ZARZĄDZENIE Nr RO.SO.0050.17.2022
Burmistrza Dobrej
z dnia 17 lutego 2022 roku

w sprawie wprowadzenia w Urzędzie Miejskim w Dobrej - Polityki bezpieczeństwa przetwarzania danych osobowych dla projektów : „DOBRA EDUKACJA. Kompleksowy program wsparcia 2 Szkół Podstawowych w Gminie Dobra.", „Przebudowa drogi gminnej Długa Wieś", „Uporządkowanie gospodarki wodno – ściekowej w miejscowości Skęczniew", „Wdrażanie usług transportowych door to door dla osób z potrzebą wsparcia w zakresie mobilności", „Stawiamy na dobry start"

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE tzw. RODO zarządza się, co następuje:

§ 1

Wprowadzam i wdrażam do stosowania w Urzędzie Miejskim w Dobrej - Polityki bezpieczeństwa przetwarzania danych osobowych dla projektów : „DOBRA EDUKACJA. Kompleksowy program wsparcia 2 Szkół Podstawowych w Gminie Dobra.", „Przebudowa drogi gminnej Długa Wieś", „Uporządkowanie gospodarki wodno – ściekowej w miejscowości Skęczniew", „Wdrażanie usług transportowych door to door dla osób z potrzebą wsparcia w zakresie mobilności", „Stawiamy na dobry start", stanowiącą załącznik do niniejszego zarządzenia

§ 2

Wszystkie osoby, które zostały dopuszczone do przetwarzania danych osobowych powinny zostać zapoznane z wyżej wskazaną dokumentacją.

§ 3

Wykonanie zarządzenia powierza się Inspektorowi ochrony danych osobowych Urzędu Miejskiego w Dobrej.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik do Zarządzenia Nr RO.SO.0050.17.2022
Burmistrza Dobrej z dnia 17 lutego 2022 roku
w sprawie wprowadzenia w Urzędzie Miejskim w Dobrej Polityki bezpieczeństwa" przetwarzania danych osobowych dla projektów : „DOBRA EDUKACJA. Kompleksowy program wsparcia 2 Szkół Podstawowych w Gminie Dobra.", „Przebudowa drogi gminnej Długa Wieś", „Uporządkowanie gospodarki wodno – ściekowej w miejscowości Skęczniew", „Wdrażanie usług transportowych door to door dla osób z potrzebą wsparcia w zakresie mobilności", „Stawiamy na dobry start"

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH DLA PROJEKTÓW:

„DOBRA EDUKACJA. Kompleksowy program wsparcia 2 Szkół Podstawowych w Gminie Dobra."
„Przebudowa drogi gminnej Długa Wieś"
„Uporządkowanie gospodarki wodno – ściekowej w miejscowości Skęczniew"
„Wdrażanie usług transportowych door to door dla osób z potrzebą wsparcia w zakresie mobilności"
„Stawiamy na dobry start"

Rozdział 1
Postanowienia ogólne

§ 1

Polityka Bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Dobrej określa zasady i tryb postępowania przy przetwarzaniu danych osobowych podczas realizacji w/w projektu.

§ 2

Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 10 maja 2018 r. (t.j. Dz. U. z 2019 r. poz. 1781) o ochronie danych osobowych dotyczącymi zasad przetwarzania danych, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych).

§ 3

Celem Polityki Bezpieczeństwa jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Urzędzie Miejskim w Dobrej informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych przy realizacji projektów, przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 4

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 5

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w projektach, rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. 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

Administratorem Danych Osobowych przetwarzanych w projektach jest Urząd Miejski w Dobrej.

Rozdział 2
Definicje

§ 7

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miejskim w Dobrej w związku z realizacją projektów. **Administrator Danych Osobowych** – *dalej jako* Administrator Danych; rozumie się przez to Urząd Miejski w Dobrej.
2) **Inspektor Ochrony Danych** - rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych określonych w RODO i przepisach krajowych;
3) **Biuro** – Biuro Projektu;
4) **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);
5) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
6) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7) **Zbiór danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
8) **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
9) **Usuwanie danych osobowych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
10) **Przetwarzanie danych osobowych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu a zwłaszcza tych, które wykonuje się w systemach informatycznych;
11) **System informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
12) **Metoda tradycyjna** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
13) **Beneficjent** – rozumie się przez to Gmina Dobra ;

14) **Projekt** – rozumie się przez to realizowane projekty/umowy;
15) **Użytkownik** - rozumie się przez to upoważnionego przez Administratora Danych Osobowych lub Inspektora Ochrony Danych, wyznaczonego do przetwarzania danych osobowych pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych.

Rozdział 3
Zakres oraz zasady zabezpieczania danych osobowych

§ 8

1. Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni Administrator Danych.
2. Nadzór nad poprawnością realizacji przepisów o ochronie danych osobowych, w szczególności zasad opisanych w Polityce, oraz nad wykonywaniem zadań związanych z ochroną danych osobowych w projektach u Beneficjenta sprawuje Inspektor Ochrony Danych.

§ 9

Przetwarzanie danych osobowych w projekcie jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielenia wsparcia, realizacji projektu, ewaluacji, monitoringu, sprawozdawczości i kontroli, w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2014-2020.

§ 10

Przetwarzanie danych osobowych w projekcie nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych 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.

§ 11

W przypadku zbierania jakichkolwiek danych osobowych na potrzeby projektu bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do przekazania tej osobie informacji o:
1) celu zbierania danych osobowych;
2) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
3) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie realizowanym w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2014-2020.

§ 12

1. Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.
2. Przetwarzanie danych osobowych znajdujących się w projekcie może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 9, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia oraz umowy o dofinansowanie projektu.

Rozdział 4
Przetwarzanie danych osobowych

§ 13

1. Do przetwarzania danych osobowych w projekcie mogą być dopuszczone jedynie osoby posiadające odpowiednie upoważnienie wydane przez Administratora Danych. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach do umowy o dofinansowanie projektu i stanowią załącznik nr 1 i 2 do niniejszej Polityki Bezpieczeństwa.
2. Każda osoba, przed dopuszczeniem jej do przetwarzania danych osobowych w projekcie, musi być zapoznana z przepisami dotyczącymi ochrony danych osobowych oraz Polityką bezpieczeństwa przetwarzania danych osobowych.
3. Każda osoba mająca dostęp do danych osobowych w projekcie jest wpisywana do rejestru osób upoważnionych do przetwarzania danych osobowych (załącznik nr 3).
4. Wszystkie osoby, które zostały dopuszczone do przetwarzania danych osobowych w projekcie u Beneficjenta, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania w tajemnicy przetwarzane dane osobowe. Obowiązek zachowania w tajemnicy istnieje również po ustaniu zatrudnienia jak również po zakończeniu projektu.

§ 14

Użytkownicy są w szczególności zobowiązani do:

1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w projekcie;
2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych;
4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
5) nieudzielania informacji o danych osobowych przetwarzanych w projekcie innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
6) bezzwłocznego zawiadamiania Inspektora Ochrony Danych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§ 15

Dane osobowe w projekcie gromadzone są i przetwarzane z użyciem sprzętu komputerowego oraz systemu tradycyjnego w pomieszczeniach wskazanych w załączniku nr 6 do Polityki Bezpieczeństwa.

§ 16

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych są określone w załączniku nr 7 do Polityki Bezpieczeństwa.

Rozdział 5
Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 17

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

1) stwierdzono naruszenie zabezpieczenia danych osobowych w projekcie;
2) stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych;
3) inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w projekcie.

§ 18

Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w projekcie, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Inspektora Ochrony Danych u Beneficjenta.

§ 19

1. Po przywróceniu normalnego stanu należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
2. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych w projekcie.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań Beneficjenta.

Rozdział 6
Postanowienia końcowe

§ 20

Polityka jest dokumentem wewnętrznym Beneficjenta i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 21

Do spraw nieuregulowanych w Polityce Bezpieczeństwa stosuje się przepisy o ochronie danych osobowych.

§ 22

Polityka Bezpieczeństwa nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia danych.

§ 23

Integralną część niniejszej Polityki Bezpieczeństwa stanowią następujące załączniki:

1) Załącznik nr 1 – wzór upoważnienia do przetwarzania danych osobowych w projektach.
2) Załącznik nr 2 – wzór odwołania upoważnienia do przetwarzania danych osobowych.
3) Załącznik nr 3 – Rejestr osób upoważnionych do przetwarzania danych osobowych.
4) Załącznik nr 4 - Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym są przetwarzane dane osobowe;
5) Załącznik nr 5 – Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych;
6) Załącznik nr 6 – Arkusz analizy ryzyka;
7) Załącznik nr 7 – Plan postępowania z ryzykiem.

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik nr 1
do Polityki Bezpieczeństwa przetwarzania danych osobowych

Dobra, dnia .....

U P O W A Ż N I E N I E n r.....

do przetwarzania danych osobowych

Z dniem .....2021 r. na podstawie art. 29 w związku z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 04.05.2016, str. 1) (RODO), upoważniam Panią/Pana* ..... do przetwarzania danych osobowych w zbiorze „Program Operacyjny Wiedza Edukacja Rozwój", w zakresie ..... .

Upoważnienie wygasa z chwilą ustania Pana/Pani* stosunku prawnego z Centrum Doskonalenia Nauczycieli w Koninie lub z chwilą jego odwołania/anulowania*.

.....

Czytelny podpis osoby upoważnionej
do wydawania i odwoływania
upoważnień

Upoważnienie otrzymałem/am*:

.....

Oświadczam, że zapoznałem/am* się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także z obowiązującym w Centrum Doskonalenia Nauczycieli w Koninie opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.
Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi się zapoznałem/am*, oraz sposobów ich zabezpieczania zarówno w okresie trwania umowy, jak również po ustaniu stosunku prawnego łączącego mnie z Centrum Doskonalenia Nauczycieli w Koninie.

.....
Data i czytelny podpis osoby składającej
oświadczenie
*niepotrzebne skreślić

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik nr 2
do Polityki Bezpieczeństwa przetwarzania danych osobowych

ODWOŁANIE UPOWAŻNIENIA Nr _____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ..... r., na podstawie art. 29 w związku z art. 28 Rozporządzenia 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. Urz. UE L 119 z 04.05.2016, str. 1) (RODO) –odwołuję upoważnienie Pana/Pani .....do przetwarzania danych osobowych nr ..... wydane w dniu .....

.....
Czytelny podpis osoby, upoważnionej do wydawania i odwoływania upoważnień

.....
(miejscowość, data)

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik nr 3
do Polityki Bezpieczeństwa przetwarzania danych osobowych

Rejestr osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Data zapoznania z dokumentem	Stanowisko/funkcja	Typ umowy/porozumienia			Zakres rzeczowy uprawnienia	Ramy czasowe	
				Pracownik	Współpracownik	Praktyka/Staż		od ...[1]	do ...[2]
1									
2									
3									
4									
5									

BURMISTRZ
DĘBNEJ
Tadeusz Gebler

Załącznik nr 4
do Polityki Bezpieczeństwa przetwarzania danych osobowych

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

Lp.	Budynek – dane adresowe	Pomieszczenie
	PARTER	
1		
2		

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik nr 5
do Polityki Bezpieczeństwa przetwarzania danych osobowych

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych.

I. Środki ochrony fizycznej danych:

a) klucze do pomieszczeń wydawane są wyłącznie osobom upoważnionym,

b) podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,

c) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

d) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych,

e) zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie,

f) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie,

g) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

a) sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby beneficjenta;

b) oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie;

c) dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

d) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

e) zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

III. **Środki organizacyjne:**

a) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;

b) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy;

c) monitory komputerów, na których są przetwarzane dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

d) kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe są przetwarzane na bieżąco.

BURMISTRZ
DOBREJ
Tadeusz Gebler

Załącznik nr 6
do Polityki Bezpieczeństwa przetwarzania danych osobowych

Arkusz analizy ryzyka

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie
nieuprawnione ujawnienie	1. Ujawnienie lub udostępnienie tych danych odbiorcom, którzy nie posiadają uprawnień do ich otrzymania lub uzyskania do nich dostępu. 2. Nieuprawnione przetwarzania, które narusza przepisy.	1	3	3	1. Okresowe szkolenia z zakresu ochrony danych osobowych.
nieuprawniony dostęp do danych podczas przesyłania	1. Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, tj. drogą e-mailową lub za pomocą komunikatora internetowego (*phishing*). 2. Wysłanie danych osobowych do niewłaściwego odbiorcy. 3. Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń.	2	1	2	1. Okresowe szkolenia z zakresu ochrony danych osobowych. 2. Stosowany system antywirusowy. 3. Stosowane silne hasła uwierzytelniające. 4. Stosowane oprogramowanie antyspamowe, firewall. 5. Stała aktualizacja oprogramowania.
nieuprawniony dostęp do danych podczas przechowywania	1. Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń. 2. Przechowywanie dokumentacji papierowej bez zabezpieczenia. 3. Umożliwianie dostępu do pomieszczeń i znajdującego się w nich sprzętu (komputery) osobom nieuprawnionym lub nieznanym.	2	1	2	1. Okresowe szkolenia z zakresu ochrony danych osobowych. 2. Stosowany system antywirusowy. 3. Stosowane silne hasła uwierzytelniające. 4. Stosowane oprogramowanie antyspamowe, firewall. 5. Stała aktualizacja oprogramowania.
przypadkowe lub niezgodne z prawem zniszczenie, uszkodzenie	1. Niszczenie dokumentów bez użycia niszczarki. 2. Awaria sprzętu komputerowego.	1	1	1	1. Okresowe szkolenia z zakresu ochrony danych osobowych.
przypadkowe lub niezgodne z prawem utracenie	1. Podmiot przetwarzający utracił kontrolę nad danymi lub dostęp do nich, lub nie jest już w ich posiadaniu. 2. Zagubienie dokumentacji papierowej. 3. Kradzież nośnika na którym przechowywane są dane.	2	1	2	1. Okresowe szkolenia z zakresu ochrony danych osobowych.
przypadkowe lub niezgodne z prawem zmodyfikowanie	1. Dokonanie zmiany przez pracownika treści informacji, które są zawarte w danych, w konsekwencji czego stają się niekompletne, częściowo nieczytelne lub nieprawidłowe.	1	1	1	1. Okresowe szkolenia z zakresu ochrony danych osobowych.

BURMISTRZ
DĄBRÓWKI
Tadeusz Gebler

Załącznik nr 7
do Polityki Bezpieczeństwa przetwarzania danych osobowych

	Plan postępowania z ryzykiem		
Lp.	**Zagrożenie (ryzyko do obniżenia)**	**Zabezpieczenie do wdrożenia**	**Osoba odpowiedzialna**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

BURMISTRZ
NOWEJ
Tadeusz Gebler