ZARZĄDZENIE NR 76
WÓJTA GMINY SIENNO

z dnia 17 grudnia 2019 r.

w sprawie zatwierdzenia dokumentacji dotyczącej ochronę przetwarzanych danych osobowych w Urzędzie Gminy Sienno

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 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 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.) zarządza się, co następuje:

§ 1. 1. Zatwierdza się „Politykę bezpieczeństwa w Urzędzie Gminy Sienno" stanowiącą załącznik nr 1 do zarządzenia.

2. Zatwierdza się „Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy Sienno" stanowiącą załącznik nr 2 do zarządzenia.

3. Ustala sie wzór upoważnienia do przetwarzania danych osobowych stanowiący załącznik nr 3 do zarządzenia.

§ 2. Wykonanie zarządzenia powierza się sekretarzowi gminy.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1 do zarządzenia Nr 76

Wójta Gminy Sienno

z dnia 17 grudnia 2019 r.

Polityka bezpieczeństwa
w Urzędzie Gminy Sienno

1. Wstęp

Polityka bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań rozporządzenia PE i RE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, zwane dalej "RODO".

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z tym rozporządzeniem, a także usprawnienie i usystematyzowanie organizacji pracy Administratora.

1.1. Definicje

1/ Administrator (danych) - to Wójt Gminy Sienno z siedzibą w Siennie ul. Rynek 36/40;

2/ RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 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 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.);

3/ Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej;

4/ Przetwarzanie danych osobowych - to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych;

5/ Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

6/ Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych

7/ Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić;

8/ Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania.

Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych;

9/ Podmiotem danych - jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

10/ Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

11/ Podmiot przetwarzający (procesor) - to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora;

12/ Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu i pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

13/ Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów) pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

14/ Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach;

15/ Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

16/ Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2. **Ocena skutków (analiza ryzyka)**

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować tę procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem oraz po wyrażeniu przez niego opinii.

2.1.**Opis operacji przetwarzania (inwentaryzacja aktywów)**

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.

2.2.**Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)**

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia wobec nich obowiązków prawnych. Należy przede wszystkim zapewnić, że :

1) dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO);
2) dane te są adekwatne w stosunku do celów przetwarzania;
3) dane te są przetwarzane przez określony czas – zasada ograniczonego czasu;
4) wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody);
5) opracowano klauzule informacyjne dla powyższych osób;
6) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

2.3. Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Analiza ryzyka powinna być dokonana na podstawie raportu oceny ryzyka.

2.4. Plan postępowania z ryzykiem.

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.

2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3. **Upoważnienia**

1) administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
2) każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
3) upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.
4) upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia.
5) administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych.

4. **Instrukcja postępowania z incydentami**

4.1.Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

1) nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł;
2) niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń;
3) niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.

4.2.Postępowanie Administratora danych osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia:

1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków;
2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych;
3) w razie konieczności zainicjowanie działań dyscyplinarnych;
4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości;
5) udokumentowanie prowadzonego postępowania w rejestrze naruszeń bezpieczeństwa.

4.3.Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

1) losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych;
2) losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar;
3) incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym

osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

4.4.Postępowanie Administratora lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:

1) ustalenie czasu zdarzenia będącego incydentem;

2) ustalenie zakresu incydentu;

3) określenie przyczyn, skutków oraz szacowanych zaistniałych szkód,

4) zabezpieczenie dowodów,

5) ustalenie osób odpowiedzialnych za naruszenie,

6) usunięcie skutków incydentu,

7) ograniczenie szkód wywołanych incydentem,

8) zainicjowanie działań dyscyplinarnych,

9) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,

10) udokumentowanie prowadzonego postępowania w rejestrze naruszeń.

4.5.Postępowanie Upoważnionego w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora lub upoważnionej przez niego osoby:

1) powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;

2) zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych;

3) podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

5. **Szkolenia**

1) Każda osoba przed dopuszczeniem do pracy z danymi osobowymi powinna być poddana przeszkoleniu i zapoznana z przepisami RODO.

2) Za przeprowadzenie szkolenia odpowiada Administrator Danych.

3) W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.

4) Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

6. **Rejestr czynności przetwarzania**

W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, Administrator/Inspektor Ochrony Danych taki odpowiedni rejestr prowadzą.

7. **Audyty**

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, przynajmniej raz na rok.

8. **Wykaz zabezpieczeń - zastosowane podkreślono.**

Środki organizacyjne

1. Opracowano i wdrożono politykę bezpieczeństwa.

2. Opracowano i wdrożono instrukcję zarządzania systemem informatycznym.

3. Powołano Administratora Bezpieczeństwa Informacji.

4. Powołano Administratora Systemu Informatycznego.

5. Do przetwarzania danych dopuszczono wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych.

6. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.

7. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.

8. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

9. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;

10. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

11. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco .

12. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.

13. 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.

14. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

15. W podmiocie prowadzi się politykę czystego biurka i ekranu.

Środki ochrony fizycznej danych

1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).

2. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.

3. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.

4. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.

5. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.

6. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.

7. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.

8. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.

9. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.

10. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej niemetalowej szafie.

11. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej metalowej szafie.

12. Zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętym sejfie lub kasie pancernej.

13. Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.

14. Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej metalowej szafie

15. Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętym sejfie lub kasie pancernej.

16. Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.

17. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

18. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.

2. Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.

3. Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

4. Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczono go przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

5. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

6. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.

7. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.

8. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

9. Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.

10. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

11. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.

12. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

13. Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.

14. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.

15. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

16. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

17. Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

Środki ochrony w ramach narzędzi programowych i baz danych

1. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.

2. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

3. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

4. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.

5. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.

6. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

7. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

8. Zastosowano kryptograficzne środki ochrony danych osobowych.

9. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

10. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Załącznik Nr 2 do zarządzenia Nr 76

Wójta Gminy Sienno

z dnia 16 grudnia 2019 r.

Instrukcja

postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Gminy Sienno

I. Istota naruszenia danych osobowych

§ 1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

II. Postępowanie w przypadku naruszenia danych osobowych

§ 2. 1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.

2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:

1) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;

2) dokumentacja jest niszczona bez użycia niszczarki;

3) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;

4) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.;

5) nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych;

6) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

7) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;

8) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;

9) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

10) telefoniczne próby wyłudzenia danych osobowych;

11) kradzież komputerów lub twardych dysków z danymi osobowymi;

12) utrata kontroli nad kopią danych osobowych;

13) maile zachęcające do ujawnienia identyfikatora i/lub hasła;

14) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

15) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";

16) hasła do systemów przechowywane są w pobliżu komputera.

§ 3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5. Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6. Inspektor ochrony danych podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie

w prawidłowości i ciągłości pracy;

2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej;

jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniały naruszeniem,

3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7. Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 1.

§ 8. Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

III. Naruszenie danych osobowych - odpowiedzialność

§ 9. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 10. 1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – Załącznik nr 3.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości

wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i

przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie

innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia

naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu

zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

V. Zawiadamianie osób o naruszeniu ochrony danych osobowych

§ 11. 1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego

ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydany zostaje

publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby,

których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załącznik nr 1

Raport z naruszenia ochrony danych

1. Data ……..……. godzina ……

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

……

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

……
……..…….....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……
……..…….....

5. Podjęte działania:

……

6. Wstępna ocena przyczyn wystąpienia naruszenia:

……

7. Postępowanie wyjaśniające i naprawcze:

……....

…… ……

(podpis pracownika) (data i podpis Inspektora ochrony danych)

Załącznik nr 2

Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych								
Zadanie / problem / incydent	**Źródło zgłoszenia**	**Data rozpoczęcia**	**Data zakończenia**	**Czy koniec?**	**Odpowiedzialny za realizację**	**Przyczyna niezgodności**	**Działanie korygujące / zapobiegawcze**	**Ocena skuteczności**

Załącznik nr 3

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Data ……..... Godzina ……(naruszenia)

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

…….....

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

…….....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu (*opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie);*

…….....

5. Podjęte działania:

…….....

6. Wstępna ocena przyczyn wystąpienia naruszenia (*opisywać możliwe konsekwencje naruszenia ochrony danych osobowych);*

…….....

7. Postępowanie wyjaśniające i naprawcze (*opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków);*

…….

8. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji:.....

……..…….

Załącznik Nr 3 do zarządzenia Nr 76

Wójta Gminy Sienno

z dnia 16 grudnia 2019 r.

Upoważnienie nr ……
do przetwarzania danych osobowych

Na podstawie art. 29 w związku z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej RODO, upoważniam Pana/Panią***** ……
do przetwarzania danych osobowych w zbiorze
……..
……..
(nazwa zbioru)

Upoważnienie wygasa z chwilą ustania Pana/Pani* zatrudnienia w …… /zaprzestania wykonywania przez Pana/Panią***** zadań na podstawie stosunku cywilnoprawnego*, lub z chwilą jego odwołania.

……..(czytelny podpis i pieczątka imienna osoby upoważnionej do wydawania i odwoływania upoważnień)

Oświadczam, że zapoznałem/am się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym RODO, a także z obowiązującym w …… opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia w …… / wykonywania zadań na podstawie stosunku cywilnoprawnego*, jak też po jego ustaniu/po zrealizowaniu zadań wykonywanych na podstawie stosunku cywilnoprawnego*.

…… (czytelny podpis osoby składającej oświadczenie)

Upoważnienie otrzymałem/am

……
(data, podpis)

*****niepotrzebne skreślić