ZARZĄDZENIE NR 8/2019

WÓJTA GMINY DĄBROWA

z dnia 18 lutego 2019r.

w sprawie wprowadzenia Polityki Ochrony Danych w Urzędzie Gminy w Dąbrowie

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2016 r., poz. 446) i art. 24 ust. 1 i2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/4/WE zarządza, co następuje:

§ 1 Celem określenia reguł i zasad obowiązujących przy przetwarzaniu danych osobowych w Urzędzie Gminy w Dąbrowie wprowadza się Politykę Ochrony Danych Osobowych w Urzędzie Gminy w Dąbrowie w brzmieniu jak w załączniku do niniejszego zarządzenia.

§ 2 Zobowiązuje się wszystkich pracowników Urzędu Gminy w Dąbrowie do przestrzegania postanowień zawartych w Polityce Ochrony Danych Osobowych.

§ 3. Traci moc Zarządzenie nr 6/2015 Wójta Gminy Dąbrowa z dnia 27 stycznia 2015r. w sprawie ustalenia Polityki przetwarzania danych osobowych w Urzędzie Gminy w Dąbrowie i Instrukcji zarządzania systemów informatycznym do przetwarzania danych osobowych Urzędu Gminy w Dąbrowie.

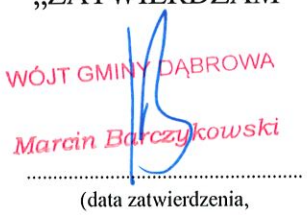
§ 6 Zarządzenie wchodzi w życie z dniem 18 lutego 2019r.

WÓJT

Marcin Barczykowski

Urząd Gminy w Dąbrowie

„ZATWIERDZAM”



.....

(data zatwierdzenia,
podpis i pieczątka Administratora)

POLITYKA OCHRONY DANYCH

Rodzaj dokumentu:	Regulacja wewnętrzna – wyłącznie do użytku wewnętrznego - objęta obowiązkiem zachowania poufności

Historia zmian:

Wersja dokumentu	Data wprowadzenia	Data wycofania	Opis zmian

Dąbrowa 2018

SPIS TREŚCI

ROZDZIAŁ I
CEL DOKUMENTU / PODSTAWY PRAWNE

1. CEL DOKUMENTU

Polityka Ochrony Danych (POD) w Urzędzie Gminy w Dąbrowie jest dokumentem precyzującym zasady przetwarzania danych osobowych, w szczególności w odniesieniu do zapewnienia ochrony przetwarzanych danych osobowych przed zagrożeniami utraty poufności, integralności i dostępności, realnymi zarówno zewnątrz, jak i wewnątrz Urzędu.

POD ma zastosowanie do wszystkich osób przetwarzających dane osobowe w Urzędzie Gminy, w szczególności pracowników Urzędu, a także osób niezwiązanych umową o pracę, które legalnie uzyskały dostęp do danych. Zasady określone w tym dokumencie mają także wpływ na realizację działań poprzez podmioty zewnętrzne, które przetwarzają dane osobowe w imieniu Administratora.

Postanowienia tego dokumentu określają m.in:

a) środki techniczne i organizacyjne niezbędne dla zapewniania poufności, integralności oraz dostępności przetwarzanych danych,
b) wymagania w zakresie udostępniania i bezpieczeństwa przetwarzania danych osobowych,
c) zasady prowadzenia wymaganych rejestrów,
d) zasady nadawania i cofania upoważnień do przetwarzania danych osobowych,
e) procedery postępowania w przypadku powstania incydentu lub naruszenia w zakresie ochrony danych osobowych.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje całkowitego bezpieczeństwa systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające przede wszystkim z błędów ludzkich. Dokumentacja zawiera niezbędne podstawy przetwarzania danych osobowych, w tym postępowania z ryzykiem, oraz uwzględnia postępowanie wynikające ze specyfiki przetwarzana danych w Urzędzie.

Zagadnienia wiążące się z koniecznością ich modyfikacji opracowano w postaci załączników, stanowiących zbiór szczegółowych procedur, polityk i instrukcji będących integralną częścią niniejszego dokumentu, których wykaz zawiera Załącznik nr 1. Wprowadzenie nowych załączników oraz dokonanie zmian w istniejących załącznikach uważa się za obowiązujące z dniem ich skutecznego opublikowania w Urzędzie. Wprowadzenie zmian wymaga każdorazowo aktualizacji załącznika nr 1. Zmiany w dokumencie głównym niniejszej Polityki dokumentowane są tabeli pn.: „Historia zmian".

2. PODSTAWY PRAWNE

- ✓ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. U. E. L 119/1 z 4.5.2016),
- ✓ Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000)

3. Wykaz użytych pojęć

1. **ADO** albo **Administrator** – Administrator Danych Osobowych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w jednostkach samorządu terytorialnego Administratorem jest gmina, reprezentowana przez Wójta.
2. **ANALIZA RYZYKA** – etap w zarządzaniu ryzykiem polegający na określeniu prawdopodobieństwa wystąpienia zagrożenia, w celu określenia wartości punktowej ryzyka,
3. **ASI** – Administrator Systemu Informatycznego, osoba odpowiedzialna w Urzędzie za prawidłowe funkcjonowanie systemu informatycznego,
4. **B2B** – Współpraca na zasadzie Biznes to Biznes
5. **DANE DOTYCZĄCE ZDROWIA** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
6. **DANE OSOBOWE** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
7. **DOSTĘPNOŚĆ** – właściwość polegająca na zapewnieniu, że osoby upoważnione mają dostęp do informacji wtedy, gdy jest to potrzebne.
8. **IDENTYFIKATOR UŻYTKOWNIKA** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. **INCYDENT** – zdarzenie lub podejrzenie zdarzenia mogącego mieć negatywny wpływ na bezpieczeństwo danych osobowych.
10. **IND** – informatyczny nośnik danych wykorzystywany do przetwarzania danych osobowych, w szczególności dysk twardy, dysk SSD, płyty CD/DVD/BD, pendrive.
11. **INTEGRALNOŚĆ** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
12. **IOD** – Inspektor Ochrony Danych.
13. **LADO** – Lokalny Administrator Danych Osobowych to pracownik kierujący komórką organizacyjną albo zespołem pracowników, będący przełożonym lub kierującym

pracownikiem mających dostęp do danych osobowych, w zakresie podległej komórki; LADO jest właścicielem zasobów podległej mu komórki.

14. **NARUSZENIE OCHRONY DANYCH OSOBOWYCH** – 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.
15. **ODBIORCA** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane niezależnie od tego czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
16. **OGRANICZENIE PRZETWARZANIA** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
17. **ORGAN NADZORCZY** albo **PUODO** – Prezes Urzędu Ochrony Danych Osobowych,
18. **PODATNOŚĆ** – właściwość lub system działań stwarzający możliwość zewnętrznej lub wewnętrznej, nieupoważnionej ingerencji naruszającej jego zasady.
19. **PODMIOT PRZETWARZAJĄCY** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
20. **POD** – Polityka Ochrony Danych;
21. **POUFNOŚĆ** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom oraz innym podmiotom.
22. **PRACOWNIK** – Upoważniona osoba świadcząca pracę, osoby na umowach cywilno-prawnych (o dzieło, zlecenie), a także stażyści oraz praktykanci,
23. **PROFILOWANIE** – dowolna forma 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.
24. **PRZETWARZANIE** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
25. **PSEUDONIMIZACJA** – przetworzenie danych w sposób uniemożliwiający ich przypisanie 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.
26. **URZĄD** lub **URZĄD GMINY** – Urząd Gminy w Dąbrowie.
27. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. U. E. L 119/1 z 4.5.2016).

28. **ROZLICZALNOŚĆ** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
29. **RYZYKO** – niepewność związana z wystąpieniem okoliczności lub zdarzenia, grożącego brakiem lub ograniczeniem możliwości realizacji zamierzonych celów jednostki organizacyjnej, określanych zarówno w perspektywie krótko jak i długoterminowej.
30. **SKD** – system kontroli dostępu do obiektów lub pomieszczeń.
31. **SSNiW** – system sygnalizacji napadu i włamania do obiektów lub pomieszczeń.
32. **STRONA TRZECIA** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
33. **SYSTEM INFORMATYCZNY** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
34. **UODO** – Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2018 r., poz. 1000).
35. **USUNIĘCIE DANYCH** - zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
36. **WŁAŚCICIEL ZASOBU** – osoba, która korzysta z określonych zasobów oraz ponosi odpowiedzialność za ich bezpieczeństwo.
37. **WSPÓŁADMINISTRATOR** – osoba lub podmiot, która w ramach pełnienia obowiązków ADO w zespole składającym się co najmniej dwóch administratorów prowadzi działania w oparciu o wspólnie uzgodnione cele i sposoby przetwarzania danych.
38. **ZAGROŻENIE** – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub jednostce organizacyjnej.
39. **ZARZĄDZANIE RYZYKIEM** – skoordynowane działania podejmowane przez kierownika jednostki organizacyjnej mające na celu identyfikację zagrożeń i podatności, minimalizację zagrożeń do poziomu ryzyka akceptowalnego poprzez zastosowanie zabezpieczenia lub zabezpieczeń.
40. **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.
41. **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.

ROZDZIAŁ II
OBSZAR PRZETWARZANIA DANYCH

1. Obszar przetwarzania danych

Obszar przetwarzania danych w Urzędzie Gminy ograniczony jest do części budynku i znajdujących się tam pomieszczeń służbowych. Dopuszczalne jest przetwarzanie danych w siedzibach innych podmiotów, np. w związku z prowadzonymi czynnościami szkoleniowymi czy serwisowymi pod warunkiem, że odbywa się to pod nadzorem pracowników Urzędu .

2. Zasady ochrony obszaru przetwarzania danych

1. Dostęp do budynku oraz poszczególnych pomieszczeń, w których odbywa się przetwarzanie danych osobowych, zabezpieczony jest co najmniej za pomocą drzwi zamykanych zamkiem patentowym. Dodatkowo budynek zabezpieczony jest alarmem, kody do alarmu posiadają wyznaczeni pracownicy zgodnie z rejestrem.
2. Budynek jest wolnostojący i częściowo ogrodzony, teren przyległy częściowo pozostaje pod stałym nadzorem kamery.
3. Wejście do części budynku wykorzystywanej przez Urząd oraz wejścia do pomieszczeń, w której są przetwarzane dane osobowe, w czasie godzin pracy pozostają pod stałym nadzorem pracowników. Po godzinach służbowych pomieszczenia są zamknięte, a klucze zdane do przechowania. Klucze do pomieszczeń wydawane są uprawnionym pracownikom na podstawie wykazu sporządzonego przez Administratora. Klucz do wejścia do budynku są w posiadaniu wyznaczonych pracowników zgodnie z rejestrem
4. Niedopuszczalne jest pozostawianie klucza w zamku drzwi wejściowych do pomieszczenia zarówno w trakcie godzin pracy jak i po godzinach pracy.
5. Pracownicy zobowiązani są do zabezpieczania przed dostępem osób nieuprawnionych pomieszczeń, w których przetwarzają dane osobowe. W szczególności osoby te zobowiązane są do zamykania pomieszczeń na klucz, jeżeli opuszczają je jako ostatni, zarówno w razie ich chwilowej nieobecności, jak i po zakończeniu wykonywania pracy.
6. Interesanci mogą przebywać w pomieszczeniach służbowych wyłącznie pod stałym nadzorem pracownika. W przypadku konieczności opuszczenia pomieszczenia, pracownik jest zobowiązany zapewnić nadzór nad interesantem przez innego pracownika, albo polecić interesantowi opuszczenie pomieszczenia.
7. Po zakończeniu pracy każda osoba upoważniona do przetwarzania danych osobowych zamyka dokumenty zawierające dane osobowe oraz IND w szafach metalowych albo meblach biurowych zamykanych na klucz. Klucze do tych mebli biurowych pracownik zabezpiecza przed opuszczeniem pomieszczenia.
8. Praca na stanowisku powinna przebiegać zgodnie z „zasadą czystego biurka", opisaną w załączniku pn.: „Polityka czystego ekranu i biurka".
9. Dokumentacja zawierająca dane osobowe może być przechowywana w powszechnie dostępnych częściach pomieszczeń, bez stosowania środków, o których mowa w ust. 5 powyżej wyłącznie na czas wykonywania pracy na tych dokumentach w danym dniu pracy,

przy jednoczesnej obecności w tym pomieszczeniu osoby upoważnionej do przetwarzania danych osobowych.

10. Sprzątanie pomieszczeń, w których skuteczne zabezpieczenie danych osobowych jest niemożliwe, może się odbywać wyłącznie w obecności i pod nadzorem upoważnionego pracownika.

ROZDZIAŁ III –
STRUKTURA OCHRONY DANYCH OSOBOWYCH

1. Zasady Ogólne – Funkcje osób w procesie ODO

Administrator danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne oraz organizacyjne, aby ich przetwarzanie było zgodne z RODO oraz UODO.
Za prawidłowe przetwarzanie danych osobowych odpowiada ADO.

2. Administrator Danych Osobowych

ADO realizuje obowiązki wynikające z przepisów poprzez:

1) zatwierdzenie i wdrożenie do stosowania dokumentacji oraz jej nowelizacji, a także innych regulacji wewnętrznych z zakresu przetwarzania danych osobowych;
2) wyznaczenie:
   a) Inspektora Ochrony Danych,
   b) Administratora Systemu Informatycznego, wykorzystywanego do przetwarzania danych osobowych,
   c) pracownika realizującego czynności związane z ochroną danych, w tym m.in. prowadzenie rejestrów/wykazów, przygotowania upoważnień itp.;
3) zapewnienie sił oraz środków na realizację czynności związanych z zapewnieniem bezpieczeństwa przetwarzanych danych, w szczególności tych zaleconych przez IOD;
4) wdrożenie zabezpieczeń organizacyjnych i technicznych zapewniających bezpieczeństwo przetwarzania danych osobowych, z uwzględnieniem potencjalnych zagrożeń dla tego bezpieczeństwa oraz wyników okresowo przeprowadzanej analizy ryzyka;
5) zapewnienie prowadzenia rejestru czynności oraz rejestru kategorii czynności przetwarzanych danych;
6) podejmowanie decyzji w sprawie skierowanych przez IOD rekomendacji i wniosków w sprawach dotyczących danych osobowych.

3. LADO - Właściciel Zasobu

LADO - w zakresie podległej im komórki w szczególności:

1) sprawuje bieżący nadzór nad bezpieczeństwem przetwarzanych danych osobowych;
2) wnioskuje o nadawanie, zmianę lub wycofanie uprawnień do przetwarzania danych osobowych podległym pracownikom;
3) zapewnia realizację obowiązku informacyjnego, o którym mowa w art. 13 i art. 14 RODO;

4) prowadzi rejestru czynności przetwarzania podległych mu zasobów (kopie przekazuje ADO);
5) realizuje bieżące zalecenia IOD mające na celu zapewnienie prawidłowego przetwarzania danych osobowych;
6) zgłasza wykryte przypadki naruszenia/incydentu (lub ich podejrzenia) bezpieczeństwa danych osobowych;
7) sprawuje nadzór nad prawidłowym przetwarzaniem danych osobowych przez podległych pracowników;
8) w zakresie czynności, uprawnień i odpowiedzialności podległych pracowników określa szczegółowo zakres obowiązków i uprawnień związanych z przetwarzaniem danych osobowych;
9) organizuje i nadzoruje właściwe zabezpieczenie pomieszczeń, w których przetwarzane są dane osobowe;
10) sporządza wykaz pomieszczeń, w których sprzątanie musi odbywać się w godzinach urzędowania pod nadzorem upoważnionych pracowników;
11) wykaz pracowników upoważnionych do pobierania i zdawania na przechowanie kluczy do pomieszczeń, w których przetwarzane są dane osobowe;
12) nadzoruje udostępnianie informacji ze zbiorów danych przetwarzanych w podległej komórce oraz dokumentowanie tych czynności;
13) określa zasady i częstotliwość sporządzania oraz przechowywania kopii zapasowych zbiorów przetwarzanych i przechowywanych lokalnie, wyłączonych z systemu sporządzania kopii zapasowych realizowanych przez ASI;
14) występuje do IDO o wydanie upoważnienia do przetwarzania danych osobowych;
15) zapewnia realizację szkolenia w zakresie ochrony danych osobowych podległych pracowników oraz zapoznanie pracowników z dokumentacją, w tym POD,
16) występuje z wnioskiem do ASI o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych w systemie informatycznym;
17) informuje IDO o wszelkich stwierdzonych nieprawidłowościach związanych z przetwarzaniem danych osobowych;
18) informuje ASI o:
    - nieprawidłowościach w działaniu systemu informatycznego oraz konieczności unowocześnienia lub naprawy sprzętu,
    - konieczności dokonania zmian w konfiguracji sprzętu i oprogramowania ze szczególnym uwzględnieniem wymagań określonych w zarządzeniu,
    - konieczności zniszczenia wycofanego z użycia nośnika informatycznego albo trwałego usunięcia danych z nośnika informatycznego wykorzystywanego do przetwarzania danych osobowych przewidzianego do użytkowania w innym systemie teleinformatycznym,
19) występuje do IDO z propozycjami zmian w organizacji i zabezpieczeniu przetwarzania danych osobowych zmierzającymi do usprawnienia pracy i bezpieczeństwa danych osobowych;
20) informuje IOD i konsultuje z nim projekt odpowiedzi na zapytania skierowane do ADO w związku z realizacją praw osób, których dane dotyczą;
21) dokumentuje realizację w/w czynności.

4. Inspektor Danych Osobowych

1. Inspektor ochrony danych ma następujące zadania:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochronie danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
   d) współpraca z organem nadzorczym;
   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji w innych sprawach.
2. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

5. ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

W celu zapewnienia odpowiedniej obsługi informatycznej systemów, w których przetwarzane są dane osobowe, ADO wyznaczył Administratora Systemu Informatycznego, którym jest osoba odpowiedzialna za obsługę informatyczną Urzędzie.

ASI realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym ADO, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji profilu administratora,
2) przeciwdziała nieupoważnionemu dostępowi do sieci wewnętrznej oraz wszystkich urządzeń sieciowych, w których przetwarzane są dane osobowe,
3) prowadzi rejestr pracowników (w tym także ich identyfikatorów) upoważnionych do przetwarzania danych osobowych w systemie informatycznym,
4) prowadzi rejestr komputerów, w których przetwarzane są dane osobowe,
5) przydziela, na pisemny wniosek LADO, użytkownikowi identyfikator oraz hasło do systemu informatycznego, nadaje i odbiera uprawnienia, a także usuwa konta użytkowników zgodnie z odpowiednią procedurą,
6) nadzoruje działanie zastosowanych mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

7) konfiguruje system informatyczny w oparciu o zasady określone w procedurze, a w szczególności dba o:
   - konfigurację systemu operacyjnego oraz programów (jeżeli istnieje taka możliwość) w komputerach, w których przetwarzane są dane osobowe, wymuszającą okresową zmianę haseł użytkownika,
   - stosowanie i prowadzenie listy haseł do ustawień konfiguracyjnych BIOS komputerów (hasło ASI),
   - konfigurację dziennika zdarzeń systemu w sposób umożliwiający kontrolę czasu pracy poszczególnych użytkowników, a także pracy w programach obsługujących zbiory (jeżeli istnieje taka możliwość),
   - zakładanie kont użytkownikom komputera w oparciu o minimalne uprawnienia użytkownika określone w systemie operacyjnym Windows jako „użytkownik",
   - wyłącza dostęp do komputera przez konto „gość" oraz nieużywane urządzenia do komunikacji zewnętrznej,
   - z poziomu BIOS ustawia dysk twardy komputera jako jedyną lokalizację systemu operacyjnego,
8) prowadzi rejestr naruszeń i incydentów związanych z bezpieczeństwem danych osobowych,
9) informuje IDO o stwierdzonych nieprawidłowościach związanych z bezpieczeństwem systemu informatycznego i podejmuje czynności zmierzające do zabezpieczenia systemu,
10) występuje do IDO z propozycjami zmian w organizacji i zabezpieczeniu przetwarzania danych osobowych zmierzającymi do usprawnienia pracy i bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
11) sprawuje nadzór nad:
   - wykonywaniem napraw i konserwacją urządzeń i oprogramowania w systemie informatycznym,
   - wykonywaniem kopii zapasowych serwera oraz innych zasobów wskazanych przez LADO, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
12) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej,
13) na wniosek LADO:
   - niszczy wycofane z użycia IND wykorzystywane w systemach IT do przetwarzania danych osobowych,
   - usuwa bezpowrotnie dane osobowe z nośników informatycznych wykorzystywanych do przetwarzania danych osobowych, które mają być wykorzystywane w innych systemach informatycznych;

6. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zapewnienia poufności przetwarzanych danych osobowych oraz stosowania się do obowiązujących w tym zakresie uregulowań. W szczególności zobowiązana jest do:

1) przetwarzania danych osobowych wyłącznie:
   - w ramach tego zbioru, do którego otrzymała upoważnienie,
   - w sposób i w zakresie wynikającym z posiadanych uprawnień i obowiązków oraz faktycznych potrzeb służbowych, określonych przez LADO,
2) zachowania w tajemnicy przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z zajmowanego stanowiska:
   - danych osobowych uzyskanych w trakcie wykonywania czynności służbowych,
   - wszelkich informacji o stosowanych procedurach i zabezpieczeniach danych osobowych i systemów informatycznych,
3) zapoznania się i stosowania do przepisów prawa i uregulowań wewnętrznych dot. ochrony danych osobowych,
4) udziału w szkoleniach z zakresu ochrony danych osobowych,
5) właściwego zabezpieczenia danych osobowych przetwarzanych w formie tradycyjnej (papierowej) poprzez uniemożliwienie dostępu do dokumentów osobom nieupoważnionym - w szczególności poprzez zabezpieczenie dokumentów w szafach zamykanych na klucz i zamykaniu pomieszczenia służbowego,
6) właściwego zabezpieczenia danych osobowych przetwarzanych w formie elektronicznej, nieudostępniania swojego identyfikatora i hasła oraz posiadanych informacji o zastosowanych zabezpieczeniach, a także do zabezpieczenia oprogramowania i IND,
7) niezwłocznego informowania LADO o stwierdzonych nieprawidłowościach, w szczególności:
   - dotyczących zabezpieczenia pomieszczeń,
   - śladach wskazujących na podmianę sprzętu lub jego elementów, włamanie do systemu,
   - utracie, braku dostępu lub nieautoryzowanej modyfikacji danych,
   - innych stwierdzonych nieprawidłowościach mających wpływ na bezpieczeństwo danych osobowych,
8) wykorzystywania do pracy w systemie wyłącznie przydzielonego przez ASI profilu z wyłączeniem systemu informatycznego, w którym ze względu na charakter programu wykorzystywanego do obsługi zbioru nie jest to możliwe,
9) niewykonywania we własnym zakresie kopii przetwarzanych danych bez wiedzy i zgody LADO oraz na nośnikach niewydanych przez LADO lub ASI,
10) niepodejmowania jakichkolwiek prób obejścia zastosowanych zabezpieczeń oraz dokonywania zmian w konfiguracji systemu operacyjnego, wyłączania programu antywirusowego i zrywania nalepek zabezpieczających,
11) niedokonywania samodzielnej podmiany elementów lub przenoszenia zestawu komputerowego.

ROZDZIAŁ IV
ZASADY POSTĘPOWANIA PRZY PRZETWARZANIU DANYCH

1. Zasady ogólne

Każdy pracownik lub współpracownik zbierający dane osobowe bezpośrednio od osoby, której one dotyczą bądź za pośrednictwem innych osób lub podmiotów, zobowiązany jest zapewnić poufność zebranych danych, ich merytoryczną poprawność, a także z zachowaniem przysługującego osobie, której dane dotyczą prawa do bycia odpowiednio poinformowanym.

2. Zasada legalności

Dla zapewnienia zgodności z prawem przetwarzania danych każdy pracownik lub współpracownik zobowiązany jest najpierw ustalić przesłankę legalizującą ich przetwarzanie: (1) zgodnie z art. 6 ust. 1 lit. a do lit. e RODO oraz (2) podaniem podstawy prawa krajowego. Uwaga - zgoda wyrażona na podstawie art. 6 ust. lit. a musi zostać udokumentowana

3. Rejestrowanie czynności przetwarzania / zasada przejrzystości

Administrator danych prowadzi **Rejestr czynności przetwarzania danych osobowych**, zawierający co najmniej:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
b) cele przetwarzania,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń,
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Rejestr jest prowadzony w wersji elektronicznej z zastrzeżeniem, że jest archiwizowany raz w roku wg stanu na 31 grudnia w celu przechowywania przez minimum 3 kolejne lata. Dopuszcza się archiwizowanie rejestru wydrukowanego lub skopiowanego na IND.

4. Rejestrowanie kategorii czynności przetwarzania

W przypadku przetwarzania danych osobowych pozyskanych na podstawie umowy powierzenia od innego administratora, ADO prowadzi **Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora**, zawierający co najmniej:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych,
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń,
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Rejestr jest prowadzony w wersji elektronicznej z zastrzeżeniem, że jest archiwizowany raz w roku wg stanu na 31 grudnia w celu przechowywania przez minimum 3 kolejne lata. Dopuszcza się archiwizowanie rejestru wydrukowanego lub skopiowanego na IND.

5. Warunki wyrażenia zgody

Jeżeli dane są przetwarzane na podstawie zgody osoby, której dane dotyczą należy udokumentować uzyskanie zgody na przetwarzanie danych osobowych poprzez uzyskanie pisemnego oświadczenia. Oświadczenie to w jasny, prosty i zrozumiały sposób przedstawia ten fakt, oraz precyzuje cel i czas, w jakich dane będą przetwarzane.
Uwaga - zgoda wyrażona na podstawie art. 6 ust. lit. a lub art. 9 ust. 2 lit. a musi zostać udokumentowana przed rozpoczęciem zbierania danych od osoby, której dane dotyczą, a najpóźniej w momencie rozpoczęcia ich pozyskiwania.

6. Warunki wycofania zgody

Osoba, która wyraziła zgodę może ją w dowolnym momencie wycofać. Wycofanie zgody musi zostać być udokumentowane. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

7. Przetwarzanie niewymagające identyfikacji

Jeżeli cele, w jakich administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, ADO nie ma obowiązku zachowania ani uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby której dane dotyczą wyłącznie po to by zastosować się do przepisów RODO,

8. Zasada ograniczenia czasu / Usunięcie danych

1. Usunięcie danych następuje przy spełnieniu przynajmniej jednego z poniższych warunków:
   a) po upływie określonego przepisami prawa okresu przechowywania,
   b) gdy cel, dla którego dane zebrano został osiągnięty lub dane są już zbędne dla osiągnięcia tego celu, a nie podlegają archiwizacji,
   c) w przypadku cofnięcia zgody przez osobę, której dane dotyczą, jeśli ich przechowywania nie nakazują przepisy prawa.
2. Każdy dokument papierowy zawierający dane osobowe sporządzony, jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć albo zabezpieczyć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.
3. Niszczenie błędnych lub zbędnych kopii dokumentów papierowych zawierających dane osobowe dokonuje się w przeznaczonych do tego celu niszczarkach dokumentów zgodnie z procedurą.
4. Zabronione jest wyrzucanie błędnych lub zbędnych kopii dokumentów papierowych zawierających dane osobowe bez uprzedniego dokonania ich zniszczenia w sposób wskazany w zdaniu powyżej, do koszy i śmietników komunalnych albo pozostawienia bez nadzoru materiałów przeznaczonych do zniszczenia.
5. Kopiowanie danych osobowych może odbywać się wyłącznie przez osobę w ramach posiadanego przez nią upoważnienia do przetwarzania danych, w związku z realizacją zadań zleconych jej przez ADO.
6. Dokumenty przeznaczone do zniszczenia należy przechowywać i chronić w sposób zapewniający należytą ochronę, a w szczególności zabezpieczyć przed nieuprawnionym dostępem, niekontrolowanym usunięciem (np. przez personel sprzątający lub techniczny).

9. Zasada ochrony danych w fazie projektowania

Administrator wprowadza zasady opisane w wewnętrznych politykach, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki polegają m.in. na:

- minimalizacji przetwarzania danych osobowych,
- jak najszybszej pseudonimizacji danych osobowych,
- przejrzystości co do funkcji i przetwarzania danych osobowych,
- umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych,
- umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

Osoba odpowiedzialna za prowadzenie projektu musi zapewnić właściwą ochronę danych m.in. poprzez konsultowanie danego projektu z IOD.
Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy brać pod uwagę w przetargach publicznych.

1. Administrator uwzględnia zasady ochrony danych podczas określania sposobów przetwarzania orz z w czasie jego trwania poprzez:
    a) minimalizację danych,
    b) stosowanie niezbędnych zabezpieczeń.
2. Administrator wdraża odpowiednie środki techniczne oraz organizacyjne, aby zapewnić przetwarzanie wyłącznie danych niezbędnych do osiągnięcia celu przetwarzania. Zapewnia to poprzez:
    a) właściwą ilość zbieranych danych,
    b) zakres przetwarzanych danych,
    c) okres przechowywania danych,
    d) właściwą dostępność danych.

ROZDZIAŁ V
UPOWAŻNIENIE I POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienie do przetwarzania danych

1. Do przetwarzania danych osobowych dopuszczeni mogą być wyłącznie pracownicy i współpracownicy, upoważnieni pisemnie przez ADO.
2. Nadanie uprawnień do pracy w systemach informatycznych służących do przetwarzania danych osobowych może nastąpić po uzyskaniu właściwego upoważnienia do przetwarzania danych osobowych.
3. Upoważnienia do przetwarzania danych osobowych są nadawane w zakresie niezbędnym do wykonywania przez osoby upoważniane pracy lub realizacji czynności zleconych. Zabronione jest nadawanie upoważnień w zakresie szerszym, niż wynikający z obowiązków służbowych osoby upoważnianej bądź czynności zleconych tej osobie.
4. Niedozwolone jest zlecanie nowo zatrudnionej osobie, wobec której złożono wniosek o nadanie upoważnienia do przetwarzania danych osobowych, pracy związanej z przetwarzaniem tych danych, przed otrzymaniem przez tę osobę stosownego upoważnienia.

2. Umowa powierzenia / przetwarzania w imieniu ADO

1. Do przetwarzania danych osobowych dopuszczone mogą być wyłącznie podmioty, z którymi zawarto umowę powierzenia danych.
2. W imieniu podmiotu przetwarzającego dostęp do danych mogą uzyskać wyłącznie osoby, z którym zawarł on stosowną umowę lub wydał upoważnienie do przetwarzania danych.
3. Przetwarzanie danych osobowych w imieniu Administratora może odbywać się wyłącznie na podstawie pisemnej umowy lub stosownej klauzuli powierzenia zawartej w umowie łączącej Administratora Danych Osobowych z tym podmiotem. Procesor może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w tej umowie.
4. LADO może konsultować z IOD projekty umów oraz czynności planowane w tym zakresie oraz wynikające z realizacji umowy.

3. Rodzaj przetwarzanych danych

Dane przetwarzane przez ADO w zależności od sposobu ich pozyskania dzielą się na dwie grupy:

- dane osobowe dotyczące własnej działalności,
- dane osobowe pozyskane od podmiotów, którym ADO świadczy usługę lub pozostaje z nimi we współpracy.

4. Nadanie / zmiana / cofanie upoważnień do przetwarzania danych osobowych

Za nadawanie, zmianę lub cofania uprawnień do przetwarzania danych odpowiada Administrator. LADO odpowiada za terminowe przygotowanie i przedstawienie wniosków w tej sprawie. Szczegółowe zasady postępowania reguluje odrębna procedura.

ROZDZIAŁ VI
ZASADY KORZYSTANIA Z URZĄDZEŃ I SYSTEMU INFORMATYCZNEGO

1. Zasady ogólne

1. ADO oraz wszyscy uprawnieni użytkownicy przetwarzający dane osobowe w systemie informatycznym stosowanym w Urzędzie Gminy są odpowiedzialni za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych.
2. Obowiązkiem ADO jest zapewnienie sił i środków do zabezpieczenia sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.
3. System przetwarzania danych w Urzędzie stanowią wszystkie działające serwery, komputery stacjonarne i przenośne oraz smartfony i tablety, a także urządzenia peryferyjne i sieciowe.
4. ADO może stosować narzędzia do monitorowania systemów informatycznych pod kątem funkcjonowania wdrożonych mechanizmów bezpieczeństwa, w tym także monitorowania czynności użytkowników.
5. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ASI do eksploatacji licencjonowane oprogramowanie, którego to ASI prowadzi ewidencję.
6. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   a) mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika,
   b) mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,
   c) mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   d) urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,
   e) mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,
   f) mechanizmy zarządzania zmianami.

2. Praca w systemie informatycznym

Użytkownicy systemów informatycznych, w których przetwarzane są dane osobowe, zobowiązani są do przestrzegania zasad określonych w polityce bezpieczeństwa i niniejszej instrukcji oraz innych postanowień zapewniających bezpieczeństwo przetwarzanych danych. Do przetwarzania danych osobowych w systemie informatycznym można wykorzystywać wyłącznie urządzeń służbowych Administratora. Jeżeli w trakcie pracy w systemie w pomieszczeniu znajdują się osoby postronne, należy upewnić się, że nie mają one możliwości wglądu do przetwarzanych danych.

Komputery muszą zostać skonfigurowane przez ASI zgodnie z procedurą przed oddaniem do użytkowania. Dostęp do systemu wymaga podania indywidualnego identyfikatora oraz hasła. ASI prowadzi rejestr identyfikatorów wszystkich użytkowników oraz komputerów, na których przetwarza się dane osobowe.

3. Rozpoczęcie, zawieszenia i zakończenie pracy.

Korzystając z systemu informatycznego do przetwarzania danych osobowych użytkownik jest zobowiązany do przestrzegania obowiązujących zasad i uregulowań.

1) tryb pracy na poszczególnych stacjach roboczych:

a) przed rozpoczęciem pracy użytkownik jest zobowiązany do sprawdzenia, czy zestaw komputerowy nie nosi śladów mogących świadczyć o włamaniu do systemu,

b) w przypadku stwierdzenia nieprawidłowości użytkownik zobowiązany jest do zabezpieczenia zestawu komputerowego i nośników przed nieuprawnionym dostępem oraz niezwłocznego poinformowania LADO o stwierdzonych nieprawidłowościach,

c) o wszelkich nieprawidłowościach LADO bezzwłocznie informuje ASI,

d) po uruchomieniu komputera użytkownik wprowadza swój login (identyfikator) i hasło,

e) zabrania się wykorzystywania konta innego użytkownika lub przydzielania jednego konta kilku osobom,

f) w systemach, w których administrator zbioru ustala inne zasady kontroli dostępu, np. poprzez zastosowanie indywidualnych kart i kodów PIN, obowiązują zasady łączne albo o wyższym poziomie zabezpieczeń,

g) w pomieszczeniu, w którym przetwarzane są dane osobowe, interesanci mogą przebywać pod nadzorem użytkownika,

h) przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach,

i) monitory komputerów chronione są włączającym się automatycznie wygaszaczem ekranu – wznowienie wyświetlenia następuje po wprowadzeniu hasła zalogowanego użytkownika (wymuszone przez system),

j) w przypadku konieczności krótkotrwałego opuszczenia stanowiska użytkownik obowiązany jest aktywować wygaszacz ekranu lub w inny sposób zablokować stację roboczą (kombinacja klawiszy: znak „Windows" oraz „L"),

k) zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary serwera (nie dotyczy komputerów, które nie mają dostępu do sieci lub przechowujących dane lokalnie), a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w listwie zasilającej, jeżeli komputer nie jest podłączony do sieci dedykowanej,

l) przed opuszczeniem pokoju należy:

- schować do zamykanych na klucz szaf przenośne nośniki informatyczne, dokumenty i wykonane wydruki zawierające dane osobowe oraz zniszczyć w niszczarce wydruki wstępne,
- schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe, umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,

- zamknąć okna, zamknąć pomieszczenie, aktywować system alarmowy (jeżeli istnieje),
- zdać klucze na przechowanie w miejscu określonym przez LADO;

2) tryb pracy na komputerach przenośnych:

a) zasadniczo zbiory danych osobowych przetwarzane są w komputerach stacjonarnych,

b) przetwarzanie danych osobowych przy wykorzystaniu komputerów przenośnych powinno być ograniczone do niezbędnych przypadków,

c) przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie na podstawie pisemnej zgody ADO (o uzyskaniu zgody LADO informuje ASI),

d) zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzanych danych LADO określa na piśmie,

e) komputery przenośne podlegają zabezpieczeniom o poziomie nie niższym, niż przewidzianym dla komputerów stacjonarnych,

f) cały dysk twardy komputera musi być zabezpieczony programem szyfrującym z AES-256,

g) zabronione jest wynoszenie komputera przenośnego z pomieszczenia służbowego głównego użytkownika, w którym nie zastosowano zasad kont i haseł opisanych w instrukcji zarządzania,

h) komputerów przenośnych nie wolno pozostawiać bez nadzoru,

i) nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach, innych miejscach publicznych i w samochodach,

j) informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu,

k) w uzasadnionych przypadkach wykorzystywanie komputerów przenośnych ADO w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione,

l) w domu osoby upoważnionej niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do ADO – użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym,

m) ASI, w razie potrzeby, wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:

- postępowania w razie nieobecności w pracy dłuższej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym LADO i uzgodnić z nim zwrot komputera przenośnego,
- zwrotu sprzętu w razie zakończenia pracy u ADO,

n) w zakresie nieuregulowanym w polityce bezpieczeństwa, do pracy z wykorzystaniem komputerów przenośnych, stosuje się postanowienia instrukcji zarządzania systemem informatycznym,

Użytkownikom zabrania się:

1) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody ADO,
2) udostępniania stanowisk roboczych osobom nieuprawnionym,
3) wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez ADO,
4) samowolnego instalowania i używania programów komputerowych,
5) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
6) umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym,
7) używania komputera bez zainstalowanego oprogramowania antywirusowego.

4. Zabezpieczenie danych

W celu właściwego zabezpieczenia przetwarzanych danych stosuje się:

1. Zabezpieczenia Fizyczne – mające na celu uniemożliwienie lub utrudnienie dostępu do chronionych obszarów,
2. Zabezpieczenia Techniczne – mające na celu zabezpieczenie sprzętu przed ingerencją, nieupoważnionym dostępem lub awarią zasilania,
3. Zabezpieczenia Organizacyjne – mające na celu wzrost świadomości użytkowników, w zakresie zachodzących procesów, ścieżek komunikacji oraz reagowania na zagrożenia.

Zabezpieczenie danych osobowych realizuje się dodatkowo poprzez:

a) Stosowanie indywidualnych kont użytkowników oraz właściwego dla nich systemu haseł,
b) Oprogramowanie Antywirusowe,
c) Legalność i aktualizację stosowanych programów i aplikacji,
d) Wykonywanie kopii zapasowych.

ROZDZIAŁ VII
SZKOLENIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

1. Zasady ogólne

W celu zapewnienia prawidłowego procesu wdrożenia oraz utrzymania standardów oraz wymagań w zakresie ochrony danych osobowych wprowadza się system szkoleń osób otrzymujących oraz mających. Szkolenie ma charakter seminarium / samokształcenia kierowanego zapoznającego z ogólnymi zasadami i regulacjami wewnętrznymi w tym zakresie.

LADO odpowiada za to, aby każdy podległy mu pracownik odbył szkolenie w tym zakresie.

2. Rodzaje szkoleń w zakresie ochrony danych

System szkoleń przewiduje:

- szkolenie podstawowe / okresowe,
- szkolenia uzupełniające / doraźne,
- samokształcenie.

Szczegółowe regulacje, program oraz wzory upoważnień w tym zakresie określa **Polityka szkoleń**.

ROZDZIAŁ IX
ZARZĄDZANIE RYZKIEM

1. Zasady ogólne

Zarządzanie Ryzykiem związane z przetwarzaniem informacji jest kluczowym elementem procesu bezpieczeństwa, determinującym i uzasadniającym działania podejmowane w celu jego obniżenia do poziomu akceptowalnego.

Dla wszystkich zidentyfikowanych procesów przetwarzania danych przeprowadzono Ocenę Ryzyka a także wdrożono w ramach Planu Postępowania z Ryzykiem odpowiednie środki zabezpieczające. Dodatkowo, w ramach procesu Zarządzania Ryzykiem został opracowany Plan Monitorowania i Przeglądu Ryzyka.

2. Ocena Ryzyka w zakresie Ochrony Danych Osobowych

Istotnym elementem procesu Zarządzania Ryzykiem jest Ocena Ryzyka dla zidentyfikowanych procesie inwentaryzacji aktywów w procesach przetwarzania. Za identyfikację ryzyk i odpowiednie postępowanie z nimi odpowiada LADO, który jest właścicielem zasobu, w którym zidentyfikowano ryzyko.

Jeśli przeprowadzona ocena ryzyka wskaże, że przetwarzanie danych powodowałoby wysokie ryzyko mino zastosowanych środków do jego minimalizacji to przed rozpoczęciem ich przetwarzania ADO konsultuje się z organem nadzorczym.

3. Plan Postępowania z Ryzykiem

Z procesu Oceny Ryzyka wynika Plan Postępowania z Ryzkiem obejmujący swoim zakresem:

a) monitorowanie ryzyka dla ryzyk zidentyfikowanych w procesie Oceny Ryzyka jako akceptowalne lecz wymagające monitorowania,
b) wdrażanie zabezpieczeń i podejmowanie środków zaradczych dla ryzyk zidentyfikowanych jako nieakceptowalne w procesie Oceny Ryzyka,
c) ocenę ryzyka szczątkowego po wdrożeniu działań zaradczych i zabezpieczeń,

4. Monitorowanie i Przegląd Ryzyka

Monitorowanie i Przegląd Ryzyka w ochronie danych osobowych jest realizowane na bieżąco w całym procesie Zarządzania Ryzykiem.

Dodatkowo, co najmniej raz do roku lub w przypadku modyfikacji kontekstu przetwarzania danych prowadzona jest weryfikacja:

a) kompletności inwentaryzacji procesów przetwarzania danych,

b) aktualności stosowanej technologii lub rozwiązań biznesowych dla procesów przetwarzania,
c) odpowiedniej wraz z upływem czasu skuteczności stosowanych zabezpieczeniach w procesach przetwarzania danych,

Wyniki procesu Monitorowania i Przeglądu Ryzyka podlegają dokumentowaniu w postaci protokołów z przeprowadzonych działań.

ROZDZIAŁ X
DOKUMENTACJA DOTYCZĄCA NARUSZEŃ

1. Określenie incydentu

Incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia procesu przetwarzania danych osobowych, mogących skutkować naruszeniem bezpieczeństwa danych.
W ochronie danych osobowych można wyróżnić trzy zasadnicze grupy incydentów:

1) umyślne incydenty (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
2) zdarzenia losowe wewnętrzne (np. awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych),
3) zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata zasilania, utrata łączności).

Osoba, która zidentyfikowała incydent albo ma uzasadnione podejrzenie jego wystąpienia niezwłocznie informuje o tym LADO i ASI.

2. Zgłaszanie naruszenia ochrony danych

Za naruszenie należy uznać każde poważne zdarzenie dot. ochrony danych mogące skutkować utratą podstawowych atrybutów, tj. poufności, integralności lub dostępności.

1. W przypadku naruszenia ochrony danych osobowych ADO bez zbędnej zwłoki – w miarę możliwości ale nie później niż w terminie 72 h od stwierdzenia naruszenia zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, że naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Do zgłoszenia po upływie 72 h dołącza się wyjaśnienie przyczyn opóźnienia.
3. Podmiot przetwarzający dane (w imieniu) ADO po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je ADO.
4. Zgłoszenie naruszenia ochrony danych osób, zawiera:
   a) Opis charakteru naruszenia, wskazuje kategorię oraz liczbę osób których dane dotyczą, oraz kategorię oraz liczbę wpisów danych osobowych których dotyczy naruszenie,
   b) Imię i nazwisko oraz dane kontaktowe IOD,
   c) Opis możliwych konsekwencji naruszenia ochrony danych,
   d) Opis środków zastosowanych oraz proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych w tym w stosowanych przypadkach środki zastosowania w celu zminimalizowania jego ewentualnych negatywnych środków,
5. Jeżeli powyższych informacji zawartych w pkt 4. lit. a – d nie da się udzielić od razu, należy je udzielać sukcesywnie bez zbędnej zwłoki.

6. ADO dokumentuje wszelkie naruszenia ochrony danych w tym okoliczności naruszenia, jego skutki oraz podjęte w związku z nim działania. Dokumentacja musi pozwalać organowi nadzorczemu na weryfikację przestrzegania art. 33 RODO.

3. Zawiadamianie osoby, której dane dotyczą

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, administrator bez zbędnej zwłoki ma obowiązek zawiadomić taką osobę.
2. Zgłoszenie naruszenia ochrony danych osoby, której dane dotyczą, zawiera:
   a) Imię i nazwisko oraz dane kontaktowe IOD,
   b) Opis możliwych konsekwencji naruszenia ochrony danych,
   c) Opis środków zastosowanych oraz proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych w tym w stosowanych przypadkach środki zastosowania w celu zminimalizowania jego ewentualnych negatywnych środków.
3. Zawiadomienie nie jest konieczne, jeśli:
   a) administrator wdrożył odpowiednie środki techniczne lub organizacyjne uniemożliwiające odczyt osobom nieuprawnionym, np. szyfrowanie,
   b) zastosował następnie po naruszeniu środki eliminujące prawdopodobieństwo wysokiego ryzyka,
   c) wymagałoby niewspółmiernie dużego wysiłku – w tym przypadku ADO wydaje publiczny komunikat lub stosuje inny podobny środek, za pomocą którego informuje w równie skuteczny sposób.

4. Rejestr Incydentów

Za prowadzenie ewidencji incydentów i naruszeń odpowiada ASI.
Rejestr jest prowadzony w wersji elektronicznej z zastrzeżeniem, że jest archiwizowany raz w roku wg stanu na 31 grudnia w celu przechowywania przez minimum 3 kolejne lata. Dopuszcza się archiwizowanie rejestru wydrukowanego lub skopiowanego na IND.

ROZDZIAŁ XI
REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Zasady Ogólne

1. Administrator danych osobowych podejmuje niezbędne środki w celu zapewnienia właściwej informacji o podjętych działaniach w stosunku do osób, których dane dotyczą:
   a) udziela informacji o dostępie do danych osobowych poprzez:
      - podanie swoich danych kontaktowych oraz swojego przedstawiciela,
      - podstawę prawną przetwarzania danych osobowych,
   b) uzasadnienie interesu przetwarzania danych (jeśli odbywa się ono zgodnie z art. 6 ust. 1 lit. f),
   c) informacje o odbiorcach lub ich grupach, jeśli istnieją,
   d) informację o zamiarze przekazywania do państw trzecich lub organizacji międzynarodowych,
   e) stwierdzenie lub brak stwierdzenie odpowiedniego stopnia zabezpieczeń przez komisję oraz odpowiednich lub właściwych zabezpieczeniach,
   f) informacje o możliwości uzyskania kopii danych oraz miejscu ich udostępniania.

2. Podczas procesu pozyskiwania danych ADO podaje osobie, której dane dotyczą podstawowe informacje:
   a) pełną nazwę, dane kontaktowe (adres, email, nr telefonu),
   b) dane kontaktowe IOD (email, nr telefonu),
   c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania,
   d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   e) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
   f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   g) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   h) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   i) informacje o prawie wniesienia skargi do organu nadzorczego,
   j) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   k) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

ROZDZIAŁ XII
UDOSTĘPNIANIE DANYCH INNY PODMIOTOM / PRZEKAZYWANIE DO PAŃSTW TRZECICH

1. Zasady Ogólne

1. Dane osobowe mogą być udostępnione podmiotom lub osobom uprawnionym do ich żądania na podstawie powszechnie obowiązujących przepisów prawa (np. organy ścigania).
2. Udostępnienie danych osobowych podmiotom innym niż uprawnione na podstawie przepisów prawa, może nastąpić wyłącznie za wiedzą bezpośredniego Przełożonego pracownika bądź współpracownika, do którego wniosek o udostępnienie został skierowany bądź, w którego obszarze kompetencji ma dojść do udostępnienia danych.
3. Administrator wydaje zgodę na udostępnienie danych akceptując w tym celu dane/dokumenty, przygotowane przez właściwego LADO.
4. Przed udostępnieniem danych, o którym mowa w pkt. 1 powyżej, należy zweryfikować czy podmiot występujący o udzielenie informacji jest uprawniony do ich otrzymania (np. czy dysponuje odpowiednią podstawą prawną do otrzymania danych). W przypadku zaistnienia wątpliwości dot. udostępnienia danych LADO konsultuje się z IOD.
5. Zabronione jest **udostępnianie danych osobowych przez telefon** w sytuacji, w której nie da się zidentyfikować rozmówcy. Udzielanie informacji przez telefon jest dopuszczalne na podstawie pisemnej zgody udzielonej przez osobę, której dane dotyczą. Warunkiem udzielenia informacji przez telefon jest identyfikacja numeru dzwoniącego w aparacie telefonicznym pracownika Urzędu.
6. Dopuszcza się złożenie wniosku o udostępnienie danych osobowych w formie wiadomości e-mail podpisanej kwalifikowanym podpisem elektronicznym zgodnie z ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r., poz. 1579) lub poprzez Profil Zaufany platformy ePUAP.
7. ADO wyznacza pracownika do prowadzenia rejestru udostępnień, zawierający:
   a) datę dokonania udostępnienia danych,
   b) podstawy prawnej,
   c) oznaczenie podmiotu, któremu udostępniono dane,
   d) zakres danych, które udostępniono, w tym wskazanie osoby, której dane dotyczą, oraz wskazanie pracownika/współpracownika dokonującego udostępnienia.

ROZDZIAŁ XIII
POSTANOWIENIA KOŃCOWE

Nieprzestrzeganie zasad ochrony danych osobowych grozi m.in. odpowiedzialnością karną wynikającą z art. 107 i 108 UODO oraz wynikającą z art. 100 Kodeksu Pracy.

WÓJT GMINY DĄBROWA

Marcin Banczykowski

.....