Załącznik do zarządzenia nr 23/2018 Wójta Gminy Janowice Wielkie z dnia 24 maja 2018 r.
w sprawie polityki bezpieczeństwa i instrukcji zarzadzania systemami informatycznymi
w Urzędzie Gminy w Janowicach Wielkich zgodnie z zasadami RODO

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Kod dokumentu:	RODO
Wersja:	0.1
Data wersji:	14.05.2018
Utworzony przez:	Adam Szumowski
Zatwierdzony przez:	K. Kowalski
Poziom poufności:	Do użytku wewnętrznego

Historia zmian

Data	**Wersja**	**Utworzona przez**	**Opis zmiany**
2018-05-14	0.1	Adam Szumowski	Pierwsza wersja dokumentu

Spis treści

1. Cel, zakres i użytkownicy

Realizując postanowienia art. 19 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) **wprowadza się „Politykę bezpieczeństwa danych osobowych w Urzędzie Gminy w Janowicach Wielkich"** (zwaną dalej Polityką Bezpieczeństwa).
Niniejsza Polityka Bezpieczeństwa jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych.
Polityka Bezpieczeństwa ma zastosowanie do ochrony danych osobowych przetwarzanych w Urzędzie Gminy w Janowicach Wielkich w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.
Użytkownikami niniejszego dokumentu są wszyscy pracownicy Urzędu Gminy w Janowicach Wielkich, jak również odnośne podmioty zewnętrzne.

2. Dokumenty referencyjne

Instrukcja Zarządzania Systemem w Urzędzie Gminy w Janowicach Wielkich

3. Określenia i skróty użyte w Polityce Bezpieczeństwa

Poufność – właściwość informacji zapewniająca jej dostęp wyłącznie dla osób uprawnionych.
Integralność – właściwość informacji zapewniająca możliwość dokonywania w niej zmian tylko przez uprawnione osoby lub procesy, w dozwolony sposób.
Dostępność – właściwość informacji zapewniająca możliwość dostępu do tej informacji przez uprawnione osoby w każdym czasie, gdy dana informacja jest potrzebna.
Bezpieczeństwo informacji – zapewnienie poufności, integralności oraz dostępności informacji.
Polityka - rozumie się przez to Politykę Bezpieczeństwa Danych Osobowych w Urzędzie Gminy w Janowicach Wielkich;
Instrukcja - rozumie się przez to Instrukcję Zarządzania Systemami Informatycznymi w Urzędzie Gminy w Janowicach Wielkich;
Administrator Danych – dalej zwany też AD - Urząd Gminy w Janowicach Wielkich, reprezentowany przez Wójta Gminy Janowice Wielkie, decydującego o celach i środkach przetwarzania danych osobowych;
Inspektor Ochrony Danych - osobę powołaną przez AD w Urzędzie Gminy w Janowicach Wielkich, wpisaną do prowadzonego przez organ nadzorczy rejestru inspektorów ochrony danych, zwaną dalej „IOD";
Administrator Systemów Informatycznych (ASI) – osobę wyznaczoną przez AD, odpowiedzialną za infrastrukturę techniczną systemów;
Rozporządzenie - 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)
Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
Zgoda 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;
Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
Użytkownik - pracownik Urzędu Gminy w Janowicach Wielkich, posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
Zabezpieczenie systemu informatycznego - należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
Nośnik komputerowy (wymienny) - nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde, dysku flash, pendrive;
Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
Identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie.
Urząd – należy przez to rozumieć Urząd Gminy w Janowicach Wielkich

4. Obszary przetwarzania danych osobowych

4.1. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Administrator Danych Osobowych przy ustalaniu środków bezpieczeństwa wdraża odpowiednie środki bezpieczeństwa w szczególności minimalizację przetwarzanych danych osobowych, ochronę danych w fazie projektowania oraz domyślną ochronę danych osobowych. Ustalanie środków bezpieczeństwa jest ściśle związane z przeprowadzanym regularnie procesem oceny skutków dla ochrony danych osobowych. Poszczególne formy zabezpieczeń są przedmiotem regularnych audytów w celu oceny ich skuteczności i mierzenia stopnia ich realizacji.

4.1.1. Zabezpieczenia organizacyjne

1) Został wyznaczony i zgłoszony do organu nadzorczego inspektor ochrony danych nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych, określenie systemu przetwarzania danych osobowych,
2) Został wyznaczony Administrator Systemów Informatycznych,
3) Określono właścicieli zasobów danych osobowych,
4) Została opracowana i wdrożona polityka bezpieczeństwa,
5) Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
6) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,
7) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
8) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
9) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
10) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
11) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe,
12) Wyznacza się strefy podwyższonego bezpieczeństwa, gdzie całkowicie zabrania się przebywania osób nieuprawnionych: [Serwerownia, Archiwum]
13) Dochowuje się staranności zabezpieczenia danych przy ich gromadzeniu oraz udostępnianiu,
14) Określono postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych.

4.1.2. Zabezpieczenia ochrony fizycznej danych osobowych

Zabezpieczenia fizyczne ochrony danych osobowych określone zostały w **załączniku nr 1** do Polityki Bezpieczeństwa - „**Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe**". Dodatkowo określono obszar przetwarzania danych osobowych w **załączniku nr 2** – **„Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe"**.

4.1.3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

4.1.4. Zabezpieczenia narzędzi programowych i baz danych

Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

5. Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

5.1. Uprawnienia Inspektora Ochrony Danych

W celu realizacji powierzonych zadań IOD w Urzędzie Gminy w Janowicach Wielkich ma prawo:

1) kontrolować komórki organizacyjne Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia na piśmie kierownikom komórek organizacyjnych Urzędu w zakresie bezpieczeństwa danych osobowych – pod warunkiem natychmiastowego poinformowania AD o takiej potrzebie;
3) informować AD o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

5.2. Obowiązki Inspektora Ochrony Danych

Obowiązki Inspektora Ochrony Danych są zgodne z art. 34 Rozporządzenia:

1) informowanie administratora oraz pracowników zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy rozporządzenia oraz na mocy innych przepisów prawa Unii i prawa Polski dotyczących ochrony danych;
2) monitorowanie przestrzegania rozporządzenia, innych przepisów prawa Unii i prawa Polski dotyczących ochrony danych oraz realizowanie polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział obowiązków, działania podnoszące świadomość i szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) przedstawianie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego wobec organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownym przypadku prowadzenie konsultacji we wszelkich innych sprawach.

5.3. Obowiązki właścicieli zasobów danych osobowych

Administrator Danych osobowych wyznacza właścicieli zasobów danych osobowych. Rolę właścicieli zasobów danych osobowych pełnią kierownicy referatów. Do obowiązków właścicieli zasobów danych osobowych należy w szczególności:

1) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez kierowane referaty;
2) bieżące przekazywanie informacji o czynnościach przetwarzania danych osobowych w referacie;
3) udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
4) przestrzeganie obowiązków dotyczących obszaru przetwarzania, zastosowania zabezpieczeń zbiorów;
5) zapoznawanie pracowników mających dostęp do danych osobowych z zasadami bezpieczeństwa podczas szkolenia stanowiskowego.

5.4. Obowiązki Administratora Systemu Informatycznego

Administrator Systemu Informatycznego odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu Gminy w Janowicach Wielkich. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności

1) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie Gminy w Janowicach Wielkich;
2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
3) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;
4) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie Gminy w Janowicach Wielkich, w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;
5) nadzór nad przesyłaniem danych osobowych drogą teletransmisji;

6) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;
7) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
8) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;
9) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
10)podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

5.5. Obowiązki Stanowiska ds. kadrowych

1) Wydawanie, zbieranie i ewidencjonowanie oświadczeń osób zatrudnianych na podstawie umowy o pracę, umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy; wzór formularza oświadczenia stanowi **załącznik nr 3 – „Oświadczenie o zachowaniu poufności"** do Polityki Bezpieczeństwa Danych Osobowych;
2) Przygotowywanie i przekazywanie do podpisu Administratorowi Danych upoważnień do przetwarzania danych osobowych stanowiących **załącznik nr 4 – „Upoważnienie do przetwarzania danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych;
3) Prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, wzór ewidencji stanowi **załącznik nr 5 – „Ewidencja osób upoważnionych do przetwarzania danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych.

6. Gromadzenie danych osobowych

Dane osobowe przetwarzane w Urzędzie Gminy w Janowicach Wielkich mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

6.1. Wykorzystywanie danych

Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.
Jeżeli dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, AD jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

7. Obowiązek informacyjny

Kierownicy komórek organizacyjnych Urzędu Gminy w Janowicach Wielkich, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:
1) tożsamości i danych kontaktowych Administratora Danych Osobowych;
2) danych kontaktowych Inspektora Ochrony Danych;
3) celach przetwarzania danych osobowych lub prawnie uzasadnionych interesach realizowanych przez administratora;
4) informacjach o odbiorcach i kategoriach odbiorców , jeżeli istnieją;
5) okresie bądź kryteriach ustalania okresu przechowywania danych osobowych
6) prawie wglądu do treści swoich danych oraz możliwości ich sprostowania, usunięcia, ograniczenia przetwarzania lub prawie do wniesienia sprzeciwu wobec przetwarzania danych oraz o prawie do przenoszenia danych;
7) w przypadku wyrażenia zgody na przetwarzanie danych osobowych o możliwości jej cofnięcia;
8) prawie do wniesienia skargi do organu nadzorczego;
9) dobrowolności bądź wymogu ustawowym podania danych osobowych oraz o konsekwencjach niepodania danych.
W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 14 Rozporządzenia. W celu realizacji obowiązku informacyjnego stosuje się klauzule informacyjne określone w **załączniku nr 6 – „Wzorce**

stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych" do Polityki Bezpieczeństwa Danych Osobowych**.**

8. Zgody na przetwarzanie danych osobowych

Jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanej danych osobowych, o której mowa w artykule 6 ust. 1 pkt a) rozporządzenia Urząd Gminy w Janowicach Wielkich dba, aby zgody były wyrażane dobrowolnie oraz żeby były zrozumiałe. Stosowane oświadczenia woli w Urzędzie zostały określone w **załączniku nr 6 – „Wzorce stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych**.**
W przypadku zbierania zgód należy poinformować osobę o możliwości jej wycofania, Urząd nie ogranicza form wycofania zgód na przetwarzanie danych osobowych.

9. Udostępnienie danych osobowych

AD udostępnia dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
2) na podstawie umowy z innym podmiotem, w ramach, której istnieje konieczność udostępnienia danych;
3) na podstawie wniosku osoby, której dane dotyczą.

Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi **załącznik nr 7 – „Wniosek o udostępnienie danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych.
Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje niezwłocznie.
Wniosek o udostępnienie przekazywany jest do właściciela zasobów danych osobowych, który podejmuje decyzję o udostępnieniu i ewidencjonuje przypadki udostępnień danych osobowych w komórce organizacyjnej przykład ewidencji stanowi **załącznik nr 8 – „Ewidencja udostępnionych danych osobowych komórki organizacyjnej"** do Polityki Bezpieczeństwa Danych Osobowych.

9.1. Odmowa udostępnienia danych

Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

10. Ochrona przetwarzania danych osobowych

10.1. Obowiązki podmiotu przetwarzającego i powierzenie danych

Powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu odbywa się zgodnie z art. 22 Rozporządzenia na podstawie umowy zawartej na piśmie pomiędzy AD a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
Właściciel zasobów danych osobowych informuje Inspektora o zamiarze powierzenia danych osobowych do przetwarzania. Inspektor przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
W projekcie umowy należy wyspecyfikować prawa i obowiązki administratora oraz podmiotu przetwarzającego w szczególności:
1) Stosowanych środków bezpieczeństwa w szczególności zasady uwzględniania ochrony danych w fazie projektowania oraz zasadę domyślnej ochrony danych
2) Działanie tylko i wyłącznie zgodnie z poleceniami administratora;
3)Zapewnienie o zachowaniu poufności i zachowania w tajemnicy danych osobowych;
4) Udzielanego wsparcia w zakresie przestrzegania przepisów o prawach osób, których dane dotyczą;
5) Kwestie usunięcia lub zwrócenia danych osobowych po zakończeniu świadczenia usługi;
6) Udostępnianie i przekazywanie informacji dla właściwej ochrony danych osobowych;

7) Reguluje kwestie podpowierzenia danych osobowych i dalszego ich przekazywania.
8) Obowiązku zgłaszania naruszeń do Administratora Danych Osobowych.

Projekt umowy jest przedkładany przez Inspektora do akceptacji i podpisu AD. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 9 – „Umowa powierzenia przetwarzania danych osobowych – wzorzec"** do Polityki Bezpieczeństwa Danych osobowych. Urząd Gminy w Janowicach Wielkich ewidencjonuje przypadki powierzeń przetwarzania danych osobowych, **załącznik nr 10 „Rejestr podmiotów przetwarzających, którym powierzono przetwarzanie danych osobowych"**.

11. Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

Przepisy niniejszego rozdziału stosuje się w przypadku:
1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;
2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

Zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

11.1. Przypadki naruszenia bezpieczeństwa danych osobowych

Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

11.2. Postępowanie w razie wykrycia naruszeń

W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub Inspektora (ewentualnie osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.

Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;
2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;
4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

IOD podejmuje działania mające na celu:
1) minimalizację negatywnych skutków zdarzenia;
2) wyjaśnienie okoliczności zdarzenia;
3) zabezpieczenie dowodów zdarzenia,
4) umożliwienie dalszego bezpiecznego przetwarzania danych.

Dla realizacji celów określonych powyżej IOD ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

Zgodnie z art. 30 Rozporządzenia po przeprowadzonej analizie przypadku naruszenia oraz możliwych konsekwencji wystąpienia naruszenia dla praw i wolności osób fizycznych IOD opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi **załącznik nr 11 – „Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych. IOD przekazuje raport do Administratora Danych Osobowych, który podejmuje decyzje w ciągu 72 godzin po stwierdzeniu naruszenia o zgłoszeniu przypadku naruszenia organowi nadzorczemu.

Zgłoszenie powinno zawierać co najmniej:
a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wykazów danych osobowych, których dotyczy naruszenie;
b) imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) możliwe konsekwencje naruszenia ochrony danych osobowych;
d) środki zastosowane lub proponowane przez administratora w celu naprawy naruszenia ochrony danych osobowych, w tym w stosownym przypadku zminimalizowania jego ewentualnych negatywnych skutków.

12. Rejestr czynności przetwarzania

Administrator zgodnie z obowiązkiem wynikającym z art. 30 ust. 1 Rozporządzenia prowadzi wewnętrzny rejestr czynności przetwarzania stanowiący **załącznik nr 12 – „Rejestr czynności przetwarzania danych osobowych"** do Polityki Bezpieczeństwa Danych Osobowych. Rejestr jest udostępniany na żądanie organu nadzorczego.

13. Rejestr wszystkich kategorii czynności przetwarzania

W sytuacji gdy Urząd staje się podmiotem przetwarzającym na polecenie innych administratorów danych, sytuacja ta jest odnotowywana w prowadzonym wewnętrznie rejestrze wszystkich kategorii czynności przetwarzania stanowiący **załącznik nr 13 – „Rejestr wszystkich kategorii czynności przetwarzania"** do Polityki Bezpieczeństwa Danych Osobowych. Rejestr prowadzony jest zgodnie z obowiązkiem wynikającym z art. 30 rozporządzenia, rejestr jest udostępniany na żądanie organu nadzorczego.

14. Ocena skutków dla ochrony danych

Celem niniejszej procedury jest zdefiniowanie metodyki oceny skutków dla ochrony danych osobowych związanymi z przetwarzaniem informacji oraz określenie akceptowalnych poziomów ryzyk.

14.1. Proces

Ocena skutków dla ochrony danych osobowych wykonywane jest z użyciem Tabeli szacowania ryzyka oraz rejestru czynności przetwarzania. Proces szacowania skutków jest koordynowany przez IOD i ASI, identyfikacja zagrożeń i podatności jest wykonywana przez właścicieli aktywów, natomiast szacowanie konsekwencji oraz prawdopodobieństwa jest wykonywane przez właścicieli ryzyka.

14.1.1. Aktywa, podatności i zagrożenia

Pierwszym krokiem w ocenie skutków dla ochrony jest zidentyfikowanie wszystkich czynności przetwarzania będących w zakresie ochrony danych osobowych – oznacza to wszystkie operacje, które mogą wpływać na poufność, integralność i dostępność informacji w Urzędzie. Podczas identyfikacji operacji, konieczne jest także określenie ich właścicieli – osób lub jednostek organizacyjnych odpowiedzialnych za poszczególne aktywa.
Kolejnym krokiem jest identyfikacja wszystkich zagrożeń i podatności związanych z poszczególnymi aktywami. Identyfikacji zagrożeń i podatności dokonuje się z użyciem katalogów znajdujących się w Tabeli szacowania ryzyka. Poszczególne aktywa mogą być związane z więcej niż jednym zagrożeniem, a każde zagrożenie może być związane z więcej niż jedną podatnością.

14.1.2. Określanie właścicieli ryzyka

Dla każdego ryzyka należy określić właściciela ryzyka, czyli osobę lub jednostkę organizacyjną odpowiedzialną za to ryzyko. Osoba ta może być jednocześnie właścicielem aktywu.

14.1.3. Konsekwencje i prawdopodobieństwo

Gdy właściciele ryzyk zostali już określeni, należy dla każdego aktywu oraz każdej kombinacji zagrożenie-podatność oszacować liczbowo znaczenie skutków zdarzenia, w którym dana podatność została wykorzystana przez dane zagrożenie:

Skutki niewielkie	0	Utrata poufności, dostępności lub integralności nie wpływa na przepływy pieniężne w Urzędzie, zobowiązania umowne lub prawne lub jej reputację.
Skutki średnie	1	Utrata poufności, dostępności lub integralności powoduje konsekwencje finansowe oraz ma niski lub średni wpływ na zobowiązania prawne, umowne lub reputację Urzędu.
Skutki znaczące	2	Utrata poufności, dostępności lub integralności ma znaczący i/lub natychmiastowy wpływ na przepływy pieniężne w Urzędzie, jej działanie, zobowiązania prawne lub

		umowne i/lub jej reputację.

Po oszacowaniu skutków konieczne jest określenie prawdopodobieństwa zdarzenia, tj. prawdopodobieństwa, że dane zagrożenie wykorzysta podatność danego aktywu:

Prawdopodobieństwo niskie	0	Istniejące zabezpieczenia są silne i zapewniały dotychczas odpowiedni poziom ochrony. Nie oczekuje się w przyszłości nowych incydentów.
Prawdopodobieństwo średnie	1	Istniejące zabezpieczenia w większości przypadków zapewniały odpowiedni poziom ochrony. Nowe incydenty są możliwe, ale nie są wysoce prawdopodobne.
Prawdopodobieństwo wysokie	2	Istniejące zabezpieczenia są nieefektywne. Prawdopodobieństwo incydentów w przyszłości jest wysokie.

Po wprowadzeniu wartości skutków oraz prawdopodobieństwa do Tabeli szacowania ryzyka, poziom ryzyka jest obliczany automatycznie. Istniejące zabezpieczenia wpisuje się w ostatniej kolumnie Tabeli szacowania ryzyka.

14.2. Kryteria akceptacji ryzyka

Wynikowe wartości ryzyka 0, 1 i 2 są ryzykami akceptowalnymi, podczas gdy wartości 3 i 4 są ryzykami nieakceptowalnymi. Należy zaplanować postępowanie z ryzykami nieakceptowalnymi.

14.3. Postępowanie z ryzykiem

Postępowanie z ryzykiem planuje się z użyciem Tabeli szacowania ryzyka wzór tabeli stanowi **załącznik nr 14 – „Tabela szacowania ryzyka"** do Polityki Bezpieczeństwa Danych Osobowych. Za postępowanie z ryzykiem odpowiada IOD i ASI.

Dla każdego ryzyka oszacowanego na poziomie 3 lub 4 należy wybrać jedną lub więcej opcji postepowania z ryzykiem:

1. Wybranie zabezpieczenia;
2. Transfer ryzyka do strony trzeciej – np. poprzez ubezpieczenie ryzyka lub podpisanie innych umów (z dostawcą, partnerem)
3. Uniknięcie ryzyka poprzez zaprzestanie działań, które mogą to ryzyko powodować
4. Akceptacja ryzyka – ta opcja dopuszczalna jest jedynie wtedy, gdy wybór innej opcji postępowania z ryzykiem wiązałby się z kosztami wyższymi niż skutki finansowe incydentu związanego z tym ryzykiem.

Wyboru opcji dokonuje się w Tabeli szacowania ryzyka. Zwykle jest to opcja nr 1 – wybór jednego lub więcej zabezpieczeń. Jeśli dla danego ryzyka wybiera się więcej niż jedno zabezpieczenie, to zabezpieczenia te wymienia się kolejnych wierszach tabeli bezpośrednio pod wierszem zawierającym dane ryzyko.

14.4. Regularne przeglądy dotyczące szacowania ryzyka i postępowania z ryzykiem

Właściciele ryzyka muszą dokonywać przeglądów istniejących ryzyk, określać nowe ryzyka oraz odpowiednio aktualizować Tabelę szacowania ryzyka. Przeglądu takiego należy dokonywać raz w roku – lub częściej w przypadku znaczących zmian organizacyjnych, zmian w stosowanych technologiach, celach przetwarzania danych osobowych Urzędu Gminy w Janowicach Wielkich.

15. Załączniki

- Załącznik 1: Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe
- Załącznik 2: Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe
- Załącznik 3: Oświadczenie o zachowaniu poufności
- Załącznik 4: Upoważnienie do przetwarzania danych osobowych
- Załącznik 5: Ewidencja osób upoważnionych do przetwarzania danych osobowych
- Załącznik 6: Wzorce stosowanych klauzul informacyjnych i zgód na przetwarzanie danych osobowych
- Załącznik 7: Wniosek o udostępnienie danych osobowych
- Załącznik 8: Ewidencja udostępnionych danych osobowych komórki organizacyjnej
- Załącznik 9: Umowa powierzenia przetwarzania danych osobowych – wzorzec
- Załącznik 10: Rejestr podmiotów przetwarzających, którym powierzono przetwarzanie danych osobowych
- Załącznik 11: Raport z naruszenia bezpieczeństwa zasad ochrony danych osobowych
- Załącznik 12: Rejestr czynności przetwarzania danych osobowych
- Załącznik 13: Rejestr wszystkich kategorii czynności przetwarzania
- Załącznik 14: Tabela szacowania ryzyka

16. Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 14.05.2018 r. Zarządzającym wobec niniejszego dokumentu jest IOD, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację niniejszego dokumentu, co najmniej raz w roku. W ocenie efektywności i właściwości niniejszego dokumentu należy wziąć pod uwagę następujące kryteria:

- liczbę pracowników i podmiotów zewnętrznych, których dotyczy proces przetwarzania danych osobowych, a którzy nie zapoznali się z niniejszym dokumentem;
- zgodność dokumentacji przetwarzania danych osobowych z przepisami prawa, obowiązkami branżowymi, zobowiązaniami umownymi oraz innymi dokumentami wewnętrznymi organizacji;
- efektywność wdrożenia i obsługi procesu danych osobowych;
- podział odpowiedzialności za wdrożenie dokumentacji przetwarzania danych osobowych.