych jest dobrowolne lecz niezbędne do realizacji ustawowych zadań Wójta Gminy Żołynia.
6. Dane udostępnione przez Panią /Pana nie będą podlegały udostępnieniu do państw trzecich lub organizacji międzynarodowych. Odbiorcami danych mogą być tylko instytucje upoważnione z mocy prawa.
7. Dane udostępnione przez Panią/Pana nie będą podlegały profilowaniu (forma zautomatyzowanego przetwarzania danych osobowych).
8. Dane osobowe będą przechowywane przez okres określony przepisami prawa.

W przypadku jakichkolwiek wątpliwości czy pytań w zakresie przetwarzania danych osobowych może się Pani/Pan kontaktować z Inspektorem Ochrony Danych w Urzędzie Gminy:

a) listownie na adres Urzędu Gminy w Żołyni;
b) telefonicznie 17 224 30 18;
c) e-mailowo apodgorska@zolynia.pl .

WÓJT
mgr Andrzej Benedyk

Załącznik nr 11
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

Raport o naruszeniu danych osobowych

1. **Opis naruszenia ochrony danych osobowych**

W dniu …….. zidentyfikowano naruszenie ochrony danych osobowych w zakresie ujawnienia (wskazać rodzaj danych osobowych):

---

2. **Lokalizacja zdarzenia, okoliczności towarzyszące oraz przybliżona liczba osób/ wpisów danych których dotyczy naruszenie**

……

3. **Możliwe konsekwencje naruszenia ochrony danych osobowych**

……

4. **Opis środków zastosowanych lub proponowanych do zastosowania w celu zaradzenia naruszeniu ochrony danych osobowych**

……
……
……

WÓJT
mgr Andrzej Benedy

Załącznik nr 12
do Polityki ochrony danych osobowych
w Urzędzie Gminy Żołynia

Zawiadomienie o naruszeniu danych osobowych

Informuję, że w dniu ..... doszło do naruszenia Pani/Pana danych osobowych w zakresie ujawnienia następujących danych osobowych:
.....
.....
.....
Naruszenie zostało spowodowane ..... (np. włamaniem/ kradzieżą danych z bazy....., nieprawidłowym przesłaniem danych przez pracownika, złym zabezpieczeniem danych itp.).

Wobec powyższego istnieje duże ryzyko kradzieży Pani/Pana tożsamości, co może spowodować niekorzystne straty (np. utrata dobrego imienia) w przypadku wykorzystania tych danych przez osoby nieuprawnione w sposób niezgodny z prawem.

W celu zminimalizowania negatywnych skutków naruszenia, o którym Panią/Pana informuję proszę jak najszybciej zastrzec dowód tożsamości/ zmienić hasło dostępu.....

Ze swej strony obiecuję zgłosić zdarzenie do odpowiednich organów ścigania.

Bardzo przepraszamy za niedogodności, dodatkowe informacje można uzyskać pod numerem telefonu: .....

WÓJT
mgr Andrzej Benedyk