ZARZĄDZENIE NR 68.2024
WÓJTA GMINY KOWALA

z dnia 30 kwietnia 2024 r.

w sprawie aktualizacji dokumentu pn. „Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Kowali - Stępocinie”

Na podstawie art. 31 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2024 r. poz. 609) oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz. Urz. UE L 119 z 04.05.2016, zarządzam co następuje:

§ 1. Zatwierdzam i wprowadzam aktualizację w dokumencie pn. „Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Kowali - Stępocinie" załączonym do niniejszego Zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Kowala

Dariusz Bulski

Załącznik do Zarządzenia nr 68.2024
Wójta Gminy Kowala
z dnia 30 kwietnia 2024 r.

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy w Kowali - Stępocinie

Gmina Kowala
siedziba: ul. Marii Walewskiej 7, 26-624 Kowala - Stępocina
tel: 48/610 17 60
fax: 48/610-17-22
www.kowala.pl www.kowala.biuletyn.net
e-mail: kowala(@kowala.pl

Zatwierdził:
Wójt Gminy Kowala

Dariusz Bulski

Kwiecień 2024 r.

Głównym celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych jest organizacyjne, techniczne i logiczne zabezpieczenie posiadanych danych osobowych oraz cykliczne szkolenia użytkowników systemu ochrony danych osobowych.

Deklaracja

Administrator danych mając świadomość, iż przetwarza dane osobowe deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100% szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich

§1 PRZEPISY OGÓLNE

1. Polityka Bezpieczeństwa Przetwarzania Danych Osobowych (zwana dalej „Polityką") została opracowana na podstawie obowiązujących przepisów prawa:
1) Rozporządzenia Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.l - zwane RODO
2) Konstytucja RP (Dz. U. z 2009 r. nr 114 poz. 946);
3) Ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2019 r. poz. 1791); dalej zwana „UODO";
4) ustawy z dnia 08.03.1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609)

2. Oprócz przepisów prawa zawartych w ust. 1 niniejszego paragrafu, Polityka została opracowana także według zasad Systemu Zarządzania Bezpieczeństwem Informacji - Norma Międzynarodowa ISO/IEC 27001:2017-06, Polska Norma PN-ISO/IEC 27002:2017-06.

3. Administratorem Danych w Gminie Kowala (siedziba: ul. Marii Walewskiej 7, 26-624 Kowala - Stępocina) jest:
a. Gmina Kowala - w sprawach dotyczących zakresu działań i zadań wynikających z ustawy z dnia 08.03.1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609)
b. Urząd Gminy w Kowali – Stępocinie - jako jednostka organizacyjna gminy w sprawach dotyczących świadczenia pomocy Wójtowi w zakresie realizacji jego zadań określonych przepisami prawa.

4. Zakres stosowania:
1) w Urzędzie Gminy w Kowali – Stępocinie przetwarzane są dane osobowe mieszkańców Gminy Kowala, pracowników, kandydatów do pracy, stażystów, osób zatrudnionych na podstawie umów cywilno-prawnych oraz dostawców. Dane te są zebrane w zbiorach danych osobowych - informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej;
2) w Gminie Kowala przetwarzane są dane osobowe uzyskane w zakresie niezbędnym do realizacji zadań gminy na podstawie ustawy z dnia 08.03.1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609).

5. Polityka niniejsza zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych wprowadzonych na podstawie analizy ryzyka zabezpieczeń.
6. Zakresy ochrony danych osobowych określone przez Politykę oraz inne z nią związane dokumenty mają zastosowanie do:

1) wszystkich obecnie istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
2) wszystkich obecnych i przyszłych lokalizacji- budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) obecnych i przyszłych pracowników, stażystów, osób zatrudnionych na podstawie umów cywilno-prawnych i innych osób mających dostęp do informacji podlegających ochronie.

7. Do stosowania zasad określonych przez Politykę oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści, osoby zatrudnione na podstawie umów cywilnoprawnych oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.
8. Zgodnie z Rozporządzeniem 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.L nr 119, str.l - zwane RODO, każdy mieszkaniec ma możliwość zapoznania się z informacjami zawartymi w Klauzuli informacyjnej o przetwarzaniu danych osobowych stanowiącej załącznik nr 1 do niniejszej Polityki. Klauzula została zamieszczona na stronie BIP Gminy Kowala www.kowala.biuletyn.net. stronie www.kowala.pl oraz w gablotach w budynku Urzędu Gminy i wszystkich referatach Urzędu. Ponadto podczas spotkania z pracownikiem Urzędu, każda osoba, której dane dotyczą zostanie poinformowana o przysługujących jej prawach względem ochrony danych osobowych oraz w przypadku konieczności zostanie poproszona o wyrażenie zgody na przetwarzanie jego danych osobowych, o której mowa w dalszej części niniejszej Polityki.

§2 OBJAŚNIENIA

1. Polityka w uporządkowanej formie opisuje działania organizacyjne i techniczne, których celem jest zapewnienie bezpieczeństwa danych osobowych przez Administratora oraz powierzenia danych osobowych wykonawcom w ramach realizowanych projektów lub umów.
2. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach działalności Administratora.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zestaw praw, reguł i zaleceń, regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych przez Administratora.
4. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych przez Administratora rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
5. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp

do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

6. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych.
7. Niniejszą Politykę stosuję się do:

1) danych osobowych:

a. przetwarzanych w systemach informatycznych,
b. zapisanych na zewnętrznych nośnikach informacji,
c. przetwarzanych tradycyjnie.

2) informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:

a. służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
b. dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

8. Bez względu na zajmowane stanowisko w Urzędzie Gminy w Kowali - Stępocinie, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe. W tym celu każda osoba przetwarzająca dane osobowe w zbiorach zgromadzonych przez Administratora oświadcza, iż zapoznała się z Polityką oraz zobowiązuje się do ich stosowania. Wzór Oświadczenia osoby przetwarzającej dane osobowe stanowi załącznik nr 2 do niniejszej Polityki. Ponadto każda osoba przetwarzająca dane osobowe w zbiorach zgromadzonych przez Administratora poświadcza, że uczestniczyła w szkoleniu dotyczącym ochrony danych osobowych - Oświadczenie o przeszkoleniu, którego wzór stanowi załącznik nr 3. a także poprzez złożenie oświadczenia i podpisu w rejestrze, który prowadzi IOD - Rejestr szkoleń, którego wzór stanowi załącznik nr 4 do niniejszej Polityki.
9. **Użytkownik, który przetwarza w zbiorze danych dane osobowe, do których przetwarzania nie jest upoważniony, podlega odpowiedzialności na zasadach określonych w przepisach prawa oraz dyscyplinarnej określonej przepisami Kodeksu pracy.**

§3 DEFINICJE

Użyte w niniejszej Polityce pojęcia oznaczają:

1. „RODO" - Rozporządzenia Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119;
2. „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. „dane szczególnych kategorii" oznaczają dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające:

a. pochodzenie rasowe lub etniczne

b. poglądy polityczne;
c. przekonania religijne lub filozoficzne;
d. stan zdrowia;
e. przynależność partyjna, związkowa lub wyznaniowa;
f. kod genetyczny;
g. nałogi;
h. życie seksualne;
i. skazania i orzeczenia dotyczące mandatów i kar;
j. dane genetyczne, dane biometryczne (w celu jednoznacznego zidentyfikowania osoby) lub dotyczące zdrowia lub seksualności i orientacji seksualnej.

4. „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:
a. zbieranie,
b. utrwalanie,
c. organizowanie,
d. porządkowanie,
e. przechowywanie,
f. adaptowanie lub modyfikowanie,
g. pobieranie,
h. przeglądanie,
i. wykorzystywanie,
j. ujawnianie poprzez przesłanie,
k. rozpowszechnianie lub innego rodzaju udostępnianie,
l. dopasowywanie lub łączenie,
m. ograniczanie, usuwanie lub niszczenie;
5. „ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
6. „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
7. „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
8. „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
9. „administrator" (AD) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Administratorem danych osobowych, którym jest:
a. Gmina Kowala - w sprawach dotyczących zakresu działań i zadań wynikających z ustawy

z dnia 08.03.1990 r. o samorządzie gminnym (Dz. U. z 2024r. poz. 609)

b. Urząd Gminy w Kowali – Stępocinie - jako jednostka organizacyjna gminy w sprawach dotyczących świadczenia pomocy Wójtowi w zakresie realizacji jego zadań określonych przepisami prawa.
10. „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
11. „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia;
12. „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Formularz Zgody na przetwarzanie danych osobowych- wzór stanowi załącznik nr 5.
13. „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
14. „dane genetyczne" oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
15. „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
16. „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;
17. „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
18. „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO, czyli Urząd Ochrony Danych;
19. „inspektor ochrony danych" (IOD) oznacza osobę powołaną przez AD zgodnie z art. 37 RODO do nadzorowania przestrzegania zasad i wymagań w zakresie ochrony danych, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych. Wyznaczenie IOD następuje na podstawie Zarządzenia Wójta Gminy Kowala.
20. „administrator systemów informatycznych" (ASI) oznacza osobę z zakresu informatyki odpowiedzialną za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w systemach informatycznych, wyznaczoną przez AD.
21. „bezpieczeństwo przetwarzania danych osobowych" oznacza zachowanie poufności, integralności i rozliczalności danych osobowych. Dodatkowo mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
22. „system informatyczny" oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
23. „system tradycyjny" oznacza zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze

24. „bezpieczeństwo systemu informatycznego" oznacza wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych oraz ochrona przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub nieuprawnionym pozyskaniem danych osobowych, a także ich utratą (zamierzoną lub przypadkową).
25. „incydent" oznacza pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
26. „integralność danych" oznacza właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
27. „integralność systemu" oznacza nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
28. „identyfikator użytkownika" (LOGIN) oznacza ciąg znaków literowych i cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
29. „hasło" oznacza ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
30. „użytkownik systemu" oznacza osobę posiadającą upoważnienie nadane przez AD i uprawniona do bezpośredniego dostępu do przetwarzania danych osobowych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
31. „nośnik" oznacza narzędzie do zapisywania, przenoszenia i odczytywania danych i informacji na nim zapisanych. Nośnikiem może być urządzenie elektroniczne, optyczne, karty SIM, magnetyczne lub papierowy.
32. „właściciel zbioru danych osobowych" oznacza osobę kierującą komórką organizacyjną, stanowisko samodzielne, odpowiedzialna za ochronę danych osobowych. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
33. „sieć lokalna" oznacza połączenie funkcjonujących w Urzędzie Gminy w Kowali - Stępocinie systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
34. „stacja robocza" oznacza stacjonarny lub przenośny komputer, rozpoznawany przez system IT, wchodzący w skład systemu informatycznego, umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie.
35. „sieć telekomunikacyjna” oznacza sieć telekomunikacyjna w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2024 r., poz. 34).
36. „zalogowanie" oznacza uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 4 SCHEMAT ORGANIZACYJNY

1. Administrator Danych (AD) realizuje zadania w zakresie ochrony danych osobowych, zgodnie z RODO art. 24 oraz prawodawstwie krajowym, w tym:

1) wyznacza cele i środki przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji Administratora Danych oraz technik zabezpieczenia danych osobowych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
3) odwołuje upoważnienia do przetwarzania danych osobowych;
4) wyznacza Inspektora Ochrony Danych oraz określa zakres jego zadań i czynności zgodnie z RODO oraz prawodawstwem krajowym;
5) wyznacza ASI jako właściwego do zapewnienia bezpieczeństwa ochrony danych osobowych w systemach informatycznych i współpracującą z IOD.
6) Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
7) Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
8) Administrator zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.

2. Inspektor Ochrony Danych (IOD) realizuje zadania w zakresie przestrzegania zasad bezpieczeństwo przetwarzania danych osobowych, zgodnie z RODO art. 39 oraz prawodawstwem krajowym, w tym:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz ustawodawstwa krajowego oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania rozporządzenia RODO oraz ustawodawstwa krajowego, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych

z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

6) Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
7) IOD w zakresie swojego działania podlega bezpośrednio AD lub pełnomocnikowi AD lub osobie przez niego upoważnionej.
8) IOD sprawuje nadzór nad kierownikami komórek organizacyjnych urzędu w zakresie przetwarzania danych osobowych w ich komórkach.
9) Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia RODO i ustawodawstwa krajowego.
10) IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

3. Administrator Systemów Informatycznych (ASI) realizuje zadania w zakresie zapewnienia bezpieczeństwa przetwarzania danych osobowych, w tym:

1) Zarządzanie i administrowanie bazami danych.
2) Zarządzanie sprzętem informatycznym w Urzędzie.
3) Zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania.
4) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
5) Zarządzanie i administrowanie serwerami aplikacyjnymi: konfigurowanie, optymalizacja, monitorowanie, analizowanie zdarzeń systemowych, lokalizowanie błędów, diagnostyka i ich usuwanie.
6) Bieżące monitorowanie poziomu bezpieczeństwa w systemie informatycznym, w szczególności bieżącego stanu aktualizacji systemów operacyjnych i serwerów oraz sygnatur programów antywirusowych.
7) Bieżące monitorowanie systemu informatycznego i systemu monitoringu wizyjnego urzędu i przekazywanie informacji o zagrożeniach IOD, a w przypadku jego nieobecności AD.
8) Cykliczne przeglądy i weryfikacja :

a. pomieszczeń dopuszczonych do przetwarzania danych,
b. rozmieszczenia stacji roboczych,
c. sprawności użytkowanego sprzętu, w tym konserwację i likwidację sprzętu i oprogramowania,
d. legalności zainstalowanego oprogramowania,
e. harmonogramu logowania do systemu informatycznego dla poszczególnych użytkowników,
f. systemu informatycznego pod kątem obecności nieuprawnionego i szkodliwego oprogramowania,

9) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacja umów z firmami świadczącymi usługi pogwarancyjne sprzętu komputerowego.
10) Prowadzenie bieżącej ewidencji licencji oprogramowania.
11) Przygotowywanie niezbędnej dokumentacji związanej z prawidłowym funkcjonowaniem sieci informatycznej (w tym: opisy systemów IT i zasilania).
12) Uczestnictwo w pracach projektowych i wdrożeniowych nowych rozwiązań.
13) ASI jest obowiązany do ścisłej współpracy z AD i IOD oraz zgłaszania im wszelkich problemów, incydentów i naruszeń.

§ 5 PROCESY I PROCEDURY

Wprowadzenie niniejszej Polityki ma na celu określenie jednolitych zasad dla całego systemu przetwarzania danych.

1. Procesy i procedury podlegające wdrożeniu to:

1) ochrona przetwarzanych i gromadzonych informacji, w tym danych osobowych dotyczy:

a. zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
b. metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
c. procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
d. ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
e. określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,

2) oszacowanie i zmniejszenie ryzyka utraty informacji,
3) określenia zakresu obowiązków pracowników - w części dotyczącej bezpieczeństwa danych, w tym danych osobowych,
4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych informacji.

2. Powyższe procesy i procedury odnoszą się w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
2) informacji będących własnością Urzędu lub jednostek organizacyjnych gminy, o ile zostały przekazane do Urzędu na podstawie umów lub porozumień,
3) wszystkich nośników danych, na których są lub będą znajdować się informacje podlegające ochronie,
4) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
5) wszystkich obecnych i przyszłych pracowników w rozumieniu przepisów Kodeksu Pracy, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

§ 6 DOSTĘP DO DANYCH OSOBOWYCH

1. Przetwarzanie danych jest zabronione w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Przetwarzanie tych danych jest jednak dopuszczalne, jeżeli:

1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,
2) przepis szczególny zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony,
3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której

dane dotyczą lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

4) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
5) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,
6) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

2. W celu organizacji zasad ochrony, zabezpieczenia i kontroli przetwarzania danych osobowych, AD powołuje Inspektora Ochrony Danych (IOD).
3. W celu prawidłowego funkcjonowania infrastruktury informatycznej (sprzęt, systemy iaplikacje informatyczne) AD powołuje Administratora Systemów Informatycznych (ASI).
4. Dostęp do systemu informatycznego oraz urządzeń z nimi powiązanych możliwy jest wyłącznie na podstawie upoważnienia wydanego przez AD.
5. Dostęp do zbioru danych osobowych oraz ich przetwarzania posiadają wyłącznie osoby wpisane do Ewidencji Wydanych Upoważnień prowadzonego przez IOD.
6. Użytkownicy przetwarzający dane osobowe w systemach informatycznych zobowiązani są do postępowania zgodnie z Instrukcją Zarządzania Systemem Informatycznym - załącznik nr 6 oraz z Instrukcją postępowania w przypadku naruszenia danych osobowych - załącznik nr 7 do Polityki.
7. Użytkownicy zaangażowani w procesie przetwarzania danych osobowych są zobowiązani do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
8. Przed dopuszczeniem do pracy w systemie informatycznym, każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz niniejszą Polityką.
9. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.
10. Zasady udostępniania i przetwarzania danych osobowych:

1) dane osobowe przetwarzane we własnych zbiorach Urzędu można udostępnić wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania z mocy przepisów prawa;
2) zbiory danych udostępnia się na pisemny wniosek, chyba że przepisy prawa stanowią inaczej;
3) wniosek jest składany do IOD, który po analizie przekazuje go bezpośrednio AD.
4) decyzję w sprawie udostępnienia podejmuje AD osobiście po konsultacji z IOD;
5) AD może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób;
6) Upoważnienie do przetwarzania danych osobowych w systemach informatycznych i/lub w zbiorach w wersji papierowej wydaje AD przy kontrasygnacie IOD na wniosek kierownika komórki organizacyjnej lub na wniosek pracownika w przypadku zajmowania przez niego samodzielnego stanowiska. Wzór Wniosku o nadanie/zmianę/odwołanie upoważnienia do przetwarzania danych osobowych w systemach stanowi załącznik nr 8 do Polityki. Wzór Upoważnienia/odwołanie do przetwarzania danych osobowych w systemach stanowi załącznik nr 9 do Polityki.
7) W przypadku osób zatrudnionych na podstawie umów cywilno-prawnych i stażystów, wniosek o nadanie uprawnień do przetwarzania danych osobowych w systemach informatycznych i/lub zbiorach danych osobowych sporządza odpowiednio: Wójt/ Sekretarz / kierownik komórki organizacyjnej;
8) W pozostałych sytuacjach, nadanie uprawnień do przetwarzania danych osobowych należy

skonsultować z IOD;

9) Kierownicy komórek organizacyjnych oraz osoby zajmujące samodzielne stanowiska zobowiązane są na bieżąco i bez zbędnej zwłoki do aktualizacji upoważnień oraz do sporządzenia wniosku o cofnięcie upoważnienia jeżeli sytuacja tego wymaga, np. rozwiązanie stosunku pracy z pracownikiem;
10) I0D odpowiada za prowadzenie ewidencji osób upoważnionych do przetwarzania danych w postaci ewidencji wydanych upoważnień. Wzór Ewidencji wydanych upoważnień do przetwarzania danych osobowych stanowi załącznikiem nr 10.

§ 7 OBOWIĄZEK INFORMACYJNY WZGLĘDEM IOD

1. Użytkownicy przetwarzający dane osobowe zobowiązani są do informowania IOD o ewentualnych incydentach/naruszeniach bezpieczeństwa systemu ochrony danych osobowych we wszystkich administrowanych zbiorach.
2. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana będzie jako naruszenie obowiązków pracowniczych.
3. Nieprzestrzeganie zasad postępowania określonych w niniejszej Polityce stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
4. Tryb postępowania określa Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych załącznik nr 7.

§ 8 UDOSTĘPNIANIE I/LUB POWIERZANIE DANYCH OSOBOWYCH

1. Dane osobowe mogą być uzyskiwane:

1) bezpośrednio od osób, których te dane dotyczą, w zakresie:

a. spełnienia obowiązku wynikającego z przepisów prawa (obowiązkowe);
b. swobodnego i autonomicznego oświadczenia woli (dobrowolne).

2) pozyskiwane w inny sposób niż od osoby, której dane dotyczą;

2. W zasobach osobowych Administratora występują:

a. zbiory trwałe;
b. zbiory doraźne, tymczasowe i techniczne (spisy wyborców, listy uczestników rekrutacji, listy kandydatów/uczestników konkursów itp.).

3. Zbierane dane osobowe, mogą być wykorzystywane wyłącznie do celów, w jakich są lub będą przetwarzane. Po wykorzystaniu danych osobowych, przetwarzane są w postaci uniemożliwiającej identyfikację osób, których dotyczą (anonimizacja danych) lub poddanie procesom archiwizacji, według potrzeb administratora i w zgodności z przepisami prowadzenia archiwizacji.
4. Najważniejsze przesłanki i zasady udostępniania danych:

1) Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
2) Nie ma znaczenia (ujmując problem technicznie) czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd.
3) Udostępnianie i przetwarzania danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
4) Dane osobowe, z wyłączeniem danych szczególnych kategorii, mogą być udostępniane nie w oparciu o przepisy prawa, jeżeli osoba wnioskująca w sposób wiarygodny uzasadni potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.
5) Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające

wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
6) Udostępnione i powierzone dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
7) Udostępnianie danych osobowych rejestrowane jest w Formularzu do odnotowywania udostępniania danych osobowych stanowi załącznik nr 11 do Polityki.

5. W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla Administratora danych może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

1) umowa powinna być zawarta niezależnie od posiadanej umowy określającej relacje obu stron,
2) podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie i celu przewidzianym w umowie,
3) podmiot, któremu powierzono przetwarzanie danych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych oraz spełnić wymagania określone w przepisach RODO,
4) w zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na Administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową,
5) do kontroli zgodności przetwarzania danych przez podmiot, któremu powierzono przetwarzanie danych, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy RODO.

§ 9 OBSZARY PRZETWARZANIA INFORMACJI PRAWNIE CHRONIONYCH, W TYM DANYCH OSOBOWYCH

1. Informacje prawnie chronione, w tym dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania, na które składają się pomieszczenia biurowe Urzędu Gminy w Kowali – Stępocinie oraz części pomieszczeń, gdzie AD prowadzi działalność, czyli:

a) pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania informacji prawnie chronionych, w tym danych osobowych;
b) pomieszczenia, w których przechowuje się zbiory nieinformatyczne, dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające informacje prawnie chronione, w tym dane osobowe;
c) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające informacje prawnie chronione, w tym dane osobowe.

2. Zbiory papierowe, wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych.
3. Niepotrzebne wydruki i inne dokumenty należy bez zbędnej zwłoki na bieżąco niszczyć w niszczarkach.
4. Przebywanie osób nieuprawnionych wewnątrz obszarów przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą AD.
5. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym. Szczegółowa Instrukcja postępowania z kluczami oraz zabezpieczenie pomieszczeń stanowi załącznik nr 12 do niniejszej Polityki

6. Formularz Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 13 do niniejszej Polityki.
7. Formularz Wykaz zbiorów danych osobowych stanowi załącznik nr 14 do niniejszej Polityki.
8. Wykaz systemów informatycznych służących do przetwarzania danych osobowych stanowi załącznik nr 15 do Polityki.
9. Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi oraz sposoby przepływu danych pomiędzy systemami stanowi załącznik nr 16 do niniejszej Polityki.
10. W szczególnie uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) wyłącznie za zgodą AD i na zasadach określonych przez IOD.
11. Zasady działania Punktu Potwierdzającego Profil Zaufany na platformie ePUAP określone są w odrębnym zarządzeniu Wójta Gminy Kowala.
12. W zakresie przetwarzania danych osobowych w systemach finansowo-księgowych, stosuje się również Politykę Rachunkowości oraz Instrukcję kasową.

§ 10 ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, . INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stu procentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność z przetwarzanymi danymi, świadom odpowiedzialności, postępował zgodnie z przyjętymi w niniejszym dokumencie zasadami i minimalizował zagrożenie wynikające z błędów ludzkich.
2. Ochrona danych osobowych przetwarzanych przez Administratora obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych przez Administratora, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
3. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
4. Przetwarzać dane osobowe w systemach informatycznych jak i tradycyjnych zbiorach papierowych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych otrzymane od AD.
5. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
6. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
7. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
8. Zachowanie tajemnicy służbowej obowiązuje pracownika zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
9. IOD i AD są odpowiedzialni za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur w całym systemie urzędu.
10. Techniczne środki zabezpieczające:

1) monitoring wizyjny w obrębie budynku Urzędu Gminy w Kowali - Stępocinie, lokalizacja: ul. Marii Walewskiej 7, Kowala – Stępocina.
2) nadzór elektroniczny stref bezpieczeństwa, grupy interwencyjne poza godzinami pracy

urzędu - lokalizacja siedziby urzędu, każda strefa posiada indywidualny kod aktywacji i dezaktywacji dozoru elektronicznego, znany i przypisany upoważnionej osobie do tej czynności,
3) szyfratory wejścia do budynku lokalizacji Urzędu Gminy w Kowali - Stępocinie,
4) odpowiednie zabezpieczenie w serwerowni urzędu,
5) pełne drzwi do pomieszczeń biurowych z zamkiem zabezpieczającym,
6) szyby o podwyższonej odporności w pomieszczeniach zlokalizowanych na parterze,
7) kasy pancerne do dokumentów kadrowo-płacowych i backup danych i aplikacji IT,
8) atestowane gaśnice przeciwpożarowe w pomieszczeniach biurowych,
9) dedykowana sieć zasilania elektrycznego w lokalizacji budynku Urzędu Gminy w Kowali – Stępocinie dla serwerów oraz urządzeń klasy UPS na wypadek zaniku/braku zasilania elektrycznego w serwerowni urzędu,
10) ochrona przed awarią podsystemu dyskowego.

11. Organizacyjne środki zabezpieczające:
1) indywidualne upoważnienia do dysponowania kluczami do pomieszczeń i budynków,
2) indywidualne kody dostępu do stref elektronicznie chronionych,
3) indywidualne hasła i loginy do systemów operacyjnych PC,
4) uprawnienia wynikające z zakresu obowiązków i imiennych upoważnień,
5) obowiązek otrzymania zgody na pracę w godzinach nadliczbowych lub w dni wolne,
6) obowiązek zapoznania się z Polityką oraz Instrukcją zarządzania systemem informatycznym,
7) obowiązek nadzoru nad pracownikami przez bezpośrednich przełożonych,
8) obowiązek udziału w szkoleniach z zakresu bezpieczeństwa przetwarzania danych.
9) dokumentacja urzędu w zakresie ochrony danych osobowych.

§11 SPOSÓB POSTĘPOWANIA W ZAKRESIE KOMUNIKACJI POZA SIECIĄ INFORMATYCZNĄ URZĘDU

1. Przy przesyłaniu danych osobowych poza siecią dedykowaną do transferu danych osobowych wymagane jest zastosowanie szczególnych wymagań w zakresie bezpieczeństwa. Obejmują one:
1) zatwierdzenia w formie pisemnej lub w formie elektronicznej przez AD celu wysłania danych osobowych,
2) zastosowanie mechanizmów szyfrowania danych osobowych,
2. W przypadku stosowania mechanizmów kryptograficznych AD określa wymagania w zakresie materiału kryptograficznego stosowanego do ochrony danych osobowych.
3. W wypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe, korzysta z innych mechanizmów kryptograficznych niż stosowane przez Administratora, możliwe jest zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych. W tym celu ASI lub osoba specjalnie do tego celu wyznaczona, może przeprowadzić analizę poziomu bezpieczeństwa mechanizmu kryptograficznego oraz zgodności tego mechanizmu z komponentami systemu informatycznego.
4. W przypadku wystąpienia podejrzenia przechwycenia kluczy kryptograficznych lub dostania się ich w niepowołane ręce, IOD zobowiązany jest poinformować o tym fakcie AD i zmienić parametry klucza szyfrującego.

§12 ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH, NA KTÓRYCH SĄ PRZETWARZANE DANE OSOBOWE POZA SIEDZIBĄ URZĘDU

1. Przetwarzanie danych osobowych na komputerach przenośnych poza siedzibą Urzędu Gminy w Kowali - Stępocinie, powinno być ograniczone do niezbędnego minimum i może

się odbywać wyłącznie na podstawie upoważnienia AD.

2. Każdy komputer przenośny musi być zabezpieczony indywidualnym hasłem i loginem.
3. Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących tajemnicę służbową, zwłaszcza mających charakter lokalnej bazy lub pliku czyli zlokalizowanych bezpośrednio na użytkowanym komputerze, zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. W związku z powyższym użytkownik komputera przenośnego zobowiązany jest do:

1) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 -mio znakowym zawierającym: duże i małe litery, znaki specjalne lub cyfry,
2) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:

a. transportowania komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu podręcznego;
b. nie pozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp.

3) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
4) zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym),
5) zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła,
6) wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,
7) zmianę haseł co 30 dni,
8) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,
9) regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego Urzędu Gminy w Kowali – Stępocinie w celu umożliwienia wykonania kopii awaryjnej,
10) cyklicznego podłączania komputera do sieci informatycznej Urzędu Gminy w Kowali - Stępocinie w celu wykonania aktualizacji wzorców wirusów w programie antywirusowym,

5. ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności:

1) dokonać konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł odpowiedniej jakości oraz ich cyklicznej zmiany, zgodnie z wytycznymi dotyczącymi polityki posługiwania się hasłami w systemie informatycznym Urzędu Gminy w Kowali - Stępocinie,
2) w przypadku przetwarzania danych osobowych znajdujących się bezpośrednio na komputerze przenośnym - zabezpieczyć je dodatkowo poprzez wykorzystanie oprogramowania szyfrującego
3) dokonać instalacji i konfiguracji oprogramowania antywirusowego,
4) przeprowadzić aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

6. ASI jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych poza siedzibą Urzędu Gminy w Kowali - Stępocinie. W szczególności ewidencja powinna obejmować:

1) typ i numer seryjny komputera przenośnego,
2) imię i nazwisko osoby będącej użytkownikiem komputera,
3) wykaz oprogramowania zainstalowanego na komputerze, służącego do przetwarzania danych osobowych
4) rodzaj i zakres danych osobowych przetwarzanych na komputerze.

7. W razie zgubienia lub kradzieży komputera przenośnego, pracownik zobowiązany jest do natychmiastowego powiadomienia IOD lub osoby uprawnionej zgodnie z zasadami informowania w przypadku naruszenia ochrony danych osobowych.
8. Kopie informacji przetwarzanych na komputerze przenośnym tworzone są indywidualnie przez ich użytkowników, na ich odpowiedzialność.

§ 13 ELEKTRONICZNE NOŚNIKI DANYCH

1. Administrator stosuje się nośniki danych oznaczone i zarejestrowane w Rejestrze nośników prowadzonym przez ASI, którego wzór stanowi załącznik nr 17 do niniejszej Polityki. Rejestr zawiera spis osób, którym przydzielono oznaczony nośnik.
2. Przy kontrasygnacie IOD, ASI wydaje Upoważnienie do wynoszenia nośników poza siedzibę Urzędu, którego wzór stanowi załącznik nr 18 do niniejszej Polityki.
3. ASI prowadzi Rejestr wydanych upoważnień do wynoszenia nośników poza siedzibę Urzędu Gminy w Kowali - Stępocinie, którego wzór stanowi załącznik nr 19 do niniejszej Polityki.
4. Nośniki pochodzące od jednostek zewnętrznych mogą być wykorzystane po uprzednim sprawdzeniu licencjonowanym programem antywirusowym w obecności IOD lub ASI.
5. Każdy użytkownik ma obowiązek usunięcia danych osobowych z nośników, które przeznaczone są do przekazania innemu podmiotów informacji związanych z realizacją zadań.
6. Deszyfracja i wprowadzenie do systemy informatycznego danych z nośników zewnętrznych dokonywana jest wyłącznie przez IOD.

§14 WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1	Klauzula informacyjna o danych osobowych przetwarzanych przez Administratora
Załącznik nr 2	Oświadczenie osoby przetwarzającej dane osobowe
Załącznik nr 3	Oświadczenie o przeszkoleniu
Załącznik nr 4	Rejestr szkoleń
Załącznik nr 5	Zgoda na przetwarzanie danych osobowych
Załącznik nr 6	Instrukcja zarządzania systemem informatycznym
Załącznik nr 7	Instrukcja postępowania w przypadku naruszenia danych osobowych
Załącznik nr 8	Wniosek o nadanie .zmianę, odwołanie upoważnienia do przetwarzania danych osobowych w systemach
Załącznik nr 9	Upoważnienie, odwołanie upoważnienia do przetwarzania danych osobowych
Załącznik nr 10	Ewidencja wydanych upoważnień do przetwarzania danych osobowych
Załącznik nr 11	Formularz do odnotowywania udostępniania danych osobowych

Załącznik nr 12	Instrukcja postępowania z kluczami oraz zabezpieczenia
Załącznik nr 13	Wykaz budynków, pomieszczeń lub części pomieszczeń
Załącznik nr 14	Wykaz zbiorów danych
Załącznik nr 15	Wykaz systemów informatycznych służących do przetwarzania danych osobowych
Załącznik nr 16	Opis struktur zbiorów danych oraz sposobu przepływu danych między systemami
Załącznik nr 17	Rejestr nośników
Załącznik nr 18	Upoważnienie do wynoszenia nośników
Załącznik nr 19	Rejestr wydanych upoważnień do wynoszenia nośników

Załącznik nr 1
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

KLAUZULA INFORMACYJNA O PRZETWARZANIU DANYCH OSOBOWYCH

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej również „RODO") Dz. Urz. UE L 119 z 04.05.2016, informujemy, że:

1. Administratorem Danych Osobowych w Gminie Kowala (siedziba: ul. Marii Walewskiej 7, 26-624 Kowala – Stępocina) jest:

a. Gmina Kowala – w sprawach dotyczących zakresu działań i zadań wynikających z ustawy z dnia 08.03.1990 r. o samorządzie gminnym (Dz. U. z 2024 r., poz. 609)

b. Urząd Gminy w Kowali – Stępocinie – jako jednostka organizacyjna gminy w sprawach dotyczących świadczenia pomocy Wójtowi w zakresie realizacji jego zadań określonych przepisami prawa.

2. Administrator Danych Osobowych wyznaczył Inspektora Danych Osobowych, z którym możesz się skontaktować w sprawach ochrony Twoich danych osobowych i realizacji Twoich praw poprzez (do wyboru): e -mail: iod@kowala.pl; telefonicznie: 48/610-17-60 wew. 21 lub pisemnie na adres siedziby Administratora Danych, wskazany powyżej.

3. Pani/Pana dane osobowe będą przetwarzane w celu/celach:

a. wypełnienia obowiązku prawnego, wynikającego z przepisów prawa, tj: realizacji wniosków, podań i żądań złożonych przez osobę, której dane dotyczą; realizacji umów zawartych z kontrahentami; w pozostałych przypadkach Pani/Pana dane osobowe przetwarzane są wyłącznie na podstawie wcześniej udzielonej zgody w zakresie i celu określonym w treści zgody;

b. wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;

c. wypełnienia obowiązków prawnych ciążących na Administratorze.

4. Podstawę prawną przetwarzania Państwa danych stanowią:

a. art. 6 ust. 1 lit. c i e rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej zwanym RODO;

b. ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

c. ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

5. Dane osobowe po zrealizowaniu celu, dla którego zostały zebrane, będą przetwarzane do celów archiwalnych i przechowywane przez okres niezbędny do zrealizowania przepisów dotyczących archiwizowania danych obowiązujących u Administratora.

6. W związku z przetwarzaniem Pani/Pana danych osobowych przysługują Pani/Panu następujące uprawnienia:

a. prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;

b. prawo do żądania sprostowania (poprawiania) danych osobowych;

c. prawo do żądania usunięcia danych osobowych (tzw. prawo do bycia zapomnianym);

d. prawo do żądania ograniczenia przetwarzania danych osobowych;

e. prawo do przenoszenia danych;

f. prawo sprzeciwu wobec przetwarzania danych.

7. W przypadku gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby na przetwarzanie danych osobowych (art. 6 ust. 1 lit a RODO), przysługuje Pani/Panu prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.

8. Podanie przez Panią/Pana swoich danych osobowych jest:

a. wymogiem ustawowym, w przypadku, kiedy cel, w jakim Pani/Pan je podaje, skutkuje koniecznością wypełnienia przez administratora obowiązku prawnego ciążącego na administratorze lub koniecznością wykonania przez administratora zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W takim przypadku jest Pani/Pan

zobowiązana/zobowiązany do ich podania, a ewentualne ich niepodanie będzie skutkowało brakiem możliwości realizacji Pani/Pana interesu prawnego;
b. wymogiem umownym, w przypadku, kiedy tak stanowią zapisy umowy. W takim przypadku jest Pani/Pan zobowiązana/zobowiązany do ich podania, a ewentualne ich niepodanie będzie skutkowało w szczególności problemami z prawidłowym wykonaniem umowy lub niewykonaniem umowy;
c. warunkiem zawarcia umowy, w przypadku, kiedy celem, w jakim Pani/Pan je podaje, jest zawarcie umowy. W takim przypadku jest Pani/Pan zobowiązana/zobowiązany do ich podania, a ewentualne ich niepodanie będzie skutkowało nie zawarciem umowy;
d. nieobligatoryjne, w przypadku, kiedy cel, w jakim administrator je od Pani/Pana pozyskał, nie skutkuje koniecznością wypełnienia przez administratora żadnego obowiązku prawnego lub nie skutkuje koniecznością wykonania przez administratora żadnego zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
9. Ma Pani/Pan prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych z siedzibą ul. Stawki 2, 00-193 Warszawa.
10. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą poddawane profilowaniu.
11. Odbiorcami danych osobowych są podmioty zajmujące się obsługą Administratora. W związku z przetwarzaniem danych odbiorcami Pani/Pana danych osobowych mogą być również:
a. organy władzy publicznej oraz podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa;
b. inne podmioty, które na podstawie stosownych umów podpisanych z Gminą Kowala przetwarzają dane osobowe.

…… ……
Imię i nazwisko osoby przetwarzającej dane osobowe, składającej oświadczenie — data

Oświadczenie

Oświadczam, że zapoznałem/łam się, rozumiem i będę przestrzegać obowiązków wynikających z przepisów Rozporządzenia Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.l - zwane RODO, krajowych aktów prawnych, aktów wykonawczych oraz dokumentów przyjętych przez Administratora Danych - w związku z przetwarzaniem danych osobowych, a w szczególności:

- Polityki bezpieczeństwa przetwarzania danych osobowych;
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Kowali - Stępocinie.

Zobowiązuję się do podejmowania działań zmierzających do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz unikaniem tych zachowań, które mogłyby poziom bezpieczeństwa danych osobowych obniżyć.

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskam dostęp w trakcie trwania i po zakończeniu (* niepotrzebne skreślić):

- zatrudnienia*
- stażu*
- praktyki*
- współpracy*(jakiej?) ……...
- umowy cywilno-prawnej* zawartej w dniu ……

Jednocześnie przyjmuje do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia ponoszę odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz przepisów prawnych dotyczących ochrony danych osobowych.

…….
Podpis osoby przetwarzającej dane osobowe,
składającej oświadczenie

……
Potwierdzam odbiór 1-egzemplarza (pieczątka i podpis ADO)

……..
(pieczątka i podpis IOD)

Załącznik nr 3
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

…… Kowala – Stępocina , dn. …….
Imię nazwisko

OŚWIADCZENIE

Oświadczam, że:

- **przed przystąpieniem do pracy / umowy cywilno – prawnej / stażu / praktyki / innej formy współpracy*** przy przetwarzaniu danych osobowych zostałam/em znajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z Rozporządzeniem Parlamentu i Rady (UE) 2016/676 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – ogólne rozporządzeni o ochronie danych –
(dla nowo zatrudnionych osób)
- **w trakcie trwania stosunku pracy / umowy cywilno – prawnej / staży / praktyki / innej formy współpracy*** przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z Rozporządzeniem Parlamentu i Rady (UE) 2016/676 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – ogólne rozporządzeni o ochronie danych –
(dla pracowników)

Zapoznałam/m się i rozumiem zasady dotyczące ochrony danych osobowych opisane w:

1) „Polityce bezpieczeństwa przetwarzania danych osobowych”
2) „Instrukcji zarzadzania systemem informatycznym w Urzędzie Gminy w Kowali - Stępocinie”
   A także w pozostałych dokumentach regulujących zasady przetwarzania danych osobowych przez Administratora Danych.

Zobowiązuję się do zachowania w tajemnicy danych osobowych, sposobu ich zabezpieczenia, przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami ustanowionymi przez Administratora Danych.

……..…….
Czytelny podpis

*niepotrzebne skreślić

Załącznik nr 4
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

REJESTR SZKOLEŃ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH			
LP.	**Imię i Nazwisko**	**Data szkolenia**	**Podpis**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			

Zgoda na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych, w tym danych szczególnych kategorii* przez Administratora danych, którym jest:

a. Gmina Kowala* - w sprawach dotyczących zakresu działań i zadań wynikających z ustawy z dnia 08.03.1990 r. o samorządzie gminnym
b. Urząd Gminy w Kowali - Stępocinie* - jako jednostka organizacyjna gminy w sprawach dotyczących świadczenia pomocy Wójtowi w zakresie realizacji jego zadań określonych przepisami prawa.

Siedziba Administratora Danych: ul. Marii Walewskiej 7, 26-624 Kowala - Stępocina,

w celu realizowania przez Administratora obowiązków ustawowych wynikających z poszczególnych aktów prawnych:

…….
…….
…….
…….
…….
…….
…….
…….
…….
.

□ TAK □ NIE

…….
(podpis)

Zostałem/łam poinformowany/a o zasadach przetwarzania danych zawartych w Klauzuli przetwarzania danych, która została mi udostępniona.

……..
(podpis)

* Dane szczególnych kategorii to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne wykorzystywane do identyfikacji, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, o których mowa w art 9 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).

Załącznik nr 6
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy w Kowali - Stępocinie

Zatwierdził:
Wójt Gminy Kowala

Dariusz Bulski

Kwiecień 2024 r.

System informatyczny, na którym pracują użytkownicy, jest zbiorem samodzielnych lub połączonych zależnościami podsystemów informatycznych, w których ma miejsce przetwarzanie danych osobowych.

§ 1 CELI ZAKRES OBOWIĄZYWANIA INSTRUKCJI

1. Celem niniejszej Instrukcji jest określenie zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład urządzenia, odpowiednio do skali zagrożeń i kategorii danych objętych ochroną. Stosowanie zasad określonych w niniejszej Instrukcji ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Urząd Gminy w Kowali - Stępocinie w systemach informatycznych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych osobowych oraz elementów zarządzania systemem informatycznym. W przypadku, gdy z oceny funkcjonowania instrukcji wynika, że zachodzi potrzeba wprowadzenia nowych lub modyfikacji istniejących zasad właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, wnioski w tej sprawie powinni składać użytkownicy systemu do Administratora Danych.

§ 2 DEFINICJE

Podstawowe pojęcia:

1. „RODO" - Rozporządzenia Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.l
2. „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. „dane szczególnych kategorii" oznaczają dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające:

a. pochodzenie rasowe lub etniczne
b. poglądy polityczne;
c. przekonania religijne lub filozoficzne;
d. stan zdrowia;
e. przynależność partyjna, związkowa lub wyznaniowa;
f. kod genetyczny;
g. nałogi;
h. życie seksualne;
i. skazania i orzeczenia dotyczące mandatów i kar;
j. dane genetyczne, dane biometryczne (w celu jednoznacznego zidentyfikowania osoby)

lub dotyczące zdrowia lub seksualności i orientacji seksualnej.

4. „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

a. zbieranie,
b. utrwalanie,
c. organizowanie,
d. porządkowanie,
e. przechowywanie,

f. adaptowanie lub modyfikowanie,
g. pobieranie,
h. przeglądanie,
i. wykorzystywanie,
j. ujawnianie poprzez przesłanie,
k. rozpowszechnianie lub innego rodzaju udostępnianie,
l. dopasowywanie lub łączenie,
m. ograniczanie, usuwanie lub niszczenie;

5. „ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
6. „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
7. „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
8. „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
9. „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Administratora danych osobowych, którym jest:

a. Gmina Kowala - w sprawach dotyczących zakresu działań i zadań wynikających z ustawy z dnia 08.03.1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609)
b. Urząd Gminy w Kowali – Stępocinie - jako jednostka organizacyjna gminy w sprawach dotyczących świadczenia pomocy Wójtowi w zakresie realizacji jego zadań określonych przepisami prawa.

10. „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
11. „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia;
12. „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
13. „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
14. „dane genetyczne" oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
15. „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
16. „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej

zdrowia;

17. „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
18. „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO, czyli Urząd Ochrony Danych;
19. „inspektor ochrony danych" (IOD) oznacza osobę powołaną przez AD zgodnie z art. 37 RODO do nadzorowania przestrzegania zasad i wymagań w zakresie ochrony danych, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych. Wyznaczenie IOD następuje na podstawie Zarządzenia Wójta Gminy Kowala.
20. „administrator systemów informatycznych" (ASI) oznacza osobę z zakresu informatyki odpowiedzialną za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w systemach informatycznych, wyznaczoną przez AD.
21. „bezpieczeństwo przetwarzania danych osobowych" oznacza zachowanie poufności, integralności i rozliczalności danych osobowych. Dodatkowo mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
22. „system informatyczny" oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
23. „system tradycyjny" oznacza zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze
24. „bezpieczeństwo systemu informatycznego" oznacza wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych oraz ochrona przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub nieuprawnionym pozyskaniem danych osobowych, a także ich utratą (zamierzoną lub przypadkową).
25. „incydent" oznacza pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
26. „integralność danych" oznacza właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
27. „integralność systemu" oznacza nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
28. „identyfikator użytkownika" (LOGIN) oznacza ciąg znaków literowych i cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
29. „hasło" oznacza ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
30. „użytkownik systemu" oznacza osobę posiadającą upoważnienie nadane przez AD i uprawniona do bezpośredniego dostępu do przetwarzania danych osobowych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
31. „nośnik" oznacza narzędzie do zapisywania, przenoszenia i odczytywania danych i informacji na nim zapisanych. Nośnikiem może być urządzenie elektroniczne, optyczne, karty SIM, magnetyczne lub papierowy.
32. „właściciel zbioru danych osobowych" oznacza osobę kierującą komórką organizacyjną, stanowisko samodzielne, odpowiedzialna za ochronę danych osobowych. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
33. „sieć lokalna" oznacza połączenie funkcjonujących w Urzędzie Gminy w Kowali – Stępocinie systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci

telekomunikacyjnych.

34. „stacja robocza" oznacza stacjonarny lub przenośny komputer, rozpoznawany przez system IT, wchodzący w skład systemu informatycznego, umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie.
35. „sieć telekomunikacyjna" oznacza sieć telekomunikacyjna w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne [Dz. U. z 2004r. Nr 171, poz. 1800, z późniejszymi zmianami).
36. „zalogowanie" oznacza uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3 ODPOWIEDZIALNOŚĆ

Obowiązki AD, 10D i ASI zostały szczegółowo omówione w Polityce Bezpieczeństwa Przetwarzania Danych.

Wszyscy użytkownicy są odpowiedzialni za prawidłowe wykorzystanie systemów informatycznych wykorzystywanych w Urzędzie Gminy w Kowali - Stępocinie.

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej.

Do obowiązków należy również:

1. współpraca przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu;
2. przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji;
3. informowanie IOD o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
4. wykonywania bez zbędnej zwłoki poleceń IOD w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§ 4 OPIS ROZWIĄZAŃ TECHNICZNYCH ZASTOSOWANYCH W CELU ZAPEWNIENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

1. Metody i środki uwierzytelniania w systemie informatycznym

1) Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom systemu rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

a. użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;
b. użytkownik systemu ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
c. hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;
d. użytkownik systemu nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

2) Administrator systemu jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników systemu oraz kont w systemach.
3) Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym sposobem uwierzytelniania.
4) Identyfikator użytkownika systemu powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
5) Po przekroczeniu maksymalnej ilości prób uwierzytelniania w systemie, konto powinno zostać zablokowane z możliwością odblokowania wyłącznie przez Administratora systemu.

2. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 rozporządzenia.

§ 5 OPIS PROCEDUR I ZASAD WPROWADZONYCH W CELU ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACJI, W TYM PRZETWARZANIA DANYCH OSOBOWYCH

1. Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami, a także uzyskaniem formalnego upoważnienia do przetwarzania danych osobowych - zgodnie z opisem w rozdziale VI Polityki bezpieczeństwa Przetwarzania Danych.
2. Po spełnieniu wymagań określonych powyżej, rejestrowanie użytkowników systemu i nadawanie uprawnień w systemach informatycznych, realizowane jest przez Administratora Systemu Informacji (ASI) - na podstawie polecenia AD.
3. Szczególnie wnikliwej weryfikacji powinny podlegać wnioski dotyczące tworzenia oraz dostępu do kont uprzywilejowanych, związanych z realizacją przywilejów systemowych (administracyjnych) w systemie informatycznym, dających nieograniczone lub duże - z punktu widzenia istniejących zagrożeń - uprawnienia dostępu w stosunku do tego systemu lub przetwarzanych w nim danych osobowych.
4. Hasła do kont użytkowników uprzywilejowanych powinny zostać przekazane z zamkniętej kopercie do AD, który deponuje dostarczone hasła w bezpiecznym miejscu. Wymagane jest przy każdorazowej zmianie hasła przez użytkownika uprzywilejowanego stosowane powyższej procedury.
5. Przy tworzeniu nowego konta użytkownika w systemie, ASI nadaje mu unikalny identyfikator konta, który nie może być powtórzony dla żadnego innego użytkownika systemu przez cały okres życia tego systemu.
6. ASI powinien przekazywać użytkownikom systemu tymczasowe hasła dostępowe w sposób bezpieczny. W tym celu powinni unikać pośrednictwa osób trzecich lub korzystania do tego celu z niechronionych wiadomości poczty elektronicznej.
7. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach informatycznych lub w przypadku odebrania uprawnień w systemach.
8. Zmiany dotyczące użytkownika systemu, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu informatycznego oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. W przypadku wycofania użytkownikowi systemu uprawnień do przetwarzania danych osobowych lub dostępu do systemu informatycznego przetwarzającego te dane, konto użytkownika nie podlega skasowaniu z systemu, ale skutecznemu zablokowaniu przez ASI.
10. Prawa dostępu przyznane użytkownikom systemu, którzy nie są pracownikami etatowymi Urzędu Gminy w Kowali – Stępocinie powinny mieć charakter czasowy i mogą być przyznawane wyłącznie na okres odpowiadający wykonywanemu zadaniu oraz powinny być formalnie zatwierdzane.
11. Obowiązki użytkowników systemu:

11.1 Do podstawowych obowiązków użytkowników systemu należy przetwarzanie danych osobowych wyłącznie w celu i zakresie wynikającym z obowiązków służbowych.

11.2 Użytkownicy systemu zobowiązani są do podejmowania współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.

11.3 Użytkownicy systemu zobowiązani są do:

a. przestrzegania opracowanych dla systemu zasad przetwarzania danych osobowych oraz procedur i instrukcji;
b. uniemożliwienia dostępu lub podglądu danych osobom nieupoważnionym;
c. informowania Administratora danych lub Inspektora Ochrony Danych o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;

11.4 Wykonywania bez zbędnej zwłoki poleceń Administratora danych w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.
12. Zarządzanie przywilejami:
12.1 Konta użytkownika uprzywilejowanego należy oznaczyć, zapewnić ich łatwą identyfikację oraz zapewnić, że odwołują się do jednego użytkowania.
12.2 Wyłącznie czynności, które wymagają użycia uprawnień uprzywilejowanych należy wykonywać z konta posiadającego uprawnienia uprzywilejowane.
12.3 Konta uprzywilejowane i ich uprawnienia należy okresowo przeglądać.
12.4 Czynności wykonywane za pomocą kont uprzywilejowanych należy rejestrować oraz zapewnić możliwości ich identyfikacji i rozliczalności.
13. Zarządzanie hasłami:
13.1 Przydzielanie haseł powinno być kontrolowane za pośrednictwem formalnego procesu zarządzania.
13.2 Hasła powinny być dobrej jakości:
a. długości co najmniej 8 znaków;
b. które są łatwe do zapamiętania, a trudne do odgadnięcia;
c. nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.);
d. w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra i znak specjalny;
14. Rodzaje kont:
14.1 Konto administratora;
14.2 Konto użytkownika;
15. Zakres uprawnień konta administratora:
15.1 prawa konta standardowego
15.2 tworzenie, zmiana i usuwanie kont użytkowników
15.3 zmiany w konfiguracji komputera
15.4 dostęp do wszystkich plików na komputerze
15.5 instalacja sprzętu i oprogramowania
16. Zakres uprawnień konta użytkownika:
16.1 możliwość zmiany podstawowych ustawień komputera takich jak zmiana ustawień wyświetlania oraz zarządzania energią
16.2 odbiór poczty mailowej
16.3 korzystanie z danego programu
17. Hasła w systemach informatycznych:
13.1 Użytkownicy systemu powinni wybierać hasła dobrej jakości:
a. długości co najmniej 8 znaków;
b. które są łatwe do zapamiętania, a trudne do odgadnięcia;
c. nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.);
d. w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny;
e. w których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6", „zaqlxsw2CDE#" itp.).
13.2 Hasło początkowe, które jest przydzielane przez administratora systemu, powinno umożliwiać użytkownikowi systemu zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika systemu.
13.3 Użytkownik systemu jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
a. okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła);
b. w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
13.4 Zmiana haseł użytkowników systemu powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik systemu jest zobowiązany samodzielnie zmienić hasło co 30 dni.
13.5 Wszelkie urządzenia sprzętowe lub programowe, które na początku posiadały hasło domyślne, powinny mieć zmienione hasło zgodnie z przyjętymi wymogami dotyczącymi formułowania haseł.

13.6 Należy unikać ponownego lub cyklicznego używania haseł, które już kiedyś były wykorzystywane.
13.7 Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
13.8 Hasła nie powinny być przechowywane oraz przesyłane w systemach w postaci jawnej.
13.9 Uprzywilejowane konto posiada IOD i ASI.
13.10 Na czas swojej nieobecności, IOD wyznacza osobę w zastępstwie.

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy, którym przyznano dostęp do podsystemu przetwarzania danych osobowych (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z IOD.
2. Hasło przydzielane jest ustnie i jest informacją o poufnym charakterze - należy zachować je w tajemnicy.
3. Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.
4. Hasła do wszystkich użytkowanych podsystemów należy przechowywać w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
5. Osobą mającą dostęp do listy identyfikatorów i haseł użytkowników oraz odpowiedzialną za bezpieczne przechowywanie listy identyfikatorów wraz z hasłami jest ASI.
6. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie ASI, który ustali nowe hasło.
7. Hasło składa się z ciągu co najmniej 6 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
8. Hasła są różne dla każdego z użytkowników.
9. Hasła są przechowywane w podsystemie w postaci zaszyfrowanej.
10. Para „identyfikator i hasło" przyznane jednemu użytkownikowi nie może zostać powtórnie wykorzystane.
11. Hasła są zmieniane nie rzadziej niż co 30 dni.
12. System wymusza zmianę hasła.
13. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej.
14. Jeżeli system informatyczny środkami technicznymi nie wymusza podjęcia czynności określonych w niniejszej Procedurze, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i ustanowieniu nowego, spełniającego wymogi określone w niniejszej procedurze.
15. Osobą odpowiedzialną za ustalanie poprawności haseł jest ASI. Jeśli użytkownik podsystemu odpowiedzialny za zmianę hasła nie jest pewien jego poprawności, zobowiązany jest do konsultacji z osobą odpowiedzialną za ustalanie poprawności bezpiecznych haseł.

3. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Celem określenia procedury rozpoczęcia, zawieszenia i zakończenia pracy z systemem jest zabezpieczenie go przed przechwyceniem poufnych haseł oraz odczytaniem danych przez osoby niepożądane.
2. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik systemu zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
3. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie IOD.
4. Kończąc pracę, użytkownik systemu obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz elektronicznych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich w zamykanych szafkach.
5. Stacje robocze powinny być tak skonfigurowane, aby w przypadku nieobecności użytkownika systemu dłużej niż 5 minut uruchamiał się wygaszasz ekranu odblokowywany hasłem.

Alternatywnie może obowiązywać wymaganie wylogowania się z systemu lub blokowania stacji roboczej w przypadku chwilowego opuszczenia stanowiska pracy.

6. Monitory komputerowe powinny być umieszczone tak aby osoby nieupoważnione nie mogły mieć wglądu w dane wyświetlane na monitorze.

4. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania .

1. Kopie zapasowe całościowe tworzone są raz w miesiącu.
2. Kopie zapasowe przyrostowe tworzone są codziennie po zakończonym dniu pracy ze zbiorem, chyba że danego dnia nie dokonano żadnych zmian w zbiorze.
3. Kopie całościowe przechowywane są przez okres 5 lat, a kopie przyrostowe przez 1 miesiąc.
4. Kopie przechowywane są w sejfie, do których dostęp ma ASI i informatyk.
5. Za tworzenie kopii zapasowych odpowiedzialny jest Opiekun Zbioru, którym jest osoba sprawująca funkcję kierowniczą danego referatu lub osoba na samodzielnym stanowisku.
6. Opiekun Zbioru dokonuje zapisu kopii zbiorów danych osobowych na nośnikach CD, DVD, Pendrive lub innych nośnikach informacji przynajmniej co 14 dni lub częściej jeśli zmian na zbiorze jest dostatecznie wiele lub gdy uważa to za stosowne.
7. Opiekun Zbioru oznacza i przechowuje kopie zbiorów danych w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
8. Poprawność procesu tworzenia i przechowywania kopii zapasowych - nadzoruje ASI.
9. Kopie zapasowe zawierające dane osobowe, dla których cel przetwarzania ustał, powinny być pozbawiane zapisu tych danych, a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie i/lub odzyskanie danych osobowych.
10. Tworzenie kopii bezpieczeństwa programów bazodanowych:

10.1 sQola Integra Płace; gDeklaracje:

10.1.1 Bieżąca kopia zapasowa bazy jest tworzona automatycznie przez sam program 5 razy w tygodniu w dni robocze od poniedziałku do piątku i składowana w oddzielnym folderze (ArchiwumQNT) na serwerze instalacyjnym programu.

10.1.2 Powyższa kopia zapasowa jest automatycznie replikowana raz w tygodniu na serwera backupu.

10.1.3 Istnieją 52 kopie rotacyjne umożliwiające przywrócenie bazy danych.

10.1.4 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.

10.1.5 Kopie są kopiami pełnymi.

10.1.6 Serwer backupu oraz NAS korzystają z macierzy RAID1.

10.1.7 Dodatkowa kopia bazy danych oraz instalacji programu robiona jest dwa razy w tygodniu - kopia jest pełna w liczbie 10 wersji.

10.1.8 Składowanie oraz sposób kopiowania i replikacji dodatkowej kopii jak w podpunkcie b, d i e.

10.1.9 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.

10.1.10 Dostęp do kopii mają: Dyrektor, Główny informatyk.

10.1.11 Dwa razy w miesiącu tygodniowa kopia zapasowa nagrywana jest na dysk zewnętrzny
1 składowana w szafie pancernej.

10.1.12 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.

10.1.13 Dysk zewnętrzny z kopią zapasową jest przechowywana przez 2 lata.

10.1.14 Dodatkowe kopie są replikowane i przechowywane są w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.

10.1.15 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

10.1.16 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.

10.2TALES:

10.2.1 Bieżąca kopia zapasowa jest wykonywana raz w miesiącu automatycznie przez program backupujący.

10.2.2 W czasie kiedy wprowadzane są duże ilości danych kopia zapasowa wykonywana jest co 2 dni.

10.2.3 Istnieje 30 kopii rotacyjnych umożliwiające przywrócenie bazy danych.

10.2.4 Kopia zapasowa składowana jest na serwerze backupu.

10.2.5 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.2.6 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.2.7 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.2.8 Raz w miesiącu kopia zapasowa nagrywana jest na pendrive i składowana w szafie pancernej. W okresie wprowadzania większej ilości danych kopia jest nagrywana na pendriva raz w tygodniu.
10.2.9 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.2.10 Pendrive z kopią zapasową jest przechowywana przez 2 lata.
10.2.11 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.2.12 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.2.13 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
10.3Xpertis Podatek od środków Transportowych: Xpertis Podatek rolny, leśny i od nieruchomości: Xpertis Finanse i Księgowość:
10.3.1 Bieżąca kopia zapasowa jest tworzona automatycznie przez program backupu dwa razy w tygodniu i składowana na serwerze backupu.
10.3.2 Istnieją 52 kopie rotacyjne umożliwiające przywrócenie bazy danych.
10.3.3 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.3.4 Kopie są kopiami pełnymi.
10.3.5 Serwer backupu oraz NAS korzystają z macierzy RAID1.
10.3.6 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.3.7 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.3.8 Razy w miesiącu kopia zapasowa nagrywana jest na płytę pendrive i składowana w szafie pancernej.
10.3.9 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.3.10 Dysk zewnętrzny z kopią zapasową jest przechowywana przez 2 lata.
10.3.11 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.3.12 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.3.13 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
10.4PrzelewCom; e-pity:
10.4.1 Bieżąca kopia zapasowa jest tworzona automatycznie przez program backupu co 14 dni i składowana na serwerze backupu.
10.4.2 Istnieją 52 kopie rotacyjne umożliwiające przywrócenie bazy danych.
10.4.3 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.4.4 Kopie są kopiami pełnymi.
10.4.5 Serwer backupu oraz NAS korzystają z macierzy RAID1.
10.4.6 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.4.7 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.4.8 Razy w miesiącu kopia zapasowa nagrywana jest na dysk zewnętrzny i składowana w szafie pancernej.
10.4.9 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.4.10 Dysk zewnętrzny z kopią zapasową jest przechowywany przez 2 lata.
10.4.11 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.4.12 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.4.13 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
10.5WODA: EGB5:
10.5.1 Bieżąca kopia zapasowa jest tworzona automatycznie przez program backupu dwa razy w tygodniu i składowana na serwerze backupu.

10.5.2 Istnieją 52 kopie rotacyjne umożliwiające przywrócenie bazy danych.
10.5.3 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.5.4 Kopie są kopiami pełnymi.
10.5.5 Serwer backupu oraz NAS korzystają z macierzy RAID1.
10.5.6 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.5.7 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.5.8 Razy w miesiącu kopia zapasowa nagrywana jest na pendriva i składowana w szafie pancernej.
10.5.9 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.5.10 Pendrive z kopią zapasową jest przechowywana przez 2 lata.
10.5.11 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.5.12 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.5.13 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
10.6GENESIS - Gospodarka Odpadami:
10.6.1 Bieżąca kopia zapasowa jest tworzona automatycznie przez program backupu codziennie i składowana na serwerze backupu.
10.6.2 Istnieją 52 kopie rotacyjne umożliwiające przywrócenie bazy danych.
10.6.3 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.6.4 Kopie są kopiami pełnymi.
10.6.5 Serwer backupu oraz NAS korzystają z macierzy RAID1.
10.6.6 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.6.7 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.6.8 Razy w miesiącu kopia zapasowa nagrywana jest na płytę pendriva i składowana w szafie pancernej.
10.6.9 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.6.10 Płyta pendrive z kopią zapasową jest przechowywana przez 2 lata.
10.6.11 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.6.12 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.6.13 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
10.7 System Informacji Oświatowej - SIO:
10.7.1 Bieżąca kopia zapasowa jest wykonywana raz w miesiącu automatycznie przez program backupujący.
10.7.2 Istnieje 30 kopii rotacyjnych umożliwiające przywrócenie bazy danych.
10.7.3 Kopia zapasowa składowana jest na serwerze backupu.
10.7.4 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.7.5 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.7.6 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.7.7 Raz w miesiącu kopia zapasowa nagrywana jest na pendrive i składowana w szafie pancernej. W okresie wprowadzania większej ilości danych kopia jest nagrywana na pendrive raz w tygodniu.
10.7.8 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.7.9 Pendrive z kopią zapasową jest przechowywana przez 2 lata.
10.7.10 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.7.11 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.7.12 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
10.8 System Płatnik
10.8.1 Bieżąca kopia zapasowa jest wykonywana raz w miesiącu automatycznie przez program backupujący.

10.8.2 Istnieje 30 kopii rotacyjnych umożliwiające przywrócenie bazy danych.
10.8.3 Kopia zapasowa składowana jest na serwerze backupu.
10.8.4 Kopie rotacyjne są replikowane automatycznie raz w tygodniu przez program backupu na zapasowy serwer NAS znajdujący się w lokalnej sieci.
10.8.5 W szczególnych wypadkach kopie zapasowe mogą być wykonywane manualnie.
10.8.6 Dostęp do kopii mają: Dyrektor, Główny informatyk.
10.8.7 Raz w miesiącu kopia zapasowa nagrywana jest na pendrive i składowana w szafie pancernej. W okresie wprowadzania większej ilości danych kopia jest nagrywana na pendrive raz w tygodniu.
10.8.8 Kopie zapasowe składowane na serwerze backupu oraz NAS są przechowywane przez rok. Starsze są usuwane automatycznie przez program i nadpisywane nowszą wersją.
10.8.9 Pendrive z kopią zapasową jest przechowywana przez 2 lata.
10.8.10 Serwer NAS zainstalowany jest w innym pomieszczeniu niż serwerownia, tzn. w ogniotrwałym sejfie w pomieszczeniu informatyka.
10.8.11 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
10.8.12 Niszczenie kopii bezpieczeństwa odbywa się poprzez jej zniszczenie w specjalnej niszczarce.
11. Tworzenie kopii bezpieczeństwa dokumentacji serwera:
11.1 Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu
0 wykorzystanie programowej funkcji serwera.
11.2 Kopie całościowe sporządzane są raz w miesiącu a kopie przyrostowe raz dziennie
11.3 Kopie całościowe przechowywane są przez okres 5 lat a kopie przyrostowe przez 1 miesiąc.
11.4 Kopie przechowywane są w sejfie.
11.5 Dostęp do kopii posiada informatyk.
11.6 ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
11.7 Niszczenie streamera odbywa się poprzez jego rozmontowanie i zniszczenie taśmy poprzez jej pocięcie.
11.8 Administrator systemu odpowiedzialny za tworzenie kopii zapasowych zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu.
11.9 Kopie zapasowe zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych, a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i kopii zapasowych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
a. na serwerach
b. na stacjach roboczych
c. na wymiennych nośnikach elektronicznych.
2. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.
3. Okres przechowywania nośników elektronicznych zawierających dane osobowe powinien być ustalony przez osobę kierującą komórką organizacyjną, w której te dane są przetwarzane, jednak nie powinien być krótszy niż 5 lat.
4. Na każdym nośniku powinna być odnotowywana data maksymalnego okresu przechowywania np. data ustania celu przetwarzania danych osobowych.
5. Nośniki elektroniczne zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.

6. Sposób zabezpieczenia systemu informatycznego

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik systemu nie był

w stanie wyłączyć lub pominąć etapu skanowania.

3. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują wyznaczone osoby niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
5. Wyznaczone osoby mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.
6. Każdy użytkownik systemu powinien być poinformowany o procedurze postępowania w przypadku wykrycia wirusa lub szkodliwego oprogramowania.
7. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej:

7.1 Zastosowano UPS do serwera oraz do elementów sieci typu router

7.2 Dostęp do komputera przenośnego wynoszonego poza obszar organizacji, zawierającego dane osobowe odbywa się poprzez podanie loginu i hasła

7.3 Użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa.

7.4 Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach

7.5 W przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie tego połączenia (SSL lub VPN)

7.6 W przypadku dostępu do danych osobowych przez Internet do środków teletransmisji, wymagane jest uwierzytelnienie (podanie loginu i hasła)

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

7.8 Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym (np. klientom, pracownikom innych działów,) dostęp do nich

7.9 Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej - komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

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

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

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

8. Zabezpieczenia programów i baz przetwarzających dane osobowe:

8.1 Dostęp do danych osobowych w programie lub w bazie wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła

8.2 Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania

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

8.4 Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych

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

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

8.7 Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe

8.8 Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po 10 minutach).

8.9 Na każdym stanowisku komputerowym zainstalowano oprogramowanie antywirusowe

8.10 Blokada nośników pamięci zewnętrznej

8.11 Każdy pracownik posiada pendrive z funkcją szyfrowania danych, dopisanego do tylko jednego komputera

8.12 Urządzenie do filtrowania sieci

9. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika systemu operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
10. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.
11. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.
12. W przypadku zgłoszenia sprzeciwu, o którym mowa w art. 32 ust 1 pkt 8 Ustawy o ochronie danych osobowych, wobec przetwarzania danych osobowych system powinien zapewniać odnotowywanie tej informacji.
13. Powinno się zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i udostępnienie:

a. zestawień zakresu i treści przetwarzanych na jej temat danych osobowych;
b. zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.

14. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnej aplikacji przeznaczonej do tego celu.
15. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.
16. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne.

Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiada ASI.
2. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności ASI lub innej wyznaczonej osoby.
3. W przypadku, gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia, o której mowa w art. 31 ustawy o ochronie danych osobowych.
4. Osoby nie będące pracownikami, które prowadzą prace serwisowe na rzecz AD przed rozpoczęciem prac, powinny być poddane weryfikacji tożsamości przez ASI lub inną wyznaczoną do tego celu osobę.
5. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
6. Przed przystąpieniem do naprawy nośników danych przez osoby nieupoważnione (np. serwisanci), powinno się usuwać dane osobowe. Naprawa nośników danych, z których nie da się usunąć danych osobowych, powinna odbywać się pod nadzorem ASI lub innego uprawnionego pracownika.

9. Zasady łączenia się z siecią Internet

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.
3. Administrator systemu powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:

a. kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
b. kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

4. Kontrola opisana powyżej powinna być dokumentowana przez osoby wykonujące te czynności.
5. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe w tym dane wrażliwe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:

a. ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi;
b. stosowanie metod kryptograficznych;
c. stosowanie odpowiednich zabezpieczeń fizycznych;
d. stosowanie odpowiednich zabezpieczeń organizacyjnych.

W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

6. Dane osobowe przetwarzane na komputerach przenośnych powinny być zabezpieczone w sposób zapewniający poufność tych danych, w szczególności dane te powinny być zabezpieczone metodami kryptograficznymi.
7. W zależności od „ważności" przewarzanych danych, procedura ta bywa restrykcyjna lub liberalna dla użytkowników. Prezentowana tu stanowi przykład procedury wyważonej.
8. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
9. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora systemu informatycznego i tylko w uzasadnionych przypadkach.
10. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
11. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
12. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
13. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:"
14. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
15. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny)
16. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
17. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
18. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę

o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

19. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
20. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
21. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
22. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
23. Użytkownicy powinni okresowo kasować niepotrzebne maile.
24. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości - UD W"
25. Urządzenie do zarządzania siecią Mikrotic, zarządzanie siecią, tworzenie grup, przypisywanie prędkości łącza, ograniczenia dostępowe do Internetu.

10. Załączniki

Załącznik nr 1 - Dziennik systemu informatycznego

Załącznik nr 2 - Ewidencja komputerów przenośnych

Dziennik systemu informatycznego [1]

Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania, ewentualnie wnioski	Podpis Administratora Systemu Informatycznego

[1] W tym dokumencie zapisujemy wszystkie operacje serwisowe, ważne aktualizacje itp., jakie wykonaliśmy na systemie informatycznym. Osobą zobowiązaną do prowadzenia dziennika systemu informatycznego jest Administrator Systemów Informatycznych.
W dzienniku systemu informatycznego wpisujemy działania tylko na tych sprzętach, które służą do przetwarzania danych osobowych. Nie ma potrzeby odnotowywać w nim na przykład naprawy kserokopiarki, ponieważ urządzenie to nie jest związane z przetwarzaniem danych. Jednak zmiana systemu operacyjnego w komputerze, na którym znajdują się bazy danych osobowych, już będzie taką czynnością, którą należy odnotować w dzienniku systemu informatycznego.
Dokument ten powinien być przechowywany w formie papierowej. Można również przechowywać plik do edycji w postaci cyfrowej.

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym
w Urzędzie Gminy w Kowali - Stępocinie

Ewidencja komputerów przenośnych

Typ i numer seryjny komputera	Imię i nazwisko użytkownika	Oprogramowanie służące do przetwarzania danych osobowych	Rodzaj i zakres danych osobowych

Załącznik nr 7
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

Instrukcja postępowania w przypadku naruszenia danych osobowych w Urzędzie Gminy w Kowali - Stępocinie

Zatwierdził:
Wójt Gminy Kowala

Dariusz Bulski

Kwiecień 2024 r.

1. **O naruszeniu ochrony danych osobowych mogą świadczyć symptomy występujące w następujących obszarach:**

1) w obrębie pomieszczeń, szaf lub miejsc przechowywania:

a) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych, w szczególności do serwerowni oraz kasy, gdzie przechowuje są nośniki kopii zapasowych,

b) włamanie lub próby włamania do szaf, w których przechowywane są w postaci elektronicznej lub papierowej, nośniki danych osobowych.

2) w obrębie sprzętu informatycznego:

a) kradzież komputera, w którym przechowywane są dane osobowe,

b) rozkręcona obudowa komputera.

3) w obrębie systemu informatycznego i aplikacji:

a) brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych,

b) brak możliwości zalogowania się do tej aplikacji,

c) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w strukturze aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych),

d) poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych (na przykład wgląd do szerszego zakresu danych o pracownikach),

e) inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),

inne:

f) zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, pendrive'a itp.),

g) zagubienie bądź kradzież nośnika z zawartością danych osobowych.

2. **Każda osoba, która zauważyła niepokojące zdarzenie, wystąpienie powyżej wymienionych symptomów lub innych objawów, które jej zdaniem mogą spowodować zagrożenie bądź mogą być przyczyną naruszenia ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania: bezpośredniego przełożonego, ASI, IOD lub AD.**

3. Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż AD, IOD, ASI czy bezpośredni przełożony, jest ona zobowiązana poinformować o tym fakcie AD, IOD, ASI lub przełożonego.

4. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w urzędzie naruszenia bezpieczeństwa danych osobowych, IOD we współpracy z ASI, jest zobowiązany do podjęcia następujących kroków:

1) stwierdzenia czy rzeczywiście doszło do naruszenia ochrony danych osobowych, w tym:

a) sprawdzenia okoliczności zdarzenia,

b) wyjaśnienia jego przyczyn, w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,

2) w przypadku, gdy doszło do naruszenia ochrony danych osobowych to:

a) zebranie ewentualnych dowodów,

b) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,

c) zabezpieczenia danych przetwarzanych w systemie informatycznym, jego logów systemowych, logów programu i bazy w których nastąpiło naruszenie bezpieczeństwa oraz danych konfiguracyjnych całego systemu w celu późniejszej analizy

d) usunięcia skutków incydentu i przywrócenia pierwotnego stanu systemu informatycznego tj. stanu sprzed incydentu, polegające na:

- przeprowadzeniu analizy spójności danych osobowych przetwarzanych w systemie,
- ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,
- przeprowadzeniu analizy poprawności funkcjonowania systemu informatycznego,
- powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

5. System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

6. IOD określa, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym urzędu.
7. **IOD prowadzi ewidencję interwencji związanej z zaistniałymi incydentami** w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

1) imię i nazwisko osoby zgłaszającej incydent,
2) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
3) datę zgłoszenia incydentu,
4) przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
5) wyniki przeprowadzonych działań,
6) podjęte akcje naprawcze i ich skuteczność.

8. IOD odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
2) określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
3) określenia potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

9. Zakres obowiązywania instrukcji:

Niniejsza instrukcja obowiązuje na terenie Urzędu Gminy w Kowali - Stępocinie, który obejmuje pomieszczenia biurowe Urzędu w budynku zlokalizowanym przy ul. Marii Walewskiej 7, 26-624 Kowala - Stępocina. Do stosowania postanowień zawartych w niniejszej instrukcji zobowiązani są wszyscy pracownicy Urzędu Gminy w Kowali – Stępocinie obsługujący zarówno Urząd Gminy jak i Gminę.

10. Instrukcja określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym dokumentach papierowych;
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenia zasad ochrony danych.

11. Celem instrukcji jest ustalenie jednolitych zasad postępowania w przypadku, gdy:

1) stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym nośnikach papierowych;
2) stan urządzenia, zawartość zbioru danych osobowych; ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych.

12. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

1) nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych;
2) udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom;
3) nieautoryzowany dostęp do danych przez połączenie sieciowe;
4) dostęp do pomieszczeń, w których przetwarza się dane osobowe dla osób nieuprawnionych;
5) niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe;
6) wykrycie niezabezpieczonego kanału dystrybucji danych osobowych;
7) nielegalne bądź nieświadome ujawnienie danych osobowych;
8) pozyskiwanie danych osobowych z nielegalnych źródeł;
9) przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem;
10) stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego;

11) ujawnienie indywidualnych haseł dostępu do systemu;
12) przesyłanie danych osobowych przez Internet bez zabezpieczenia;
13) przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia;
14) wykonanie nieuprawnionych kopii danych osobowych;
15) naruszenie bezpieczeństwa kopii danych osobowych;
16) kradzież nośników zawierających dane osobowe lub oprogramowanie;
17) kradzież sprzętu służącego do przetwarzania danych osobowych;
18) utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach;
19) brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii;
20) niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt;
21) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe;
22) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;
23) nie przeszkolenie pracowników w zakresie bezpieczeństwa danych osobowych;
24) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych.

13. Naruszenie ochrony danych osobowych może być skutkiem:

1) szkodliwego wpływu środowiska na system przetwarzania danych osobowych;
2) zewnętrznych zdarzeń losowych;
3) zamierzonych lub niezamierzonych czynności użytkowników systemów przetwarzania danych osobowych;
4) nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych.

14. O możliwości zaistnienia przypadku naruszenia zasad ochrony danych osobowych mogą świadczyć m. in.:

1) nadmierne, w stosunku do wykonywanych zadań (zakres upoważnienia), uprawnienia użytkownika do zasobów systemu;
2) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
3) wysoka aktywność kont, które długo pozostawały niewykorzystane;
4) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których przetwarza się dane osobowe (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.);
5) obecność osób nieupoważnionych w pomieszczeniu, w którym przetwarzane są dane osobowe.

15. **Każdy pracownik Urzędu Gminy w Kowali - Stępocinie, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany (bezpośrednio lub telefonicznie):**

1) podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony;
2) należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD;
3) powiadomić o zaistniałym zdarzeniu IOD oraz swojego bezpośredniego przełożonego;
4) określić (opisać) symptomy świadczące o możliwości naruszenia lub naruszeniu zasad ochrony danych;
5) określić sytuację i czas w jakim je zauważono;
6) podać wszelkie istotne informacje mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych;
7) nie podejmować dalszej pracy bez decyzji IOD.

16. IOD wraz z AD ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

1) dokonuje rozpoznania zdarzenia, zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Urzędu Gminy w Kowali,
2) może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,

3) ocenia wagę problemu;
4) ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu;
5) lokalizuje źródło problemu (przeprowadza analizę posiadanych danych).
6) nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba);
7) IOD 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).

17. W przypadku stwierdzenia, że podejrzenie nie świadczy o naruszeniu zasad ochrony danych, IOD po przeanalizowaniu sytuacji i wyeliminowaniu możliwości wystąpienia ich w przyszłości, podejmuje decyzję o dalszej pracy.
18. IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego załącznik nr 1.
19. Każda informacja o naruszeniu ochrony danych i jego okolicznościach, kierowana poza Urząd Gminy w Kowali, może być przekazana wyłącznie przez Administratora danych lub wyznaczoną przez niego osobę.
20. Każda osoba dopuszczona do przetwarzania danych osobowych obowiązana jest zapoznać się z niniejszą Instrukcją oraz złożyć stosowne oświadczenie dotyczące znajomości wymienionych regulacji.
21. **Osoba upoważniona do przetwarzania danych osobowych za naruszenie obowiązków, wynikających z niniejszej Instrukcji i przepisów o ochronie danych osobowych ponosi odpowiedzialność:**

1] przewidzianą w Kodeksie Pracy za ciężkie naruszenie podstawowych obowiązków pracowniczych, gdy naruszenia dopuścił się pracownik,
2) przewidzianą za istotne naruszenie innego stosunku prawnego, na podstawie którego została upoważniona do przetwarzania danych osobowych, w przypadku innej osoby niż pracownik.

22. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
23. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Raport z naruszenia bezpieczeństwa danych osobowych
w Urzędzie Gminy w Kowali- Stępocinie

1. Data: ..... Godzina: .....
(dd.mm.rrrr) (gg:mm)
2. Osoba powiadamiająca o zaistniałym zdarzeniu:
....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia:
....
(np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
....
....
....
5. Przyczyny wystąpienia zdarzenia:
....
....
....
6. Podjęte działania:
....
....
....
7. Postępowanie wyjaśniające:
....
....
....

……..
(data, podpis Inspektora Ochrony Danych)

……..
(data, podpis Administratora Danych)

Załącznik nr 8
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

WNIOSEK nr…….[1)]
o nadanie/zmianę/odwołanie [2)] uprawnień
do przetwarzania danych osobowych

w …….
(nazwa zbioru/systemu/programu)

Pani/Panu _____
stanowisko _____
nazwa referatu _____
w zakresie następujących danych osobowych:

Czynności dokonywane na danych osobowych	**Tryb dostępu** [2)]
…….. …….. ……..	O / W / M / P / U

Tryb dostępu: O-odczyt, W-wprowadzanie, M-modyfikacja, P-przechowywanie, U-usuwanie, itp.

☐ na okres do dnia …… (termin zakończenia stosunku pracy / stażu / praktyk / umowy cywilno-prawnej)

☐ na czas nieokreślony

☐ na czas wykonania określonych zadań wynikających z: ……..
……

……
……
(podpis i pieczątka IOD) (podpis i pieczątka przełożonego)

Adnotacja o realizacja wniosku[4)]:
Identyfikator użytkownika w systemie:…….
Data realizacji wniosku:…….....
Podpis ASI: ……
* Niepotrzebne skreślić

1) numer nadaje IOD 2) podkreślić właściwe 3) niepotrzebne skreślić 4) dotyczy zbiorów w systemie informatycznym

ZATWIERDZAM

.....
(podpis i pieczątka AD)

Załącznik nr 9
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

UPOWAŻNIENIE / ODWOŁANIE UPOWAŻNIENIA*
Nr ……..
do przetwarzania danych osobowych
w systemach informatycznych lub w zbiorach w wersji papierowej

CZĘŚĆ A - upoważnienie

Działając na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1) - zwanego „RODO"
z dniem _____

Upoważniam
Panią/Pana
stanowisko _____
nazwa referatu _____
do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani* zadań służbowych na zajmowanym stanowisku oraz poleceń przełożonego lub wynikających z zawartej umowy cywilno - prawnej, na poziomie HR ..... *

- ☐ na okres do dnia ..... (termin zakończenia stosunku pracy / stażu / praktyk / umowy cywilno-prawnej)
- ☐ |na czas nieokreślony
- ☐ na czas wykonania określonych zadań wynikających z:

.....

1. udzielając upoważnienia do następujących czynności:

przetwarzanych przy użyciu systemu informatycznego: (podać nazwy systemów lub programów)

i nadaję Pani/ Panu identyfikator:

2. do zbioru przetwarzanego w formie tradycyjnej o nazwie:

……

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Kodeksu pracy, a także Polityką przetwarzania danych osobowych Pracodawcy. Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Polityce.

Deklaracja osoby upoważnianej do przetwarzania danych:

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z prawem, również po ustaniu stosunku pracy, stażu, praktyk umowy cywilno-prawnej oraz do przestrzegania instrukcji i procedur związanych z bezpieczeństwem informacji, w tym z ochroną danych osobowych.

……..
czytelny podpis osoby upoważnianej do przetwarzania danych

…….. ……

Data, podpis I0D Podpis ADO

*

Poziom HR1 - pracownicy zatrudnieni na podstawie umowy o pracę na czas określony i nieokreślony. Poziom ten obejmuje uprawnienie do przetwarzania danych pracowników w okresie zatrudnienia, z prawem dostępu do informacji o wynagrodzeniach itp.
Poziom HR2 - pracownicy zatrudnieni na podstawie umowy o pracę na czas określony i nieokreślony. Poziom obejmuje uprawnienie do przetwarzania danych pracowników w okresie zatrudnienia, bez prawa dostępu do informacji o wynagrodzeniach itp.
Poziom HR3 - stażyści
Poziom HR4 - praktykanci
Poziom HR5 - umowy cywilno-prawne

CZĘŚĆ B - odwołanie upoważnienia
z dniem..... - ..... -..... r.

ODWOŁUJĘ
upoważnienie do przetwarzania danych osobowych nr .....

wydanego
- ☐ na okres do dnia ..... (termin zakończenia stosunku pracy / stażu / praktyk / umowy cywilno-prawnej)
- ☐ na czas nieokreślony
- ☐ na czas wykonania określonych zadań wynikających z:.....

Pani/Panu .....
stanowisko .....
nazwa referatu.....
W przypadku zakończenia stosunku pracy/stażu/praktyk/umowy cywilno-prawnej:
Cofam identyfikator: .....
do zbioru przetwarzanego w formie tradycyjnej o nazwie: ..... ……

…….

Podpis ADO

…….
Data, podpis IDO

Załącznik nr 10
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

EWIDENCJA WYDANYCH UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH							
LP.	Imię i Nazwisko	Zakres upoważnienia - Nazwa Zbioru Danych	Program aplikacja	Identyfikator	Nr upoważnienia	Data nadania	Data odebrania

Załącznik nr 11
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

FORMULARZ
DO ODNOTOWYWANIA UDOSTĘPNIENIA DANYCH OSOBOWYCH

Dane identyfikacyjne wniosku o udostępnienie danych osobowych

Osoba udostępniająca:	
Imię i nazwisko	
Stanowisko służbowe	
Dane osoby, której dane udostępniono	
Imię i nazwisko	
Zakres udostępnionych danych osobowych	
Informacje o odbiorcy danych osobowych	
Nazwa	
Adres	
Imię i nazwisko (jeśli znane):	
Cel udostępnienia danych osobowych	
Data udostępnienia	
Data, czytelny podpis osoby udostępniającej dane	
Data, czytelny podpis ADO	

Czy zgoda na udostępnienie ma charakter zgody (zaznaczyć X właściwy kwadrat):

- ☐ na jednorazowe udostępnienie danych
- ☐ na wielokrotne udostępnienie danych

Załącznik nr 12
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń w Urzędzie Gminy w Kowali – Stępocinie

Zatwierdził:
Wójt Gminy Kowala

Dariusz Bulski

Kwiecień 2024 r.

§ 1 POSTANOWIENIA OGÓLNE

Użyte w niniejszej instrukcji określenia oznaczają:

1. Urząd - Urząd Gminy w Kowali – Stępocinie,.
2. Strefa administracyjna - budynek Urzędu,
3. Bezpośredni przełożony:

a. dla kierowników komórek organizacyjnych i samodzielnych stanowisk - Wójt Gminy Kowala;
b. dla pozostałych pracowników Urzędu - kierownik danej komórki organizacyjnej;

4. Pracownik - pracownik Urzędu.

§2 OCHRONA BUDYNKU URZĘDU

1. Obiekt Urzędu objęty jest systemem alarmowym oraz monitoringiem wizualnym zamontowanym w budynku.
2. Budynek podlega dozorowi i ochronie polegającej na:

a. całodobowym monitorowaniu przez Agencję lokalnego systemu alarmowego zamontowanego w obiekcie;
b. całodobowym monitoringu wizualnym za pomocą lokalnego systemu kamer oraz rejestratora video zamontowanego w obiekcie.

3. Do obowiązków Agencji należy:

a. przyjmowanie i rejestracja sygnałów systemu przez całą dobę, również w dni świąteczne i wolne od pracy;
b. powiadamianie wyznaczonych osób z Urzędu o przypadkach wystąpienia alarmu w chronionym obiekcie;
c. zapewnienie gotowości do działań ochronnych grup patrolowo - interwencyjnych w przypadku wystąpienia zdarzenia załączenia alarmu;
d. zapewnienie fizycznej ochrony obiektu do czasu ustąpienia przyczyn alarmu;
e. kontrola załączeń i wyłączeń systemu zgodnie z ustalonym rozkładem pracy systemu;
f. niezwłoczne podjęcie ochrony fizycznej obiektu, a w przypadku braku możliwości monitorowania systemu, ustalenie przyczyn zdarzenia i zawiadomienie Pracownika ds. Obrony Cywilnej o zaistniałym zdarzeniu.

4. Szczegółowy zakres obowiązków i ustaleń w zakresie ochrony i dozoru reguluje umowa zawarta pomiędzy Urzędem a Agencją.
5. Konserwację i naprawę systemu alarmowego i monitoringu wizualnego w sposób zapewniający bezawaryjne jego działanie wykonuje zewnętrzna firma. Szczegółowy zakres obowiązków w zakresie konserwacji i napraw reguluje umowa zawarta pomiędzy Urzędem a zewnętrzną firmą.
6. Z uwagi na publiczny charakter Urzędu w czasie jego pracy nie obowiązuje system przepustek, ani też inny system określający uprawnienia do wejścia, przebywania i wyjścia ze strefy administracyjnej.
7. W godzinach pracy Urzędu zobowiązuje się pracowników w szczególności do:

a. zwracania uwagi na zachowanie osób wchodzących i wychodzących z Urzędu;
b. reagowania na wejście do budynku i przebywanie w strefie administracyjnej osób będących pod wpływem alkoholu lub podobnie działającego środka;
c. reagowania na próby niszczenia lub wynoszenia mienia z obiektu Urzędu;
d. reagowania na próby wnoszenia do obiektu Urzędu przedmiotów i materiałów niebezpiecznych;
e. natychmiastowego reagowania poprzez powiadomienie odpowiednich służb oraz osób o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.

ZABEZPIECZENIE POMIESZCZEŃ I POSTĘPOWANIE Z KLUCZAMI

1. Otwarcia strefy administracyjnej po porze nocnej dokonuje wyznaczony pracownik, nie wcześniej niż na 30 minut przed godziną rozpoczęcia pracy Urzędu.
2. Zamknięcie dostępu zewnętrznego do strefy administracyjnej po zakończeniu dnia pracy i załączeniu systemu alarmowego w obiekcie należy do obowiązków wyznaczonego pracownika. Niedopuszczalne jest pozostawienie pomieszczeń bez nadzoru systemu alarmowego.
3. Wszystkie klucze od pomieszczeń wewnątrz strefy administracyjnej znajdują się w zamykanej gablocie w pok. nr 27.

4. Pracownik, który pobrał klucz(e) od pomieszczenia(eń), przed uruchomieniem zamków sprawdza od strony wizualnej stan tych zamków i ewentualnych zabezpieczeń zastosowanych przy zamykaniu pomieszczeń, a także używanych plomb (jeżeli takie są lub będą przewidziane).
5. Po otwarciu pomieszczeń biurowych, jeszcze przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, a także składowanej w tych pomieszczeniach dokumentacji i innego wyposażenia.
6. W przypadku stwierdzenia zmian lub naruszeń stanu zabezpieczeń pracownik, który to stwierdził, natychmiast powiadamia o tym fakcie Wójta Gminy Kowala.
7. Od momentu pobrania kluczy do momentu ich zdania na pracownikach spoczywa pełna odpowiedzialność za ochronę kluczy i pomieszczeń biurowych.
8. W przypadku utraty, uszkodzenia lub zniszczenia kluczy użytkownik niezwłocznie powiadamia o tym fakcie Wójta Gminy Kowala.
9. Po zakończeniu dnia pracy, pracownicy Urzędu zobowiązani są do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających głównie na:

a. zabezpieczeniu dokumentacji;
b. zabezpieczeniu komputerów;
c. wyłączeniu urządzeń energetycznych zasilanych energią elektryczną;
d. zamknięciu okien i drzwi;
e. zdaniu kluczy od pomieszczeń.

10. Klucze od biurek stanowiskowych, szaf biurowych i pieczątek są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie. Po godzinach pracy biurka, szafy zawierające klucze i pieczątki są zamykane.
11. Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń Urzędu oraz drzwi zewnętrznych są przechowywane w pok. nr 27 w zamkniętej gablocie w opisanej, opieczętowanej i zaklejonej kopercie.
12. Wydawanie kluczy zapasowych pracownikom uprawnionym do ich pobrania może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych, za zgodą i wiedzą Wójta. Na powyższą okoliczność sporządza się notatkę służbową. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
13. Do otwierania pomieszczeń dla potrzeb wykonywania czynności związanych ze sprzątaniem wykorzystywany jest odrębny komplet kluczy.
14. Pomieszczenia Urzędu Stanu Cywilnego, Pracownika ds. Obrony Cywilnej, Spraw Wojskowych, Zarządzania Kryzysowego i Administratora Bezpieczeństwa Informacji, Kasy, Pracownika ds. informatycznych oraz Serwerowni sprzątane są wyłącznie w godzinach pracy Urzędu i w obecności zatrudnionych tam pracowników.
15. Dorabianie kluczy do pomieszczeń i budynku Urzędu wymaga pisemnej zgody Wójta Gminy Kowala i dozwolone jest wyłącznie w celu zastąpienia kluczy utraconych, uszkodzonych lub zniszczonych.
16. Jeżeli z okoliczności udostępnienia kluczy osobie nieupoważnionej lub jego utraty wynika, że może zostać wykorzystany do nieuprawnionego dostępu do pomieszczeń lub budynku, należy wymienić odpowiedni zamek lub jego elementy. O zaistniałej sytuacji należy niezwłocznie powiadomić Wójta Gminy Kowala.
17. Zabrania się:

a. udostępniania kluczy osobom nieupoważnionym,
b. pozostawiania otwartych pomieszczeń lub kluczy bez dozoru,
c. pozostawiania otwartych okien po zakończeniu pracy.

18. Klucze do drzwi zewnętrznych są powierzane, po złożeniu Oświadczenia - załącznik nr 1 do Instrukcji, wyznaczonym przez Wójta Gminy Kowala osobom w celu zapewnienia otwierania i zamykania Urzędu.
19. Komplet kluczy do drzwi zewnętrznych posiadają osoby upoważnione przez Wójta Gminy Kowala do otwierania i zamykania Urzędu
20. W przypadku zgubienia kluczy do drzwi wejściowych należy niezwłocznie powiadomić Wójta Gminy Kowala.
21. Wójtem Gminy Kowala niezwłocznie podejmuje czynności w celu zabezpieczenia dostępu

do drzwi, do których zostały zagubione klucze.

22. Nadzór nad kluczami oraz rejestr osób będących w posiadaniu kluczy prowadzi Wójt w porozumieniu z Sekretarzem Gminy lub wyznaczona przez niego osoba. Wzór Rejestru osób posiadających klucze do drzwi zewnętrznych Urzędu Gminy w Kowali – Stępocinie stanowi załącznik nr 2 do Instrukcji.
23. Rejestr zatwierdza każdorazowo Wójta Gminy Kowala.
24. Komplety kluczy do drzwi wejściowych na teren strefy administracyjnej są w osobistym posiadaniu następujących osób:

a. Wójta Gminy Kowala,
b. jeden pracownik Urzędu,
c. dwie osoby sprzątające.

25. Osoby wymienione w pkt. 24 uprawnione są do znajomości kodu cyfrowego systemu alarmowego w obiekcie.

POSTANOWIENIA KOŃCOWE

Utrzymanie skutecznego zabezpieczenia technicznego strefy administracyjnej, stosownie do obowiązujących wymogów w tym zakresie, podlega nadzorowi Wójta.

Załącznik nr 1
Instrukcji postępowania z kluczami
oraz zabezpieczenia pomieszczeń
w Urzędzie Gminy w Kowali – Stępocinie

Oświadczenie
o odpowiedzialności za posiadane klucze do drzwi zewnętrznych
Urzędu Gminy w Kowali - Stępocinie

Data: ____

Imię i nazwisko: ____

Oświadczam, że w związku z przekazaniem mi kluczy do drzwi zewnętrznych Urzędu Gminy w Kowali- Stępocinie ul. Marii Walewskiej 7, 26-624 Kowala - Stępocina, ponoszę pełną odpowiedzialność za szkody wynikające z mojej winy związane z nieprzestrzeganiem zasad określonych w Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Gminy w Kowali - Stępocinie, stanowiącej Załącznik do Polityki bezpieczeństwa przetwarzania danych wprowadzonej do stosowania Zarządzeniem Nr .....Wójta Gminy Kowala z dnia.....

Czytelny podpis ____

Załącznik nr 2
Instrukcji postępowania z kluczami
oraz zabezpieczenia pomieszczeń w
Urzędzie Gminy w Kowali - Stępocinie

Rejestr osób
posiadających klucze do drzwi zewnętrznych Urzędu Gminy w Kowali - Stępocinie

W trwałym posiadaniu są:
1. Wójt Gminy Kowala,
2. wyznaczony Pracownik Urzędu,
3. wyznaczone dwie osoby sprzątające pomieszczenia Urzędu.

Data:.....

Zatwierdzam: …….

Załącznik nr 13
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE
(wzór)

Lp	Nazwa zbioru	Kom. organizacyjna	Pokój nr

Załącznik nr 14
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

WYKAZ ZBIORÓW DANYCH OSOBOWYCH (wzór)					
Lp	**Nazwa zbioru**	**Kom. organizacyjna**	**Data zgłoszenia**	**Data wykreślenia**	**Nr księgi**
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					

Załącznik nr 15
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

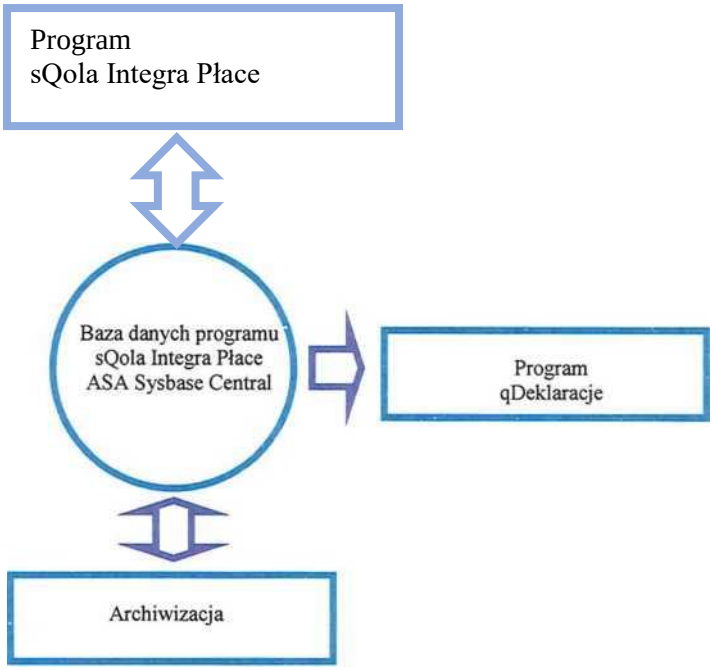
(WZÓR)
WYKAZ SYSTEMÓW INFORMATYCZNYCH
SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa zbioru	Kom. organizacyjna	Program	Serwer
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				

Załącznik nr 16
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

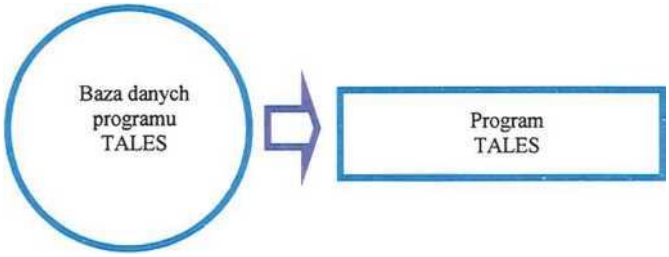
OPISY STRUKTUR ZBIORÓW DANYCH
wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi
oraz sposobu przepływu danych pomiędzy systemami

sOola Integra Płace

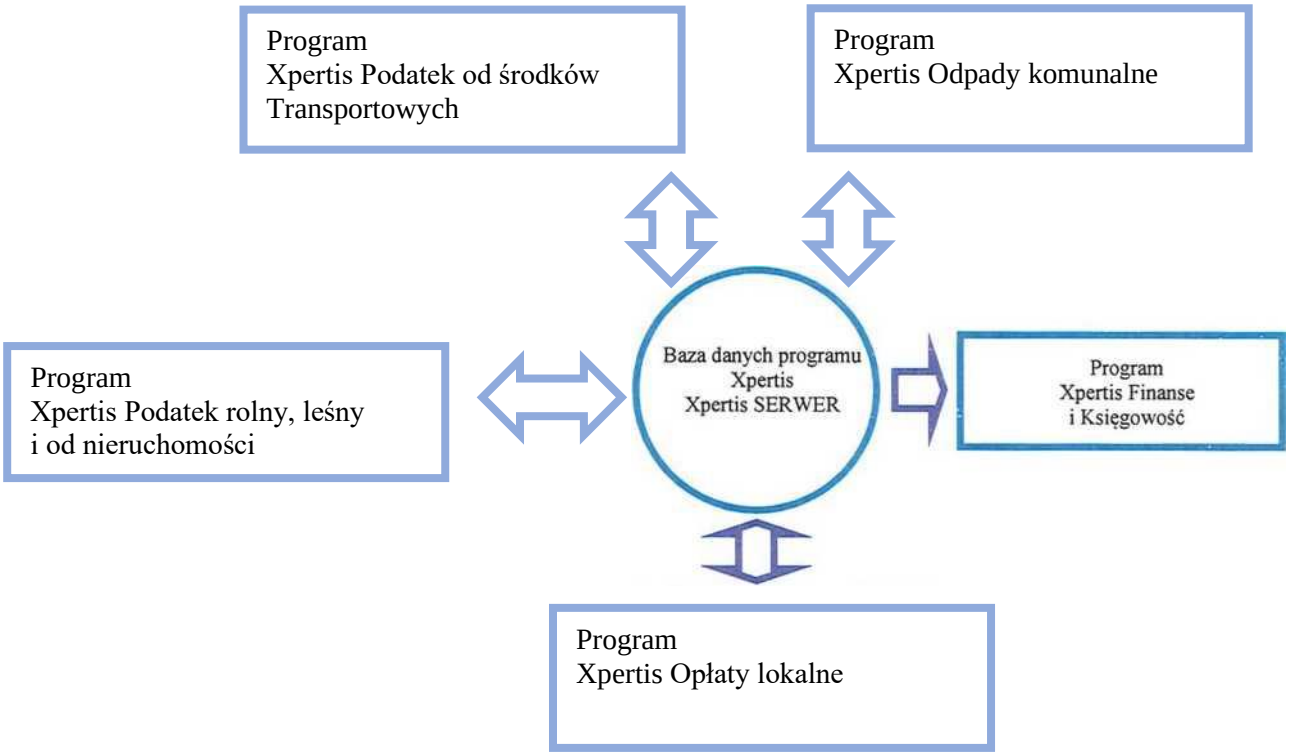


gDeklaracie

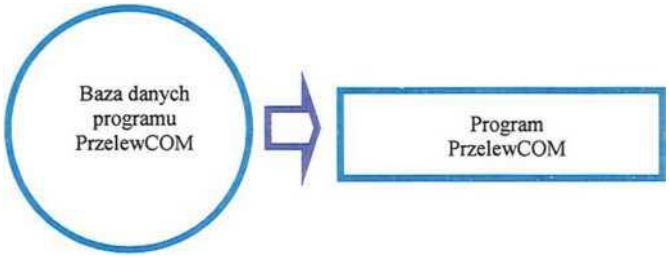
TALES



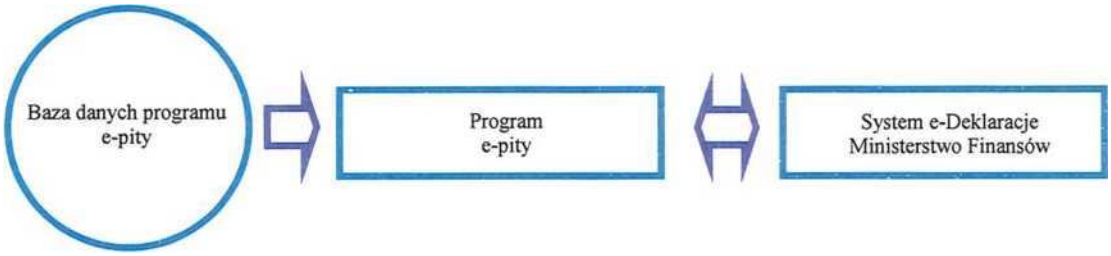
Xpertis Podatek od środków Transportowych; Xpertis Podatek rolny, leśny i od nieruchomości; Xpertis Finanse i Księgowość



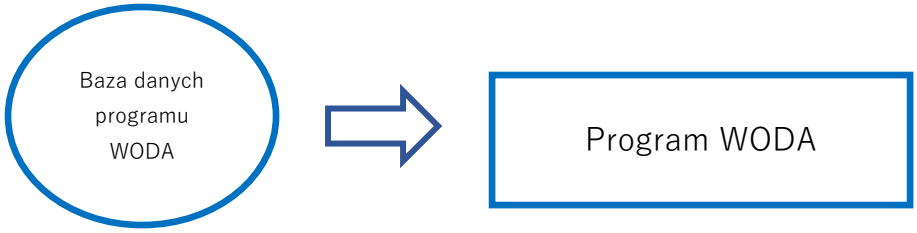
PrzelewCom



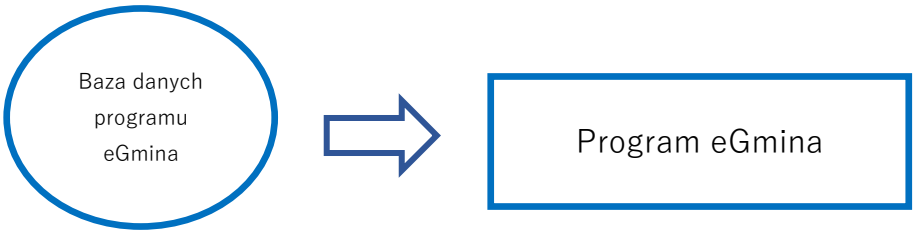
e-pity



WODA



eGmina



System Informacji Oświatowej - SIO

Rejestr nośników
(wzór)

LP.	Nazwa nośnika	Identyfikator

Załącznik nr 18
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

…….
(pieczątka)

UPOWAŻNIENIE Nr..... /

Na podstawie *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Kowali* upoważniam Panią/a* pracującą/ego na stanowisku do wynoszenia dokumentacji:

1. w systemie tradycyjnym*
2. na nośniku*

zgodnie z zakresem czynności/współpracy w obrębie:

1. gminy*
2. powiatu*
3. województwa*
4. na terenie całego kraju*

na czas:

1. nieokreślony to znaczy do dnia zakończenia pracy/współpracy* z Administratorem Danych
2. określony od..... do..... *

……
(podpis ADO)

……
(kontrasygnata IOD)

*niepotrzebne skreślić

Załącznik nr 19
do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Urzędzie Gminy w Kowali - Stępocinie

REJESTR WYDANYCH UPOWAŻNIEŃ DO WYNOSZENIA NOŚNIKÓW (wzór)							
LP.	**Imię i Nazwisko**	**Zakres upoważnienia - Nazwa Zbioru danych**	**Program aplikacja**	**Identyfikator**	**Nr upoważnienia**	**Data nadania**	**Data odebrania**