Zasadność Powołania Inspektora Ochrony Danych IOD (DPO)
WRAZ Z METODYKĄ AUDYTU WEWNĘTRZNEGO

Administrator Danych Osobowych (ADO): *GMINA NADARZYN*

o numerze NIP: *534-22-54-841*

oraz numerze REGON *013269195*

w osobie: *Dariusz Zwoliński*

dnia: *07 maja 2018 r.*

zgodnie z :

- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
- wytycznymi Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych:
    - WP 243 - Wytyczne dotyczące inspektorów ochrony danych osobowych („DPO") z dnia 13 grudnia 2016,
    - WP 248 - Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 z dnia 4 kwietnia 2017.
- międzynarodowymi normami ISO:
    - Norma PN-ISO/IEC 27001:2014-12 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji - Wymagania),
    - Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-ISO/IEC 27001:2014-12),
    - Norma PN-EN ISO 19011:2012 (Wytyczne dotyczące audytowania systemów zarządzania)

wdraża dokument o nazwie „**Zasadność powołania IOD (DPO) wraz z metodyką audytu wewnętrznego**". Zapisy tego dokumentu wchodzą w życie z dniem **25 maja 2018 r.**

§ 1

Zasadność powołania DPO wraz z metodyką audytu wewnętrznego określa konieczność powołania DPO uwzględniając czynniki techniczne i organizacyjne jednostki. Przedstawia metodę audytu wewnętrznego kluczowych obszarów przetwarzania na zgodność z SZBI będącym elementem wytycznych Grupy Roboczej Art. 29 do RODO oraz Norm ISO dookreślających procesy przetwarzania danych.

§ 2

Ilekroć w „**Zasadności powołania IOD (DPO) wraz z metodyką audytu wewnętrznego** " jest mowa o:

1. **ADMINISTRATORZE DANYCH OSOBOWYCH (ADO)** – rozumie się przez to Administratora Danych Osobowych podmiotu reprezentowanego przez osobę kierującą,
2. **ADMINISTRATORZE BEZPIECZEŃSTWA INFORMACJI (ABI)** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Bezpieczeństwa Informacji,
3. **ADMINISTRATORZE SYSTEMU INFORMATYCZNEGO (ASI)** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora Systemu Informatycznego,
4. **INSPEKTORZE OCHRONY DANYCH OSOBOWYCH IOD (DPO)** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Inspektora Ochrony Danych Osobowych w oparciu o Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016,
5. **DPO** – (ang. Data Protection Officer) - patrz § 2 pkt 4,
6. **RODO** – Rozporządzenie o Ochronie Danych Osobowych (ang. GDPR - General Data Protection Regulation) – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
7. **MOTYWIE** – rozumie się przez to preambułę do Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
8. **SZBI** – rozumie się przez to System Zarządzania Bezpieczeństwem Informacji (część całościowego systemu zarządzania organizacją, oparta na podejściu procesowym wynikającym z ryzyka), odnoszącym się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.
9. **ISO** – (ang. International Organization for Standardization) – rozumie się przez to Międzynarodową Organizację Normalizacyjną,
10. **CYKLU DEMINGA** - (określany też jako cykl PDCA z ang. Plan-Do-Check-Act lub cykl P-D-S-A z ang. Plan-Do-Study-Act lub koło Deminga) – rozumie się przez to schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia),
11. **GRUPIE ROBOCZEJ ART. 29** – rozumie się przez to Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych powołaną na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995r.,
12. **USTAWIE** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922),

§ 3

Zgodnie z zaleceniami Grupy Roboczej Art. 29, Administrator Danych Osobowych przeprowadził analizę pod kątem zasadności powołania Inspektora Ochrony Danych Osobowych (DPO) [1].

[1] Zgodnie z Ustawą o Ochronie Danych Osobowych z dnia 29 sierpnia 1997 (tekst jednolity: Dz. U. 2016r. poz. 922) oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016, Administrator Bezpieczeństwa Informacji (ABI) przyjmie nazwę „Inspektor Ochrony Danych Osobowych" (ang. „DPO") z dniem 25 maja 2018r.

Analiza zasadności powołania IOD (DPO) wraz z metodyką audytu wewnętrznego ma na celu „udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia obowiązku bądź braku obowiązku wyznaczenia IOD (DPO), celem wykazania, iż stosowne czynniki zostały uwzględnione" [2].

Zgodnie z RODO art. 24 ust. 1 czynnikami tymi są:

- czynniki techniczne,
- czynniki organizacyjne,

uwzględniając:

- charakter *(wg ISO/IEC 27001:2014-12, pkt 4.1)*
- zakres *(wg ISO/IEC 27005:2014-01, pkt 7.3)*
- kontekst *(wg ISO/IEC 27005:2014-01, pkt 3.4; 3.5)*
- cele przetwarzania *(wg ISO/IEC 27001:2014-01, pkt 5.1)*
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia *(wg ISO/IEC 27005:2014-01, pkt 8; 9)*

Analiza czynników z uwzględnieniem ich charakteru opiera się na międzynarodowych Normach ISO/IEC 27001:2014-12, ISO/IEC 27005:2014-01 oraz PN-EN ISO 19011:2012 w oparciu o wytyczne Grupy Roboczej Art. 29 - WP 248 pkt 2 [3].

§ 4

Niniejszy dokument o nazwie: „Zasadność powołania IOD (DPO) wraz z metodyką audytu wewnętrznego" zawiera 4 załączniki:

1. zasadność powołania DPO – **załącznik nr 1**,
2. metodyka audytu wewnętrznego – **załącznik nr 2**,
   a) plan audytu – **załącznik nr 2a**,
   b) karta(y) audytu – **załącznik nr 2b**.

oraz określa zasadność i metodykę powołania funkcji IOD/ DPO (Inspektora Ochrony Danych Osobowych).

WÓJT GMINY
Dariusz Zwoliński

.....
(pieczęć i podpis Administratora Danych Osobowych)

[2] Wytyczne Grupy Roboczej Art. 29 – WP 243 z dnia 13 grudnia 2016r.
[3] Grupa Robocza Art. 29 - WP 248: „Zakres wytycznych: ...międzynarodowe standardy")

ZASADNOŚĆ POWOŁANIA DPO

§ 1

TERMINOLOGIA

Określając zasadność powołania DPO wymagane jest sprecyzowanie, oraz wzięcie pod uwagę następujących terminów:

- główna działalność Administratora Danych Osobowych – określona w § 2,
- duża skala przetwarzania – określona w § 3,
- regularne i systematyczne monitorowanie osób, których dane dotyczą – określone w § 4.

§ 2

GŁÓWNA DZIAŁALNOŚĆ ADMINISTRATORA DANYCH OSOBOWYCH

Artykuł 37 ust. 1.b i c RODO zawiera zwrot „główna działalność administratora lub podmiotu przetwarzającego". Zgodnie z motywem 97 RODO przetwarzanie danych osobowych jest główną działalnością Administratora Danych Osobowych, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Tak więc „główną działalnością" będzie działalność kluczowa z punktu widzenia osiągnięcia celów Administratora Danych Osobowych albo podmiotu przetwarzającego dane.

„Głównej działalności" nie należy interpretować w sposób wyłączający działalność w zakresie przetwarzania danych nierozerwalnie związaną z działalnością główną. Dla przykładu działalnością główną szpitali będzie zapewnianie opieki medycznej. Natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna. Oznacza to, że szpitale będą miały obowiązek powołania DPO.

Kolejnym przykładem może być spółka świadcząca usługi ochrony mienia, prowadząca monitoring w szeregu prywatnych centrów handlowych i przestrzeni publicznej. Jej działalnością główną jest ochrona, natomiast związane z tym bezpośrednio jest przetwarzanie danych osobowych, co oznacza, że takie spółki również muszą powołać DPO.

§ 3

DUŻA SKALA PRZETWARZANIA

Czynniki uwzględniane przy określaniu, czy przetwarzanie następuje na „dużą skalę":

- liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa,
- zakres przetwarzanych danych osobowych,
- okres, przez jaki dane są przetwarzane,
- zakres geograficzny przetwarzania danych osobowych.

Do przykładów „przetwarzania na dużą skalę" zaliczyć można:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności,
- przetwarzanie danych osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem „kart miejskich"),
- przetwarzanie danych geo-lokalizacyjnych w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych,
- przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności,
- przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki,
- przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

§ 4

REGULARNE I SYSTEMATYCZNE MONITOROWANIE OSÓB, KTÓRYCH DANE DOTYCZĄ

Regularne i systematyczne monitorowanie osób, których dane dotyczą to:

- regularne i systematyczne monitorowanie fizyczne,
- regularne i systematyczne śledzenie i profilowanie w sieci, w tym na potrzeby reklam behawioralnych, tj. obserwacja osób w internecie w tym także późniejsze potencjalnie stosowane techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.

UWAGI:

Definicja „regularne" jako jedno lub więcej z następujących pojęć:

- stałe albo występujące w określonych odstępach czasu przez ustalony okres,
- cykliczne albo powtarzające się w określonym terminie,
- odbywające się stale lub okresowo.

Definicja „systematyczne" jako jedno lub więcej z następujących pojęć:

- występujące zgodnie z określonym systemem,
- zaaranżowane, zorganizowane lub metodyczne,
- odbywające się w ramach generalnego planu zbierania danych,
- przeprowadzone w ramach określonej strategii.

PRZYKŁADY:

obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie e-mail; profilowanie i ocenianie dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy); śledzenie lokalizacji, na przykład w aplikacjach telefonicznych; programy lojalnościowe; reklama behawioralna; monitorowanie danych o stanie zdrowia za pośrednictwem urządzeń przenośnych; monitoring wizyjny; urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa, etc.

§ 5

ANALIZA ZASADNOŚCI POWOŁANIA DPO

Artykuł 37 ust. 1 RODO wskazuje na obowiązek wyznaczenia DPO w przypadkach przedstawionych w poniższej tabeli. Zgodnie z RODO i wytycznymi Grupy Roboczej Art. 29 w sprawie wyznaczenia DPO wystąpienie choćby jednej przesłanki wymienionej w przedstawionych zakresach przetwarzania obliguje placówkę do wyznaczenia DPO.

LP	ZAKRES PRZETWARZANIA	TAK / NIE
1	Przetwarzania dokonuje organ lub podmiot publiczny za wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.	TAK
2	Przetwarzania dokonuje „organ sektora publicznego" oznaczający państwowe, regionalne lub lokalne władze, podmioty prawa publicznego oraz stowarzyszenia utworzone przez jedną lub kilka takich władz albo jeden lub kilka takich podmiotów prawa publicznego.	TAK
3	Przetwarzania dokonuje podmiot prawa publicznego ustanowiony w szczególnym celu zaspokajania potrzeb w interesie ogólnym, który nie ma charakteru przemysłowego lub handlowego.	TAK
4	Przetwarzania dokonuje podmiot prawa publicznego posiadający osobowość prawną.	TAK
5	Przetwarzania dokonuje podmiot prawa publicznego finansowany w przeważającej części przez Państwo, władze regionalne lub lokalne czy też inne podmioty prawa publicznego; lub jeżeli jego zarząd podlega nadzorowi ze strony tych podmiotów; lub jeżeli ponad połowę składu jego organu administracji, zarządu lub nadzoru stanowią osoby mianowane przez Państwo, władze regionalne lub lokalne lub inne podmioty prawa publicznego.	TAK
6	Realizacja zadań w interesie publicznym przez organ lub podmiot publiczny.	TAK
7	Realizacja zadań w interesie publicznym przez inne osoby fizyczne i prawne podlegające prawu publicznemu lub prywatnemu w sektorach takich jak transport publiczny, dostarczanie wody i energii, infrastruktura drogowa, radiofonia i telewizja, budynki użyteczności publicznej, organy powołane do zawodów regulowanych.	TAK
8	Przetwarzania danych szczególnych tj. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej osoby, dane osobowe dotyczących wyroków skazujących i naruszeń prawa.	TAK
9	Główna działalność administratora[1] lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą[2], na dużą skalę[3].	TAK

Na podstawie powyższych przesłanek Administrator Danych Osobowych: **STWIERDZA / ~~NIE STWIERDZA~~** [4] zasadność powołania Inspektora Ochrony Danych Osobowych z dniem 25 maja 2018 r. a obecnie Administratora Bezpieczeństwa Informacji w zgodzie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922) oraz Rozporządzeniem Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016r.

WÓJT GMINY
Dariusz Zwoliński

.....
pieczątka i podpis Administratora Danych Osobowych

[1] patrz § 2 tj. „Główna działalność Administratora Danych Osobowych"
[2] patrz § 4 tj. „Regularne i systematyczne monitorowanie osób, których dane dotyczą"
[3] patrz § 3 tj. „Duża skala przetwarzania"
[4] niepotrzebne przekreślić

Załącznik Nr 1
do Zarządzenia
Nr 12/2020 Wójta Gminy
Nadarzyn z dnia
10 lutego 2020 r.

SWO.142.3.2018.WS

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W

Urzędzie Gminy Nadarzyn,
ul. Mszczonowska 24, 05-830 Nadarzyn

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
GMINA NADARZYN ul. Mszczonowska 24, 05-830 Nadarzyn NIP: 534-22-54-841 tel. 22 729-81-85	WÓJT GMINY Dariusz Zwoliński	25 maja 2018

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

Powyższy wstęp określa założenia ustawodawcy przewidziane w art. 47 oraz art. 51 Konstytucji RP jak również treść art. 32 rozporządzenia ogólnego o ochronie danych osobowych, który nakazuje każdemu administratorowi danych wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku.

Rozdział 1
Postanowienia ogólne

§ 1. Ilekroć w dokumencie jest mowa o:

1) **rozporządzeniu** – rozumie się przez to 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);
2) **danych osobowych** – rozumie się przez to 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) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8) **administratorze danych** – rozumie się przez to 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;
9) **zgodzie osoby, której dane dotyczą** – oznacza to 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;
10) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, 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;
11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
14) **profilowaniu** – oznacza to 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;
15) **pseudonimizacji** – oznacza to 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;
16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

17) **naruszeniu ochrony danych osobowych** – oznacza to 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.

Powyżej określono katalog definicji wynikający z art. 4 rozporządzenia

Rozdział 2
Administrator danych

§ 2. Administrator danych w szczególności:

1. 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 i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli obowiązek ten ma zastosowanie – prowadzi rejestr czynności przetwarzania.
3. Jeżeli obowiązek ten ma zastosowanie – wyznacza Inspektora Ochrony Danych (IOD).

Zgodnie z art. 24 rozporządzenia.

Rozdział 3
Środki techniczne i organizacyjne

§ 3. W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:

a) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach zgodnie z załącznikiem nr 1,
b) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych;
c) zawarto umowy powierzenia przetwarzania danych zgodnie z załącznikiem nr 3;
d) została opracowana i wdrożona niniejsza polityka bezpieczeństwa.

§ 4. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi);
b) zbiory danych osobowych przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej;
c) pomieszczenia, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy;
d) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli dostępu;
e) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;
f) zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej niemetalowej szafie;

g) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej;
h) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
i) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 5. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
c) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
d) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
e) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
f) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
g) użyto system Firewall do ochrony dostępu do sieci komputerowej;
h) użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

§ 6. W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
b) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
c) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
d) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
e) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;
f) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
g) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 7. W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;

c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
e) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Rozdział 4
Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 8. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych lub administrator danych samodzielnie z wykorzystaniem załącznika nr 1.
§ 9. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
§ 10. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych właściciele procesów lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.
§ 11. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.
§ 12. Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr 1.
Przykładowa realizacja wymogów z art. 24 rozporządzenia

Rozdział 5
Procedura współpracy z podmiotami zewnętrznymi

§ 13. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr3.
§ 14. Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać z wykorzystaniem listy kontrolnej.
Przykładowa realizacja wymogów z art. 28 rozporządzenia

Rozdział 6
Procedura zarządzania incydentami

§ 15. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
§ 16. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.

§ 17. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.

§ 18. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych. *Przykładowa realizacja wymogów z art. 33 i 34 rozporządzenia*

Rozdział 7
Procedura realizacji praw osób

§ 19. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.

§ 20. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

§ 21. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 22. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia. *Przykładowa realizacja wymogów z art. 16–22 rozporządzenia*

Rozdział 8
Procedura odbierania zgód oraz informowania osób

§ 23. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikami nr 4.

§ 24. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikami nr 4.

§ 25. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikami nr 4. *Przykładowa realizacja wymogów z art. 7 oraz 13 i 14 rozporządzenia.*

Rozdział 9
Postanowienia końcowe

§ 26. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 27. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki:

- *Arkusz analizy zagrożeń ryzyka przy przetwarzaniu danych osobowych (załącznik nr 1),*
- *Ewidencja osób upoważnionych do przetwarzania danych osobowych (załącznik nr 2),*
- *Umowa powierzenia przetwarzania danych osobowych (załącznik nr 3),*
- *Przykładowe klauzule (załącznik nr 4),*
- *Procedura niszczenia danych na nośnikach elektronicznych i papierowych (załącznik nr 5),*
- *Procedura „czystego biurka/czystego pulpitu" (załącznik nr 6),*
- *Upoważnienia do przetwarzania danych osobowych (załącznik nr 7),*
- *Procedura postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik nr8),*
- *Rejestr umów powierzenia przetwarzania danych (załącznik nr 9),*
- *Rejestr czynności przetwarzania (załącznik nr 10),*
- *Rejestr kategorii czynności przetwarzania (załącznik nr 11),*
- *Wniosek o sprostowanie danych osobowych (załącznik nr 12),*
- *Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar w którym przetwarzane są dane osobowe (załącznik nr 13),*
- *Wykaz zbiorów danych osobowych (załącznik nr 14),*
- *Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiazania między nimi (załącznik nr 15),*
- *Sposób przepływu danych pomiędzy poszczególnymi systemami (załącznik nr 16),*
- *Oświadczenie o zachowaniu w tajemnicy przetwarzania danych osobowych (załącznik nr 17),*
- *Wyrejestrowanie uprawnień dostępu do systemów informatycznych (załącznik nr 18),*
- *Upoważnienie dla osoby odpowiedzialnej za przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych (załącznik nr 19),*
- *Instrukcja Zarządzania Systemami Informatycznymi (załącznik nr 20).*

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn

SWO.142.7.2019.WS

Załącznik Nr 1 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych

ANALIZA RYZYKA

RODO

zgodnie z art. 5 ust. 2 oraz Motywem 76 Preambuły 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).

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot:	Urząd Gminy Nadarzyn
z dnia:	2019-07-22
Zatwierdził(a):	WÓJT GMINY Dariusz Żwoliński ..... podpis administratora danych

Spis treści

1. DEFINICJE 3
2. WSTĘP 4
3. OPIS PROCEDURY ZARZĄDZANIA RYZYKIEM 5
4. OPIS METODY SZACOWANIA RYZYKA – SKALA PIĘCIOSTOPNIOWA 8
5. KONTEKST I ZAGROŻENIA 9
6. TABELA SZACOWANIA RYZYKA 11
7. WNIOSKI 13

1. DEFINICJE

Administrator Danych – jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Aktywa - kontrolowane przez jednostkę zasoby majątkowe o wiarygodnie określonej wartości, uzyskane w wyniku przeszłych zdarzeń, które spowodują w przyszłości wpływ do jednostki korzyści ekonomicznych;

Identyfikowanie ryzyka – szereg czynności polegających na określeniu sytuacji, które mogą się wydarzyć i spowodować straty/naruszenie;

Kontekst – informacje wiążące się z działaniem jednostki, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych;

Akceptacja ryzyka – określenie dopuszczalności danego ryzyka, definiowane poprzez wartość progową, przy przedziałach ryzyka;

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;

Ocena ryzyka – czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania podmiotu;

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);

Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka;

Zabezpieczenie - środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia.

2. WSTĘP

Każdy podmiot, jednostka, bądź organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem: zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, bądź dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Zgodnie z art. 24 ust. 1 jednym z zadań Administratora Danych jest wdrożenie odpowiednich zabezpieczeń, aby przetwarzanie danych odbywało się w zgodzie z RODO. Z pomocą przychodzą dokumenty: Analiza ryzyka RODO, a następnie Ocena skutków ryzyka dla ochrony danych osobowych, które są częścią ciągłego procesu udoskonalania systemu zarządzania bezpieczeństwem informacji. W celu przygotowania i przeprowadzenia analizy, wymagane jest profesjonalne podejście do zakresu ochrony informacji oraz danych, które pozwoli poznać szczegóły przeprowadzanych operacji przetwarzania danych wraz z warunkami środowiska, w którym odbywa się przetwarzanie. "Analiza ryzyka RODO", która będzie także punktem wyjścia do Oceny skutków ryzyka, pozwoli na zwiększenie poziomu bezpieczeństwa przetwarzanych danych osobowych.

Zapisy RODO uprawniają Administratora Danych do przetwarzania danych, gdy:

- upoważnia go do tego:
  - podstawa prawna;
  - wyrażenie zgody osoby, której dane dotyczą;
  - przetwarzanie jest niezbędne do wykonania umowy;
  - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
  - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
  - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
  - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
- przy przetwarzaniu danych zapewniona jest im poufność, integralność oraz dostępność;
- dane osobowe zostaną adekwatnie zabezpieczone za pomocą wdrożonych środków technicznych jak i organizacyjnych gwarantujących odpowiedni poziom bezpieczeństwa, pamiętając, że im wyższe ryzyko naruszenia występuje, tym wyższy poziom ochrony należy zastosować. Zwracając uwagę na szybki postęp technologiczny oraz podnoszenie standardów bezpieczeństwa, stosowane rozwiązania powinny pomóc na bieżąco mierzyć i oceniać ich adekwatność oraz aktualność.

Decydując o doborze środków technicznych i organizacyjnych, należy uwzględnić poniższe czynniki:

- stan wiedzy technicznej;
- koszt wdrożenia wymaganych zabezpieczeń;
- charakter, zakres, kontekst i cel przetwarzania;
- ryzyko naruszenia praw i wolności osób fizycznych.

RODO, ze względu na szereg ogólnych zapisów wskazuje na możliwość:

- tworzenia kodeksów podstępowania, których zakres doprecyzuje zastosowanie dokumentu;
- przeprowadzenia mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, które świadczą o spełnieniu obowiązków nałożonych na Administratorów.

Środkiem organizacyjnym pomagającym zapewnić bezpieczeństwo jest wydane stosowne upoważnienie każdej osobie przetwarzającej dane osobowe i zatrudnionej u Administratora. Nie należy zapominać, o zaznajomieniu pracowników z zasadami ochrony danych osobowych zastosowanych w podmiocie oraz pouczeniu o zobowiązaniu do zachowania tajemnicy, w związku z przetwarzanymi danymi.

3. OPIS PROCEDURY ZARZĄDZANIA RYZYKIEM

Przepis art. 5 ust. 1 RODO wprowadza osiem zasad przetwarzania danych osobowych, zawartych w sześciu punktach:

- zasadę legalności, rzetelności i przejrzystości przetwarzania (zgodności z prawem);
- zasadę celowości (ograniczenia celu);
- zasadę minimalizacji danych (adekwatności, proporcjonalności);
- zasadę prawidłowości (poprawności);
- zasadę ograniczenia czasowego (czasowości);
- zasadę odpowiedniego bezpieczeństwa (integralności i poufności danych).

Najważniejszą z powyższych zasad jest zasada legalności, której przestrzeganie Administrator Danych musi być w stanie wykazać. Zasada legalności oznacza wymóg, aby dane osobowe były przetwarzane zgodnie z prawem, a więc przede wszystkim zgodnie z RODO. Obowiązek legalności przetwarzania danych to przede wszystkim konieczność spełnienia

przesłanki uprawniającej do takiego przetwarzania. Przesłanki, w zależności od kategorii danych, zostały określone w art. 6 i 9 RODO. Ponadto legalność oznacza zgodność z pozostałymi przepisami RODO oraz obowiązującymi ustawami i wydanymi na ich podstawie aktami wykonawczymi.

Bezpieczeństwo danych osobowych powinno być odpowiednie. Z analizy motywów i artykułów RODO dowiemy się, że bezpieczeństwo danych ma być odpowiednie do ryzyka naruszenia praw i wolności osób, których dane dotyczą. Oznacza to, że poziom bezpieczeństwa powinien być dostosowany do tego, jaką szkodę lub krzywdę może wyrządzić osobom naruszenie bezpieczeństwa ich danych. Realizacja zasady odpowiedniego bezpieczeństwa będzie więc miała ścisły związek z szacowaniem ryzyka przetwarzanych danych. W zależności od rodzaju posiadanych danych, sposobu ich przetwarzania czy wielkości podmiotu będącego administratorem danych konieczne jest zastosowanie odpowiednich środków bezpieczeństwa minimalizujących ryzyko utraty kontroli nad przetwarzanymi danymi.

Zagadnienie dotyczące zasady odpowiedniości bezpieczeństwa w połączeniu z zasadą rozliczalności polega na tym, że jeśli nie zostanie przeprowadzona analiza i klasyfikacja ryzyka naruszenia ochrony danych, a w jej ramach ryzyka i konsekwencji naruszenia praw i wolności osób, nie będzie można wykazać, że zastosowane zostały odpowiednie środki bezpieczeństwa. Należy więc ocenić ryzyko, żeby zastosować odpowiednie do niego środki. Administrator danych powinien położyć nacisk na kwestie bezpieczeństwa, uwzględniając zagrożenia pochodzące zarówno z zewnątrz, jak i wewnątrz podmiotu. Kluczowa będzie analiza oraz podnoszenie poziomu zabezpieczeń. Digitalizacja zasobów i powszechne wykorzystywanie nowoczesnych technologii sprawiają, że sprawna realizacja celów biznesowych zależna jest od bezpieczeństwa zasobów informacyjnych i usług oraz infrastruktury teleinformatycznej umożliwiającej korzystanie z cyberprzestrzeni. Zastosowanie przez administratora danych systemów zapobiegających wyciekom danych, których ujawnienie może narazić podmiot na odpowiedzialność karną, cywilną lub innego rodzaju straty jest konieczne w aspekcie ochrony danych oraz informacji. Zasada bezpieczeństwa musi być zgodna z zasadą legalności i minimalizacji.

Niezależnie od wprowadzonej w art. 5 ust. 2 RODO zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania, w tym zasady legalności, musi być w stanie wykazać ich przestrzeganie. Dodatkowo w art. 7 ust. 1 RODO podkreślono, że jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Administrator musi zatem pamiętać o utrwaleniu faktu uzyskania zgody na przetwarzanie danych w celu wykazania, w szczególności przed organem nadzorczym, że otrzymał zgodę na przetwarzanie danych osobowych. Zgoda osoby, której dane dotyczą, musi mieć charakter uprzedni w stosunku do przetwarzania jej danych przez administratora.

Zarządzanie ryzykiem opiera się na wdrożeniu schematu postępowania nazwanego cyklem Deminga. Jest to proces polegający na ciągłej poprawie danego zagadnienia, by osiągnąć jak najwyższy poziom realizacji. Cykl Deminga charakteryzuje się czterema etapami:

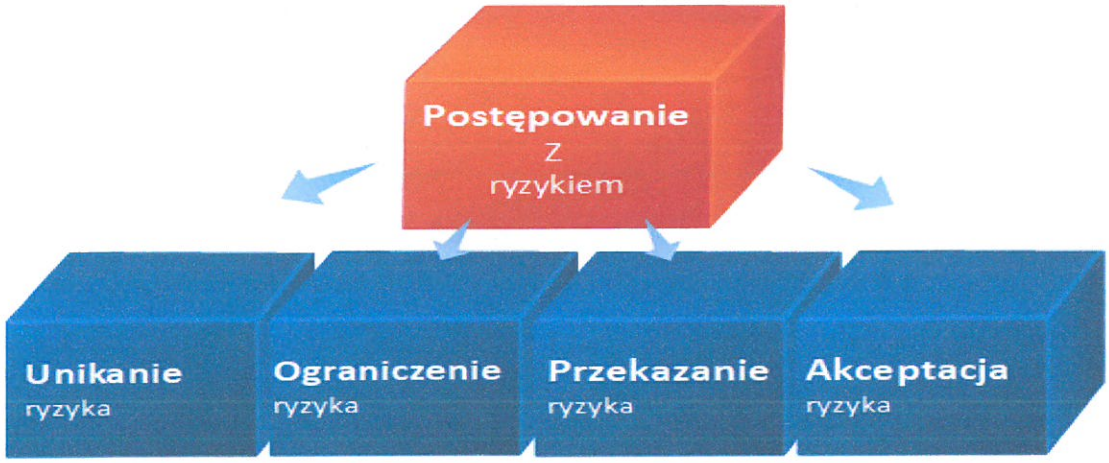
- zaplanuj;
- wykonaj;
- sprawdź;
- popraw.

Jeśli po wykonaniu ostatniego etapu nadal nie udało się osiągnąć wyznaczonego poziomu realizacji, należy całą procedurę ponowić. Dopiero w przypadku odniesienia oczekiwanych rezultatów, można uznać całą procedurę jako normę (standard) i jedynie monitorować prawidłowość jej działania.

Dla zagadnienia ochrony danych osobowych przyjęto poniższy schemat, gdzie zastosowano

odpowiednie pojęcia niezbędne przy Analizie Ryzyka RODO.

- Kontekst – wyznaczenie zagrożonych elementów podmiotu, które mają pośredni i bezpośredni wpływ na ochronę danych osobowych;
- Szacowanie ryzyka – określenie występujących w podmiocie zagrożeń, skutków ich wystąpienia oraz prawdopodobieństwa, czy dane zagrożenie może nastąpić;
- Postępowanie z ryzykiem – wybór jednej ze ścieżek postępowania (rysunek poniżej);
- Sprawdzenie – zweryfikowanie, czy po zmianach dla danego kontekstu występuje jeszcze zagrożenie przy przetwarzaniu danych osobowych.



4. OPIS METODY SZACOWANIA RYZYKA – SKALA PIĘCIOSTOPNIOWA

Do sporządzenia Analizy ryzyka RODO, obejmującej wszystkie możliwe zagrożenia oraz konteksty przetwarzań danych osobowych, posłużyła metoda szacowania ryzyka na podstawie skali pięciostopniowej. W tej metodzie korzysta się z dwóch następujących parametrów ryzyka: skutków wystąpienia danego zagrożenia oraz prawdopodobieństwa z jakim zagrożenie może wystąpić. Szacowanie zarówno skutków jak i prawdopodobieństwa określa na pięciu poziomach (w skali od 1 do 5): bardzo małym, małym, średnim, dużym i bardzo dużym dla każdego występującego zagrożenia, zgodnie z tabelą przedstawioną poniżej:

Poziom skutku i prawdopodobieństwa	Wartość skutku i prawdopodobieństwa
Bardzo małe	1
Małe	2
Średnie	3
Duże	4
Bardzo duże	5

Tym sposobem szacuje się parametry wszystkich poziomów skutków oraz prawdopodobieństw, które mogą wystąpić dla danego zagrożenia. Następnie zgodnie z tabelą zaprezentowaną poniżej należy określić poziomy danego ryzyka – w skali od 1 do 25, korzystając ze wzoru: R = s * p, gdzie:

R – ryzyko dla danego zagrożenia;

s – poziom skutku zagrożenia;

p – poziom prawdopodobieństwa wystąpienia zagrożenia.

	Prawdopodobieństwo wystąpienia zagrożenia				
Skutek wystąpienia zagrożenia	**Bardzo małe**	**Małe**	**Średnie**	**Duże**	**Bardzo duże**
Bardzo małe	Bardzo małe	Bardzo małe	Małe	Małe	Małe
Małe	Bardzo małe	Małe	Małe	Małe	Średnie
Średnie	Małe	Małe	Średnie	Średnie	Średnie
Duże	Małe	Małe	Średnie	Duże	Duże
Bardzo duże	Małe	Średnie	Średnie	Duże	Bardzo duże

Oszacowaną wartość ryzyka danego zagrożenia przyporządkowuje się odpowiedniemu poziomowi ryzyka według tabeli:

Poziom ryzyka	Wartość ryzyka
Bardzo małe	1-2
Małe	3-8
Średnie	9-15
Duże	16-20
Bardzo duże	21-25

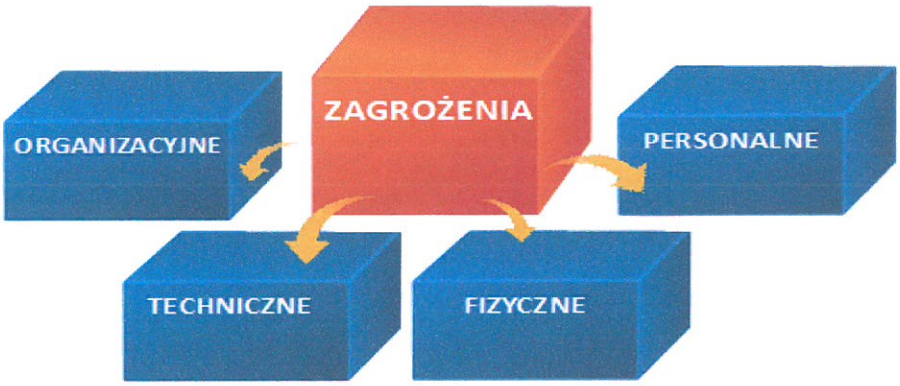
Powyższa metoda pozwala oszacować ryzyko dla każdego zagrożenia, uwzględniając poziom skutków i prawdopodobieństwa, dając tym samym możliwość określenia, czy dane ryzyko jest akceptowalne.

Poziom ryzyka	
Bardzo małe	Akceptowalne
Małe	Akceptowalne
Średnie	Akceptowalne
Duże	Akceptowalne
Bardzo duże	Nieakceptowalne

5. KONTEKST I ZAGROŻENIA

Ustalenie kontekstu jest podstawą do prawidłowego sporządzenie Analizy ryzka RODO, która jest punktem wyjścia do Oceny skutków ryzyka dla ochrony danych. Na wstępie należy przede wszystkim określić możliwe zagrożenia, które mogą mieć negatywny wpływ na uwarunkowania związane z działaniem podmiotu, a w szczególności dotyczące posiadanych danych osobowych w wersji papierowej, sprzętu, oprogramowania, pomieszczeń oraz nośników danych.

Na wymienione powyżej aktywa wpływają różne czynniki zagrożeń, zarówno zewnętrzne, jak i wewnętrzne, dlatego ważne jest sporządzenie ich listy. Identyfikacja zasobów i zagrożeń powinna być przeprowadzona na odpowiednim poziomie szczegółowości, co zapewni prawidłowe oszacowanie poszczególnych ryzyk i poziomów akceptacji. Zagrożenia można podzielić na kilka grup:



Najczęściej występujące zagrożenia, prowadzące do naruszeń:

a) Organizacyjne:

- brak nadanych upoważnień osobom przetwarzającym dane osobowe;
- brak wdrożonych polityk i procedur dotyczących ochrony danych osobowych;
- brak powołania Inspektora Ochrony Danych Osobowych w sytuacji, gdy wyznaczenie jest obligatoryjne;
- nieuprawniony dostęp do pomieszczenia, w którym są przetwarzanie dane osobowe.

b) Techniczne:

- atak hakerski;
- działanie złośliwego oprogramowania (wirusy);
- awaria nośników danych;
- awaria sprzętu sieciowego;
- awaria serwerów;
- awaria zasilania – brak UPS;
- celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych;
- przesłanie danych drogą mailową do złego odbiorcy.

c) Fizyczne:

- zalanie/powódź;
- pożar;

- kradzież sprzętu z danymi;
- kradzież danych w wersji papierowej;
- zniszczenie danych osobowych bez użycia niszczarki;
- atak terrorystyczny;
- zwarcie instalacji;
- nieodpowiednie przechowywanie danych;
- utrata przetwarzanych danych;
- niewystarczający poziom zabezpieczeń pomieszczeń.

d) Personalne:

- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
- wejście w posiadanie danych osobowych przez osobę nieuprawnioną;
- udostępnianie danych osobowych osobom nieupoważnionym;
- udostępnianie haseł innym pracownikom;
- nie zachowanie tajemnicy służbowej dotyczącej danych osobowych przez pracowników podczas pracy, jak i po jej zakończeniu;
- otwieranie podejrzanych maili, mogących zawierać wirusy komputerowe;
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

6. TABELA SZACOWANIA RYZYKA

Lp.	Zagrożenie	Aktywa zagrożone	Skutki	Prawdopodobieństwo	Ryzyko	Akceptacja ryzyka
1	Zalanie/powódź	SP, P, OP, N, WP	3	1	3	Akceptowalne
2	Pożar	SP, P, OP, N, WP	4	2	8	Akceptowalne
3	Kradzież danych w wersji papierowej	WP	3	2	6	Akceptowalne
4	Kradzież sprzętu z danymi	SP, OP	4	2	8	Akceptowalne
5	Atak hakerski	SP, OP, N	4	3	12	Akceptowalne
6	Awaria nośników danych	N	3	4	12	Akceptowalne
7	Utrata danych (brak	OP	4	1	4	Akceptowalne

	kopii zapasowych)					
8	Awaria sprzętu sieciowego	SP, OP	3	3	9	Akceptowalne
9	Awaria serwerów	OP	4	2	8	Akceptowalne
10	Nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik	OP	3	2	6	Akceptowalne
11	Wejście w posiadanie danych osobowych przez osobę nieuprawnioną	OP, N, WP	4	1	4	Akceptowalne
12	Udostępnianie danych osobowych osobom nieupoważnionym	OP, N, WP	4	2	8	Akceptowalne

Aktywa: SP- Sprzęt, P – Pomieszczenia, OP – Oprogramowanie, N – Nośniki danych, WP – Dane w wersji papierowej.

7. WNIOSKI

Po przeprowadzeniu analizy dotyczącej ryzyka wystąpienia naruszeń w zakresie ochrony danych osobowych, zwanej Analizą Ryzyka RODO,
zwrócono uwagę, iż Administrator Danych dołożył wszelkich starań, by poziom ochrony danych osobowych był jak najwyższy. Wszystkie występujące zagrożenia cechują się akceptowalnym poziomem ryzyka, dzięki czemu nie będą miały wpływu na naruszenia dotyczące ochrony danych osobowych. Jednakże Administrator Danych powinien sukcesywnie kontrolować, czy stopień ryzyka pojawienia się naruszenia nie zwiększy się w przyszłości.

W przypadku wystąpienia zbyt dużego ryzyka cząstkowego (dotyczącego jednego zagrożenia) należy dołożyć wszelkich starań, by to ryzyko zminimalizować. Artykuł 32 ust. 1 RODO wskazuje działania i środki, które mogą być wdrożone do minimalizacji ryzyka:

- pseudonimizacja i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Należy jednak pamiętać, że są to przykłady możliwych działań - konkretne rozwiązania zależą od Administratora Danych i są wynikiem Analizy Ryzyka RODO. RODO wskazuje również przypadki, gdy wywiązywanie się z obowiązku przeprowadzenia analizy ryzyka będzie ograniczone. Ma to miejsce w sytuacji, gdy organizacja stosuje zatwierdzony przez organ nadzorczy kodeks postępowania lub mechanizm certyfikacji. Należy zwrócić uwagę, że konieczne jest, aby takie dokumenty uzyskały formalną akceptację UODO (Urząd Ochrony Danych Osobowych), ponieważ bez takiej akceptacji nie dają ochrony przewidzianej przepisami.

INSPEKTOR
22.07.2019r. mgr Wiesław Sobczyński

.....
(data i podpis Inspektora Ochrony Danych)

Załącznik Nr 2 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login /identyfikator	Nazwa zbioru danych osobowych
1	2	3	4	5	6	7

Zakres upoważnienia:

d - wgląd;
w - wprowadzanie;
m - modyfikowanie;
u – usuwanie,
p – powierzanie, udostępnianie

Uwaga: dokument funkcjonuje w formie elektronicznej

Załącznik Nr 3 do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(zwana dalej „Umową")

_____ *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Podmiotem przetwarzającym"**

reprezentowana przez:

_____

oraz

_____ *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

reprezentowana przez:

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (**należy podać rodzaj danych*) ..... *np. dane zwykłe oraz dane szczególnych kategorii* ..... *(*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci* ..... *np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.*
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu ..... (**należy podać cel przetwarzania danych przez podmiot przetwarzający*) *np. realizacji umowy z dnia ..... nr ..... w zakresie prowadzenia kadr.*

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ..... (**można wskazać np. w ciągu 24 h*).

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum ..... *(*należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli)* jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji

administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ..... do ..... .*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... * okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

_____ _____

Administrator danych Podmiot przetwarzający

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75
Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn

SWO.142.3.2018.WS

PROCEDURA
NISZCZENIA DANYCH NA NOŚNIKACH ELEKTRONICZNYCH I PAPIEROWYCH

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a w szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny w tym również komisyjnie w/g Załącznika - Protokół zniszczenia uszkodzonych nośników. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera / zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie.
4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji, nagrania z procesu transportu i utylizacji.

Administrator Danych Osobowych

WÓJT GMINY

.....

Dariusz Żwoliński

Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn

Protokół zniszczenia uszkodzonych nośników komputerowych

Nadarzyn, dnia .....r.

ZATWIERDZAM

.....

Protokół
zniszczenia uszkodzonych nośników komputerowych
.....
(jednostka, komórka organizacyjna)

Dnia ..... komisja powołana przez .....
(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:

1. Przewodniczący: .....
2. Członkowie: .....

.....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....
.....
.....

komórka organizacyjna

ADMINISTRATOR SYSTEMU

.....

Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH

Dnia ..... komisja powołana przez .....

w składzie:

1. Przewodniczący: .....
2. Członkowie: .....

.....

dokonała trwałego zniszczenia zbioru danych osobowych o nazwie .....

Zniszczenie obejmuje:
- wersję papierową zbioru. Zniszczenia dokonano poprzez .....

- bazę danych. Zniszczenia dokonano poprzez .....

- kopie bezpieczeństwa. Zniszczenia dokonano poprzez .....

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

.....

SWO.142.3.UG.2018.WS

PROCEDURA CZYSTEGO BIURKA/CZYSTEGO PULPITU

w Urzędzie Gminy Nadarzyn
ul. Mszczonowska 24, 05-830 Nadarzyn

1. Niniejsza procedura czystego biurka obowiązuje wszystkich pracowników zatrudnionych w jednostce.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, umowy cywilno – prawnej a także doktoranta, studenta i stażystę, niebędących pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
3. Za pracodawcę uważa się Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn.
4. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań. W przypadku obsługi interesanta pracownik jest zobowiązany zabezpieczyć dokumenty przed nieuprawnionym dostępem.
5. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
6. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty w miejsce wyznaczone przez Administratora.
7. Po zakończonej pracy pracownik zobowiązany jest odłożyć laptopa w miejsce wyznaczone przez Administratora, nie dotyczy komputerów stacjonarnych.
8. Po zakończonej pracy pracownik zobowiązany jest sprawdzić, czy wszystkie dokumenty zostały wydrukowane i nie pozostały wydruki na drukarce, bądź w pamięci drukarki (np. z powodu braku papieru w drukarce).
9. Po zakończonej pracy na biurku mogą znajdować się jedynie komputer stacjonarny, telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
10. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.
11. Niniejsza Procedura obowiązuje od dnia 25 maja 2018 r.

Administrator Danych Osobowych

WÓJT GMINY

.....
Dariusz Zwoliński

Wykonał: Wiesław Sobczyński
wew. 197

Nadarzyn, dn. ..... r.

UPOWAŻNIENIE

do przetwarzania danych osobowych

Na podstawie Art. 29 i 32 ust. 4 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 119/1 z 4.5.2016 r.) ., zwane dalej RODO, upoważniam ~~Pana~~/Panią :

.....

~~zatrudnionego~~/zatrudnioną na stanowisku: .....

W związku z wykonywaniem obowiązków służbowych, w ramach niniejszego upoważnienia otrzymuje ~~Pan~~/Pani dostęp do poniższych zbiorów danych osobowych:

Lp.	Nazwa zbioru danych osobowych zgodna z PBI	dostęp do wersji papierowej	dostęp do wersji elektronicznej
1.		[TAK/~~NIE~~]	[TAK/~~NIE~~]
2.		[TAK/~~NIE~~]	[TAK/~~NIE~~]
3.		[TAK/~~NIE~~]	[TAK/~~NIE~~]

Okres ważności upoważnienia:

od: .....

do: rozwiązania umowy o pracę, zmiany stanowiska pracy oraz zmiany zakresu obowiązków.

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ

Niniejszym zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych z którymi mam styczność podczas wykonywania zadań służbowych lub będę miała/ł dostęp, a nieprzeznaczonych do publicznego rozpowszechniania. Potwierdzam, że zapoznałem się z Polityką Bezpieczeństwa Informacji oraz wszelkimi regulacjami z tego zakresu, wprowadzonymi przez Administratora Danych. Jednocześnie jestem świadomy/a, że osoby upoważnione do przetwarzania danych zobowiązane są zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia, także po ustaniu stosunku pracy lub po upływie ważności upoważnienia. Ponadto podlegają odpowiedzialności karnej wynikającej z art. 107 oraz art. 108 Ustawy o ochronie danych osobowych z 10 maja 2018 r.

Zobowiązuje się do nierozpowszechniania i niewykorzystywania informacji zdobytych w trakcie wykonywania obowiązków pracowniczych, a także po ustaniu zatrudnienia. Z chwilą ustania zatrudnienia zobowiązuje się do niezwłocznego zwrócenia pracodawcy wszelkich dokumentów oraz innych materiałów dotyczących informacji chronionych.

Przyjmuję do wiadomości i akceptuję, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu przepisów Kodeksu Pracy oraz, że strona poszkodowana ma prawo do dochodzenia na zasadach ogólnych odszkodowania odpowiadającego wysokości poniesionej szkody.

.....

podpis pracownika

WYPEŁNIA ADMINISTRATOR DANYCH
1. W związku z wydanym upoważnieniem, zobowiązuję Administratora Systemu Informatycznego do wydania stosownego dostępu do systemu informatycznego według poniższej tabeli. 2. Otrzymanie dostępu do systemu informatycznego polega na przydzieleniu użytkownikowi unikalnego loginu do systemu oraz hasła startowego. 3. Upoważniony jest zobowiązany zmienić otrzymane hasło startowe przy pierwszym logowaniu do systemu.

Lp.	Nazwa systemu informatycznego
1.	
2.	
3.	

....

data i podpis upoważnionego podpis Administratora Danych

W/w dostęp do systemu informatycznego został udzielony dnia:

....

podpis upoważnionego podpis Administratora Systemów

SWO.142.3.2018.WS

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

Istota naruszenia ochrony danych osobowych

§ 1

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

Naruszeniem ochrony danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, przywłaszczenia danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego,

a w szczególności:

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

§ 2

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

Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:

- ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
- dokumentacja jest niszczona bez użycia niszczarki,
- fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,

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

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

- ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,

- wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz instytucji bez upoważnienia,

- udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,

- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),

- telefoniczne próby wyłudzenia danych osobowych,

- kradzież komputerów lub twardych dysków z danymi osobowymi,

- utrata kontroli nad kopią danych osobowych,

- e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,

- pojawienie się wirusa komputerowego lub niestandardowe „zachowanie" komputerów,

- istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki",

- hasła do systemów przechowywane są w pobliżu komputera.

§ 3

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

§ 4

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

§ 5

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

§ 6

Inspektor ochrony danych podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,

- odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,

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

§ 7

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

§8

Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia

przetwarzania danych osobowych - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

§ 9

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 lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu ochrony danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 10

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

Zgłoszenie, o którym mowa w ust. 1, musi co najmniej: a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

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

§ 11

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

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

Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do ochrony danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1; c) wymagałoby ono niewspółmiernie dużego wysiłku.

W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załączniki: 3

Załącznik nr 1 - Raport z naruszenia ochrony danych - Inspektor Ochrony Danych.

Załącznik nr 2 - Rejestr incydentów, działań korygujących i zapobiegawczych - Inspektor Ochrony Danych.

Załącznik nr 3 - Zgłoszenie naruszenia ochrony danych organowi nadzorczemu - Inspektor Ochrony Danych.

Administrator Danych Osobowych

WÓJT GMINY

.....Dariusz Bodański.....

Wykonał: Wiesław Sobczyński

wew. 197

Załącznik nr 1. Raport z naruszenia ochrony danych

1. Data ..... Godzina .....

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

.....

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

.....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

5. Podjęte działania:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

7. Postępowanie wyjaśniające i naprawcze:

.....

(podpis pracownika)

.....

(data i podpis Inspektora ochrony danych)

.....

Załącznik nr 3.

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

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

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

.....

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

.....

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

.....

5. Podjęte działania:

.....

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

.....

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

.....

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

.....

.....

(data i podpis administratora)

.....

Załącznik Nr 9 do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych

Dokument funkcjonuje w formie elektronicznej

REJESTR UMÓW POWIERZENIA PRZETWARZANIA DANYCH

Lp.	Nazwa Administratora	Kategoria osób których dane dotyczą, kategoria danych osobowych, zakres przetwarzanych danych	Numer umowy powierzenia	Zakres czynności przetwarzania
1				

Przetwarzający Dane

.....

Załącznik Nr 9-1 do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych

Dokument funkcjonuje w formie elektronicznej

EWIDENCJA UMÓW

powierzenia przetwarzania danych osobowych

Lp.	*Data zawarcia umowy*	*Oznaczenie podmiotu z którym zawarta jest umowa powierzenia*	*Zakres powierzenia wynikający z umowy*	*Okres na jaki została zawarta umowa lub termin jej wygaśnięcia*	*Cel powierzenia danych osobowych*
1.					

GMINA NADARZYN
ul. Mszczonowska 24, 05-830 Nadarzyn
NIP: 534-22-54-841
tel. 22 729-81-85

REJESTR CZYNNOŚCI PRZETWARZANIA

SWO.142.UG.3.2018.WS

Gmina Nadarzyn

Imię i nazwisko lub nazwa administratora .....

ul. Mszczonowska 24, 05-830 Nadarzyn, tel. 22 729 81 85, fax. 22 729 81 75

Dane kontaktowe administratora .....

nie dotyczy

Dane współadministratorów .....

Wiesław Sobczyński, wsobczynski@nadarzyn.pl, tel. 22 729 81 85 wew. 197

Dane inspektora ochrony danych .....

Cel przetwarzania	Celem przetwarzania danych jest wypełnienie obowiązków określonych w przepisach prawa: - **ewidencja korespondencji kierowanej do Wójta Gminy Nadarzyn** - Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. 2018 poz. 994 ze zmianami), Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011 r. Nr 14, poz. 67); - **rozpatrywanie skarg i wniosków kierowanych do Rady Gminy Nadarzyn** - Ustawa z dnia 14 czerwca 1960 r. Kodeks Postępowania Administracyjnego (Dz.U. 2017 poz. 1257 ze zm.); - **rozpatrywanie skarg i wniosków kierowanych do Wójta Gminy Nadarzyn** - Ustawa z dnia 14 czerwca 1960 r. Kodeks Postępowania Administracyjnego (Dz.U. 2017 poz. 1257 ze zmianami); - **odpowiedzi na wnioski o udostępnienie informacji publicznej** - Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (j.t. Dz.U. 2016 poz. 1764 ze zmianami); - **realizacja świadczeń socjalnych pracowników, rodzin pracowników i byłych pracowników** - Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych (Dz.U. 2017 poz. 2191, ze zmianami); - **ewidencja pracowników i byłych pracowników** - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. D.U. z 2016 r. poz. 1666); Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (j. t. Dz.U. 2016 poz. 902 ze zmianami); Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz.U. z 2017 r.),Ustawa z 27 sierpnia 2009 r. o finansach publicznych (j. t. Dz.U. 2017 poz. 2077); - **ewidencja ludności** - Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz.U. 2017 poz. 1875 ze zmianami), Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (j.t. Dz.U. 2016 poz. 2064 ze zmianami), Ustawa z dnia 24 września 2010 r. o

	ewidencji ludności (j.t. Dz.U. 2017 poz. 657 ze zmianami); - **ewidencja mieszkańców** - Ustawa z dnia 24 września 2010 r. o ewidencji ludności (j.t. Dz.U. 2017 poz. 657 ze zmianami; - **wydanie decyzji o zmianie imion i nazwisk** - Ustawa z dnia 17 października 2008 r. o zmianie imienia i nazwiska (j.t. Dz.U. 2016 poz. 10 ze zmianami).; - **wydanie decyzji środowiskowych** - Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (j.t. Dz. U.2017 poz.1405 ze zmianami); - **wydanie zgody dla osób ubiegających się o dofinansowanie** - Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (j. t. Dz.U. 2018 poz. 799); - **ewidencja osób fizycznych, które złożyły deklaracje na wywóz odpadów komunalnych** - Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (j.t. Dz.U. 2017 poz. 1289 ze zmianami); - **ewidencja osób fizycznych składających wniosek o usunięcie drzewa** - Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody (j.t. Dz.U. 2018 poz. 142 ze zmianami); - **ewidencja podmiotów prowadzących działalność gospodarczą - wywóz nieczystości stałych i płynnych** - Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (j. t. Dz.U. 2017 poz. 1289 ze zmianami); - **ewidencja osób posiadających przydomowe oczyszczalnie ścieków** - Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (t.j. Dz.U. 2018 poz. 799), ustawa z dnia 18 lipca 2001 r. Prawo wodne (Dz.U. 2017 poz. 1566 ze zmianami); - **ewidencja pozwoleń o dopuszczalność emisji do środowiska** - Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (j.t. Dz.U. 2018 poz. 799); - **ewidencja osób, które złożyły wniosek o wydanie pozwolenia na chów psów ras niebezpiecznych** - Ustawa z dnia 21 sierpnia 1997 r. o ochronie zwierząt (j. t. Dz.U. 2017 poz. 1840 ze zmianami), Rozporządzenie Ministra Spraw Wewnętrznych i Administracji) z dnia 28 kwietnia 2003 r. w sprawie wykazu ras psów uznawanych za agresywne (Dz. U. z 2003 r. Nr 77, poz. 687); - **ewidencja osób wnioskujących o wydanie decyzji do projektów robót geologicznych** - Ustawa z dnia 9 czerwca 2011 r. Prawo geologiczne i górnicze (j.t. Dz.U. 2017 poz. 2126 ze zmianami); - **ewidencja osób fizycznych prowadzących działalność, w wyniku której powstają odpady niebezpieczne oraz nie zaliczone do niebezpiecznych** - Ustawa z dnia 14 grudnia 2012 r. o odpadach

	(j.t. Dz.U. 2018 poz. 21 ze zmianami); - **ewidencja osób fizycznych i prawnych zobowiązanych do ponoszenia opłaty za zmniejszoną naturalną retencję terenową** - Ustawa z dnia 20 lipca 2017 r. Prawo wodne (Dz. U. z 2017 r. poz. 1566 ze zmianami); - **wszczęcie postępowania administracyjnego w sprawie zmiany stanu wody na gruncie** - Ustawa z dnia 20 lipca 2017 r. Prawo wodne (Dz. U. z 2017 r. poz. 1566 ze zmianami); - **szacowanie strat, wydanie zezwolenia oraz powiadamianie przez urząd o obowiązku utrzymania działki w należytym stanie** - Ustawa z dnia 3 lutego 1995 r. o ochronie gruntów rolnych i leśnych (Dz. U. z 2017 r. poz. 1161); ustawa z dnia 7 lipca 2005 r. o ubezpieczeniach upraw rolnych i zwierząt gospodarskich (Dz. U. z 2017 r. poz. 2047 ze zm.); - **pobieranie od osób fizycznych opłaty rocznej z tytułu użytkowania wieczystego** - Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (j. t. Dz.U. 2018 poz. 121); - **pobieranie od osób fizycznych podatków i opłat** - Ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (j.t. Dz.U. 2017 poz. 1785 ze zmianami); - **ewidencja podatników, płatników i dłużników** - Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa, (j.t. Dz.U. 2018 poz. 800 ze zmianami), Ustawa z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (j.t. Dz.U. 2017 poz. 1785 ze zmianami), Ustawa z dnia 15 listopada 1984 r. o podatku rolnym (j.t Dz.U. 2018 poz. 928), Ustawa z dnia 30 października 2002 r. o podatku leśnym (j.t. Dz.U. 2017 poz. 1821), Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (j.t. Dz.U. 2017 poz. 1201 ze zmianami); - **ewidencja osób fizycznych prowadzących działalność gospodarczą - krajowy transport drogowy taksówką** - Ustawa z dnia 6 września 2001 r. o transporcie drogowym (j.t. Dz.U. 2017 poz. 2200 ze zmianami).; - **wydanie zezwolenia na sprzedaż napojów alkoholowych** - Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (j.t. Dz.U. 2016 poz. 487 ze zmianami); - **ewidencja osób uzależnionych** - Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (j.t. Dz. U. z 2016 r. poz. 487 ze zmianami), Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (j. t. Dz.U. 2017 poz. 783 ze zmianami); - **ewidencja obiektów hotelarskich innych** - Ustawa o usługach turystycznych (t.j. Dz.U. z 2017 r. poz. 1553 z późn. zm.);

	- **nadanie numerów porządkowych posesjom** - Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (j. t. Dz.U. 2017 poz. 2101 ze zmianami); - **wydanie decyzji o użytkowaniu wieczystym** - Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (j.t. Dz.U. 2018 poz. 121 ze zmianami). Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (j.t. Dz.U. 2017 poz. 459 ze zmianami).; - **wydanie decyzji o podziale gruntów** - Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (j. t. Dz.U. 2018 poz. 121 ze zmianami); - **wydanie decyzji o przekształceniu użytkowania wieczystego w prawo własności** - Ustawa z dnia 29 lipca 2005 r. o przekształceniu prawa użytkowania wieczystego w prawo własności nieruchomości (j. t. Dz.U. 2012 poz. 83 ze zmianami); - **wydanie decyzji o rozgraniczenie nieruchomości** - Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (j. t. Dz.U. 2017 poz. 2101 ze zmianami); - **wydanie decyzji w sprawie odszkodowania za działkę, która przeszła z mocy prawa na własność Gminy Nadarzyn** - Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (j. t. Dz.U. 2018 poz. 121 ze zmianami); - **wydanie decyzji i postanowień z zakresu urbanistyki i zagospodarowania przestrzennego** - Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (j.t. Dz.U. 2017 poz. 1073 ze zmianami); - **wypis z miejscowego planu zagospodarowania przestrzennego** - Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (j.t. Dz.U. 2017 poz. 1073 ze zmianami); - **wydanie zaświadczenia z zakresu urbanistyki i zagospodarowania przestrzennego** - Ustawa z dnia 14 czerwca 1960 r. Kodeks Postępowania Administracyjnego (j.t. Dz.U. 2017 poz. 1257 ze zmianami); - **wydanie zgody na zajęcie pasa drogowego** - Ustawa z dnia 21 marca 1985 r. o drogach publicznych (j.t. Dz.U. 2017 poz. 2222 ze zmianami), Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j Dz.U. 2017 poz. 1875 ze zmianami), Ustawa z dnia 14 czerwca 1960 r. Kodeks Postępowania Administracyjnego (j.t. Dz.U. 2017 poz. 1257 ze zmianami), Rozporządzenie Rady Ministrów z dnia 1 czerwca 2004 r. w sprawie określenia warunków udzielania zezwoleń na zajęcie pasa drogowego (j.t. Dz.U. 2016 poz. 1264).; - **wydanie Karty Nadarzyniaka** - Art. 18, ust. 2 Ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz.U. 2017 poz. 1875 ze zmianami); Uchwała Rady Gminy Nadarzyn z dnia 28 maja 2014 r., Nr XLIV/446/2014 w sprawie uchwalenia Programu Karta

	Nadarzyniaka; Uchwała Rady Gminy Nadarzyn z dnia 30 lipca 2014 r., Nr XLVI/467/2014 w sprawie zmiany uchwały Nr XLIV/446/2014 Rady Gminy Nadarzyn z dnia 28 maja 2014 r. w sprawie uchwalenia Programu Karta Nadarzyniaka; - **konkursy na stanowiska w urzędach - ewidencja osób ubiegających się o zatrudnienie** - Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (j. t. Dz.U. 2016 poz. 902 ze zmianami); - **ewidencja osób składających oświadczenia majątkowe** - Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (j. t. Dz.U. 2017 poz. 1875 ze zmianami); - **zabezpieczenie osób i mienia, pracowników oraz interesantów znajdujących się na terenie należącym do administratora danych, w tym pracownicy** - Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. 2017 poz. 2213 ze zmianami); - **ewidencja dokumentacji przekazanej do archiwum** - Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. 2011 nr 14 poz. 67); - **realizacja projektów dofinansowanych z funduszy zewnętrznych** - 1) rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego rozporządzenie Rady (WE) nr 1083/2006 (Dz. Urz. UE. L 347 z 20.12.2013, str. 320, z późn. zm.) zwanego dalej „Rozporządzeniem 1303/2013"; 2) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1304/2013 z dnia 17 grudnia 2013 r. w sprawie Europejskiego Funduszu Społecznego i uchylającego rozporządzenie Rady (WE) nr 1081/2006 (Dz. Urz. UE L 347 z 20.12.2013, str. 470) zwanego dalej „Rozporządzeniem 1304/2013"; 3) rozporządzenia delegowanego Komisji (UE) nr 480/2014 z dnia 3 marca 2014 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju

	Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego (Dz. Urz. UE L 138 z 13 maja 2014 r.) zwanego dalej „Rozporządzeniem 480/2014"; 4) rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 187/1z 26 czerwca 2014 r.); 5) rozporządzenia Komisji (UE) nr 1407/2013 z dnia 18 grudnia 2013 r. w sprawie stosowania art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej do pomocy de minimis (Dz. Urz. UE L 352/1 z dnia 24 grudnia 2013 r.); 6) rozporządzenia delegowanego Komisji (UE) nr 240/2014 z dnia 7 stycznia 2014 r. w sprawie europejskiego kodeksu postępowania w zakresie partnerstwa w ramach europejskich funduszy strukturalnych i inwestycyjnych (Dz. Urz. UE L 74/1 z dnia 14 marca 2014 r.); 7) ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 (poz. 1146, z późn. zm); 8) ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2013 r. poz. 885, z późn. zm.); 9) porozumienia w sprawie realizacji Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020 nr 1-RF/RF-II-BP/P/15/PZ z dnia 2 lipca 2015 r., zawartego pomiędzy Zarządem Województwa Mazowieckiego a Mazowiecką Jednostką Wdrażania Programów Unijnych; - **ewidencja osób, którym wydano karty przydziału do formacji Obrony Cywilnej, którym wypłaca się świadczenia rekompensujące w związku z odbytymi ćwiczeniami wojskowymi, przeznaczonych do wykonania świadczeń osobistych i rzeczowych na rzecz obrony, zwolnionych z obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny, podlegających rejestracji i zgłaszających się do kwalifikacji wojskowej** - Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (j. t. Dz.U. 2017 poz. 1430 ze zmianami); - **zamówienia publiczne** - Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (j.t. Dz.U. 2017 poz. 1579 ze zmianami). - **ewidencja sprzedaży dla celów rozliczenia podatku VAT** - Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. Z 2017 r. poz. 1221 z późn., zm.). - **udostępnianie Biuletynu Informacji Publicznej** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. z 2007 r., Nr 10 poz. 68).

Opis kategorii osób, których dane dotyczą	Rejestr korespondencji. Osoby fizyczne i prawne kierujący korespondencję do Urzędu Gminy Nadarzyn.	Nazwiska i imiona, adres zamieszkania lub pobytu, przedmiot sprawy.
	Rejestr skarg i wniosków. Osoby fizyczne i prawne składający skargi i wnioski.	Nazwiska i imiona, adres zamieszkania lub pobytu.
	Wnioski o udostępnienie informacji publicznej. Wnioskodawcy – osoby fizyczne, osoby prawne wnioskujący o udostępnienie informacji publicznej.	Nazwiska i imiona, adres zamieszkania, numer telefonu, adres e-mail, nazwa firmy, siedziba firmy.
	Zakładowy Fundusz Świadczeń Socjalnych. Osoby fizyczne, pracownicy, byli pracownicy, dzieci pracowników korzystający ze świadczeń socjalnych.	Nazwiska i imiona, PESEL, data i miejsce urodzenia, miejsce zamieszkania lub pobytu, stan cywilny, pełna informacja o rodzinie, sytuacja zawodowa pracownika, emeryta.
	Kadry, płace. Pracownicy, byli pracownicy.	Nazwiska i imiona, miejsce pracy, data urodzenia, zawód, miejsce urodzenia, wykształcenie, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer PESEL, numer telefonu, inne dane osobowe, przetwarzane w zbiorze: adres poczty elektronicznej, motywacja i zainteresowania osoby, orzeczenie o stopniu niepełnosprawności. Dane przetwarzane w zbiorze ujawniają bezpośrednio lub w kontekście stan zdrowia, orzeczenia o ukaraniu.
	Akta Urzędu Stanu Cywilnego (księgi urodzeń, zgonów, zaślubin). Mieszkańcy, wstępni, zstępni, rodzeństwo, małżonkowie, przedstawiciele ustawowi, a także osoby, które wykażą interes prawny.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego, , numer telefonu, nazwisko, imię (imiona) i płeć dziecka, miejsce i datę urodzenia dziecka, nazwiska, nazwiska rodowe rodziców, miejsce zamieszkania każdego z rodziców

		w chwili urodzenia się dziecka, płeć, nazwisko, imię i miejsce zamieszkania zgłaszającego, numer aktu urodzenia i USC sporządzającego akt, dane zawarte w zgłoszeniu urodzenia dziecka, nazwiska i imiona osób zawierających małżeństwo, nazwisko panieńskie, nazwisko z poprzedniego małżeństwa star cywilny, miejsce i datę zawarcia małżeństwa, nazwiska i imiona świadków, nazwisko (nazwiska) które będą nosić osoby zawierające małżeństwo po jego zawarciu, oraz nazwisko, które będą nosić dzieci zrodzone z tego małżeństwa, numer aktu małżeństwa i USC sporządzającego akt, informacje zawarte w zezwoleniu na zawarcie małżeństwa, godzina oraz miejsce zgonu lub znalezienia zwłok, okoliczność znalezienia zwłok, przypuszczalny rok urodzenia zmarłego, znaki szczególne zmarłego, opis odzieży oraz innych przedmiotów znalezionych przy zmarłym, nazwisko, imię (imiona) oraz nazwisko rodowe małżonka osoby zmarłej, stan cywilny, nazwiska rodowe i imiona rodziców zmarłego, nazwisko, imię (imiona) osoby zgłaszającej zgon, dane dotyczące szpitala lub zakładu, adnotacje o rozwodzie, separacji oraz o zniesieniu separacji, data rozwiązania małżeństwa, oznaczenie sądu i numer orzeczenia, data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, orzekającego przysposobienie, adopcję, data unieważnienia aktu

		małżeństwa, urodzenia, zgonu, oznaczenie sądu orzekającego oraz numer orzeczenia. Innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
	Rejestr mieszkańców. Mieszkańcy, byli mieszkańcy, osoby zameldowane na pobyt stały i czasowy, cudzoziemcy.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu , numer ewidencyjny PESEL, seria i numer dowodu osobistego, adres zameldowania, nazwiska rodowe rodziców, kraj urodzenia, stan cywilny, płeć, obywatelstwo, imię i nazwisko rodowe małżonka oraz numer PESEL jeśli był nadany.
	Zmiana imion i nazwisk. Obywatele Rzeczypospolitej Polskiej, bezpaństwowcy, jeżeli mają w RP miejsce zamieszkania, cudzoziemcy, którzy uzyskali w RP status uchodźcy. Zmiany imienia i nazwiska cudzoziemca można dokonać wyłącznie ze szczególnie ważnych powodów związanych z zagrożeniem jego prawa do życia, zdrowia, wolności lub bezpieczeństwa osobistego.	Nazwiska i imiona, PESEL jeśli został nadany, imiona rodziców, adres zamieszkania lub pobytu, nazwisko rodowe, ważne względy uzasadniające wniosek o zmianę nazwiska lub imienia, części (człony), z jakich składa się nazwisko, forma pisowni imienia lub nazwiska. Innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
	Ewidencja decyzji środowiskowych. Osoby fizyczne i prawne.	Imię, nazwisko, adres zamieszkania, nazwa firmy, siedziba firmy.
	Informacje o wyrobach zawierających azbest. Osoby fizyczne i prawne ubiegające się o dofinansowanie.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, adres działki.
	Rejestr osób składających deklaracje na wywóz odpadów komunalnych. Osoby fizyczne.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer telefonu, e-mail.
	Rejestr pozwoleń na usunięcie drzew i krzewów. Osoby fizyczne i prawne.	Imiona, nazwiska, adres zamieszkania, nazwa firmy, siedziba firmy, numer działki.

	Rejestr umów na wywóz nieczystości stałych i płynnych. Podmioty prowadzące działalność gospodarczą.	Nazwiska i imiona, adres zamieszkania lub pobytu, nazwa firmy, siedziba firmy, numer zawartej umowy.
	Ewidencja zbiorników bezodpływowych i oczyszczalni przydomowych. Osoby zobowiązane do zgłoszenia eksploatacji przydomowej oczyszczalni.	Nazwisko, imię, adres zamieszkania, adres i nr działki na której prowadzona jest eksploatacja przydomowej oczyszczalni ścieków, numer telefonu.
	Zbiór wydanych przez starostę pozwoleń o dopuszczalność emisji do środowiska. Osoby fizyczne i prawne.	Imiona, nazwiska, adres zamieszkania, nazwa firmy, siedziba firmy.
	Rejestr zezwoleń na chów psów ras niebezpiecznych dla osób postronnych. Właściciele psów.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu, metryka psa, w której podaje się imię, nazwisko i adres hodowcy.
	Rejestr decyzji wydanych do projektów robót geologicznych. Osoby fizyczne i prawne.	Imię, nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy, numer działki.
	Ewidencja podmiotów gospodarczych prowadzących działalność, w wyniku której powstają odpady niebezpieczne oraz nie zaliczone do niebezpiecznych. Osoby fizyczne i prawne.	Imię i nazwisko, adres zamieszkania, nazwa firmy, siedziba firmy, zakres działania.
	Ewidencja opłat za zmniejszoną naturalną retencję terenową. Osoby fizyczne, osoby prawne.	Imię, nazwisko, adres zamieszkania, nr telefonu.
	Postępowania w sprawie zmiany stanu wody na gruncie. Osoby fizyczne, osoby prawne.	Imię, nazwisko, adres zamieszkania, nr telefonu.
	Produkcja roślinna. Osoby fizyczne, osoby prawne.	Imię, nazwisko, adres zamieszkania, nr telefonu.
	Ewidencja opłat rocznych z tytułu użytkowania wieczystego. Osoby fizyczne.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, powierzchnia i nr działki.

	Ewidencja podatków i opłat od osób fizycznych. Osoby fizyczne, które podlegają obowiązkowi podatkowemu.	Imię i nazwisko, data urodzenia, imię ojca i matki, nr PESEL, adres zamieszkania oraz dane dotyczące nieruchomości tzn. miejsce położenia przedmiotu opodatkowania oraz nr działki, nr księgi wieczystej.
	Ewidencja podatników, płatników i dłużników. Podatnicy, płatnicy, osoby fizyczne.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, numer ewidencyjny PESEL, adres zamieszkania lub pobytu, miejsce pracy, seria i numer dowodu osobistego, księga wieczysta, numer ewid. działki, powierzchnia działki, powierzchnia budynku, dane o powierzchni lasu, nieruchomości, dochody roczne z gospodarstw rolnych, hektary przeliczeniowe, dane identyfikujące pojazd lub nieruchomość, tytuł prawny do przedmiotów opodatkowania, identyfikatory działek ewidencyjnych, dane dotyczące środków transportowych.
	Ewidencja licencji na krajowy transport drogowy taksówką. Osoby fizyczne prowadzące działalność gospodarczą.	Imię, nazwisko, adres zamieszkania, Numer Identyfikacji Podatkowej, numer Certyfikatu Kompetencji Zawodowych.
	Ewidencja zezwoleń na sprzedaż napojów alkoholowych. Wnioskodawcy ubiegający się o zezwolenie na sprzedaż napojów alkoholowych.	Nazwiska i imiona, adres zamieszkania lub pobytu, Numer Identyfikacji Podatkowej, oznaczenie rodzaju zezwolenia, oznaczenie przedsiębiorcy, jego siedzibę i adres, w przypadku stanowienia pełnomocników ich imiona, nazwiska i adres zamieszkania, przedmiot działalności gospodarczej, adres punktu sprzedaży, adres punktu składowania napojów alkoholowych (magazynu dystrybucyjnego), dokument potwierdzający tytuł prawny

		wnioskodawcy do lokalu stanowiącego punkt sprzedaży napojów alkoholowych, pisemna zgoda właściciela, użytkownika, zarządcy lub administratora budynku, jeżeli punkt sprzedaży będzie zlokalizowany w budynku mieszkalnym wielorodzinnym.
	Uzależnienia. Osoby uzależnione.	Nazwiska i imiona, adres zamieszkania, informacje dotyczące członków rodziny osoby uzależnionej, nałogi.
	Ewidencja obiektów hotelarskich innych. Osoby fizyczne.	Imię i nazwisko, miejsce zamieszkania, nazwa obiektu jeżeli usługi będą świadczone z użyciem nazwy własnej, położenie wraz z podaniem jego adresu.
	Ewidencja nadanych numerów porządkowych posesjom. Osoby fizyczne i prawne.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, położenie działki.
	Ewidencja użytkowników wieczystych. Osoby fizyczne i prawne będące użytkownikami wieczystymi.	Imię, nazwisko, adres zamieszkania, data urodzenia, PESEL, imiona rodziców, miejsce urodzenia, numer dowodu osobistego, siedziba firmy, NIP, Regon, numer księgi wieczystej, numer aktu własności, numer działki, położenie działki, powierzchnia działki.
	Ewidencja wydanych decyzji podziału gruntów. Osoby fizyczne i prawne.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, powierzchnia działki, położenie działki.
	Ewidencja wydanych decyzji przekształcenia prawa użytkowania wieczystego w prawo własności. Osoby fizyczne będące użytkownikami wieczystymi.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu, numer działki, położenie działki, powierzchnia działki.
	Ewidencja wydanych decyzji w sprawie rozgraniczenia nieruchomości. Osoby fizyczne i prawne	Nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer działki, położenie działki, powierzchnia działki.

	Ewidencja wydanych decyzji w sprawie odszkodowania za działkę, która przeszła z mocy prawa na własność gminy. Osoby fizyczne i prawne.	Nazwiska i imiona, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu, numer działki, położenie działki, powierzchnia działki.
	Rejestr decyzji i postanowień z zakresu urbanistyki i zagospodarowania przestrzennego. Osoby fizyczne i prawne wnioskujące o wydanie decyzji i postanowienia	Imię i nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy, położenie działki, numer działki.
	Rejestr wypisów z miejscowego planu zagospodarowania przestrzennego. Osoby fizyczne i prawne wnioskujące o wypis.	Imię i nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy.
	Rejestr zaświadczeń z zakresu urbanistyki i zagospodarowania przestrzennego. Osoby fizyczne i prawne wnioskujące o wydanie zaświadczenia.	Imię i nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy, położenie działki, numer działki.
	Sprawy dotyczące pasa drogowego. Osoby występujące o zajęcie pasa drogowego.	Nazwiska i imiona, adres zamieszkania lub pobytu, cel zajęcia pasa drogowego, powierzchnia zajmowanego pasa drogowego lub powierzchnia reklamy, okres zajęcia pasa drogowego, wysokość opłaty za zajęcie pasa drogowego oraz sposób jej uiszczania, sposób zabezpieczenia zajmowanego pasa drogowego, warunki przywracania pasa drogowego do poprzedniego stanu użyteczności, zakres i technologia robót przywracających stan użyteczności, sposób odbioru przedmiotowego odcinka pasa drogowego, zasady usuwania usterek i wad technicznych.

	Karta Nadarzyniaka. Osoby fizyczne – mieszkańcy gminy, którzy ukończyli 18 lat.	Imię, nazwisko, adres zamieszkania, Nr PESEL, adres e-mail, nr telefonu.
	Konkursy na stanowiska w urzędach. Osoby ubiegające się o zatrudnienie.	Nazwiska i imiona, miejsce pracy, data urodzenia, zawód, miejsce urodzenia, wykształcenie, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer PESEL, numer telefonu, inne dane osobowe, przetwarzane w zbiorze: adres poczty elektronicznej, motywacja i zainteresowania osoby, orzeczenie o stopniu niepełnosprawności. Dane przetwarzane w zbiorze ujawniają bezpośrednio lub w kontekście stan zdrowia, orzeczenia o ukaraniu.
	Oświadczenia majątkowe. Radni Gminy. Pracownicy.	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, miejsce urodzenia, miejsce pracy, zawód, posiadane zasoby pieniężne, posiadane nieruchomości, posiadane udziały w spółkach, posiadane akcje w spółkach, działalność gospodarcza, funkcje w spółkach, inne dochody, składniki mienia ruchomego o wartości powyżej 10 000 PLN, zobowiązania pieniężne o wartości powyżej 10 000 PLN.
	Zbiór danych osobowych z monitoringu wizyjnego w Urzędzie Gminy Nadarzyn. Wszystkie osoby znajdujące się na terenie należącym do administratora danych, w tym pracownicy i interesanci.	Wizerunek.
	Archiwum. Interesanci.	Nazwiska i imiona, adresy zamieszkania, przedmiot sprawy.
	Realizacja projektów dofinansowania z funduszy zewnętrznych. Osoby fizyczne, uczniowie i pracownicy jednostek organizacyjnych biorących udział w projektach dofinansowanych z funduszy zewnętrznych.	Imię, nazwisko, płeć, wiek w chwili przystąpienia do projektu, PESEL, wykształcenie, potwierdzenie bądź zaprzeczenie zatrudnienia, potwierdzenie bądź zaprzeczenie niepełnosprawności adres zamieszkania, telefon, adres poczty elektronicznej.

	Sprawy obronne. Osoby, którym wydano karty przydziału do formacji Obrony Cywilnej, którym wypłaca się świadczenia rekompensujące w związku z odbytymi ćwiczeniami wojskowymi, które przeznaczono do wykonania świadczeń osobistych i rzeczowych na rzecz obrony, które są zwolnione z obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny, podlegające rejestracji i zgłaszające się do kwalifikacji wojskowej.	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, miejsce urodzenia, kategoria zdolności do czynnej służby wojskowej, stopień, wojskowy, specjalność wojskowa, adres siedziby firmy, numer rejestracyjny pojazdu, marka pojazdu, numer książeczki wojskowej.
	Zamówienia publiczne. Zamawiający, wykonawcy i inni uczestnicy postępowania o udzielenie zamówień publicznych.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, informacje na temat przeciętnej liczby zatrudnionych pracowników oraz liczebności personelu kierowniczego, wykaz niezbędnych do wykonania zamówienia narzędzi i urządzeń, jakie posiada wykonawca, wykaz osób i podmiotów, które będą wykonywać zamówienie lub będą uczestniczyć w wykonywaniu zamówienia, wraz z informacjami na temat ich kwalifikacji niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nich czynności, wykaz wykonanych w okresie ostatnich pięciu lat robót budowlanych, wykaz wykonanych w okresie ostatnich trzech lat dostaw lub usług, informacje banku, w którym wykonawca posiada podstawowy rachunek

		bankowy, potwierdzające wysokość posiadanych środków finansowych lub zdolność kredytową wykonawcy, polisa lub inny dokument ubezpieczenia potwierdzające, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej, koncesje, zezwolenia lub licencje, aktualne zaświadczenia właściwego naczelnika urzędu skarbowego oraz właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające odpowiednio, że wykonawca nie zalega z opłacaniem podatków, opłat oraz składek na ubezpieczenie zdrowotne lub społeczne, lub zaświadczenia, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu, dokumenty stwierdzające, że osoby, które będą wykonywać zamówienie, posiadają wymagane uprawnienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień, dane dotyczące skazań.
	Ewidencja sprzedaży dla celów rozliczenia podatku VAT. Osoby fizyczne.	Imiona, nazwiska, adres zamieszkania lub pobytu, NIP.
	Biuletyn Informacji Publicznej. Pracownicy administratora, klienci, kontrahenci, odbiorcy korespondencji administratora.	Imiona, nazwiska, nazwa stanowiska, numer telefonu.
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione	Dane będą udostępniane na każdorazowo uzasadniony wniosek odbiorcy. Odbiorcą będą organy publiczne, jednostki które mogą otrzymywać dane w ramach wypełniania obowiązku ustawowego.	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w państwach trzecich	**nie dotyczy**	

Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych	**nie dotyczy**	
Planowane terminy usunięcia poszczególnych kategorii danych	Dane osobowe będą przechowywane przez czas określony w szczegółowych przepisach prawa.	
Opis środków bezpieczeństwa	techniczne	organizacyjne
	Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) w zamkniętych nie metalowych szafach. Kopie zapasowe (archiwalne) przechowywane są w zamkniętym sejfie lub kasie pancernej. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek. Zastosowano urządzenia typu UPS i wydzieloną sieć elektroenergetyczną, chroniącą system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatorów i haseł. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł. Zastosowano system rejestracji dostępu do zbiorów danych osobowych. Zastosowano środki ochrony przed szkodliwym oprogramowaniem. Wdrożono urządzenie UTM (Unified Threat Management) do ochrony dostępu do sieci komputerowej. Zastosowano systemowe środki pozwalające na określenie	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco. Zastosowano środki bezpieczeństwa na poziomie wysokim.

	odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	

Administrator Danych Osobowych

WÓJT GMINY

.....Dariusz Żywiński.....

GMINA NADARZYN
ul. Mszczonowska 24, 05-830 Nadarzyn
NIP: 534-22-54-841
tel. 22 729-81-85

REJESTR CZYNNOŚCI PRZETWARZANIA

SWO.142.4.2018.WS

Imię i nazwisko lub nazwa administratora ..... **Gmina Nadarzyn**

Dane kontaktowe administratora ..... **ul. Mszczonowska 24, 05-830 Nadarzyn, tel. 22 729 81 85, fax. 22 729 81 75**

Dane współadministratorów ..... **nie dotyczy**

Dane inspektora ochrony danych ..... **Wiesław Sobczyński, wsobczynski@nadarzyn.pl, tel. 22 729 81 85 wew. 197**

Cel przetwarzania	Celem przetwarzania danych jest wypełnienie obowiązków określonych w przepisach prawa: **Ewidencja przedstawicieli Wójta Gminy Nadarzyn do sprawowania stałego, zewnętrznego dozoru lokali wyborczych –** Rozporządzenie Ministra Spraw Wewnętrznych z dnia 28 sierpnia 2014 r. w sprawie szczegółowych wymagań w zakresie ochrony lokali obwodowych komisji wyborczych w czasie przerwy w głosowaniu, spowodowanej nadzwyczajnymi wydarzeniami (Dz. U. z 2014 r., poz. 1152).	
Opis kategorii osób, których dane dotyczą	Przedstawiciele Wójta Gminy Nadarzyn do sprawowania stałego, zewnętrznego dozoru lokali wyborczych.	Imiona, nazwiska, adresy zamieszkania, numery dowodów osobistych, numery telefonów.
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione	Dane będą udostępniane na każdorazowo uzasadniony wniosek odbiorcy. Odbiorcą będą organy publiczne, jednostki które mogą otrzymywać dane w ramach wypełniania obowiązku ustawowego.	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w państwach trzecich	**nie dotyczy**	

Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych	**nie dotyczy**	
Planowane terminy usunięcia poszczególnych kategorii danych	Dane osobowe będą przechowywane przez czas określony w szczegółowych przepisach prawa.	
Opis środków bezpieczeństwa	techniczne	organizacyjne
	Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) w zamkniętych nie metalowych szafach. Kopie zapasowe (archiwalne) przechowywane są w zamkniętym sejfie lub kasie pancernej. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek. Zastosowano urządzenia typu UPS i wydzieloną sieć elektroenergetyczną, chroniącą system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatorów i haseł. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł. Zastosowano system rejestracji dostępu do zbiorów danych osobowych. Zastosowano środki ochrony przed szkodliwym	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco. Zastosowano środki bezpieczeństwa na poziomie wysokim.

	oprogramowaniem. Wdrożono urządzenie UTM (Unified Threat Management) do ochrony dostępu do sieci komputerowej. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	

Administrator Danych Osobowych

Z up. Wójta Gminy
ZASTĘPCA WÓJTA

.....

mgr inż. Janusz Rajkowski

Nadarzyn, 13.02.2019 r.

REJESTR CZYNNOŚCI PRZETWARZANIA

SWO.142.1.2019.WS

Gmina Nadarzyn

Imię i nazwisko lub nazwa administratora .....

ul. Mszczonowska 24, 05-830 Nadarzyn, tel. 22 729 81 85, fax. 22 729 81 75

Dane kontaktowe administratora .....

nie dotyczy

Dane współadministratorów .....

Wiesław Sobczyński, wsobczynski@nadarzyn.pl, tel. 22 729 81 85 wew. 197

Dane inspektora ochrony danych .....

Cel przetwarzania	Celem przetwarzania danych jest wypełnienie obowiązków określonych w przepisach prawa: **Wydawanie zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów** – Ustawa z dnia 20 lipca 2018 r. o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów (Dz. U. z 2018r., poz. 1716 z późn. zm.)	
Opis kategorii osób, których dane dotyczą	Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów. Osoby fizyczne.	Imiona, nazwiska , adres zamieszkania, numer księgi wieczystej, numer ewidencyjny działki.
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione	Dane będą udostępniane na każdorazowo uzasadniony wniosek odbiorcy. Odbiorcą będą organy publiczne, jednostki które mogą otrzymywać dane w ramach wypełniania obowiązku ustawowego.	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w państwach trzecich	**nie dotyczy**	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych	**nie dotyczy**	

Planowane terminy usunięcia poszczególnych kategorii danych	Dane osobowe będą przechowywane przez czas określony w szczegółowych przepisach prawa.	
Opis środków bezpieczeństwa	techniczne	organizacyjne
	Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) w zamkniętych nie metalowych szafach. Kopie zapasowe (archiwalne) przechowywane są w zamkniętym sejfie lub kasie pancernej. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek. Zastosowano urządzenia typu UPS i wydzieloną sieć elektroenergetyczną, chroniącą system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatorów i haseł. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł. Zastosowano system rejestracji dostępu do zbiorów danych osobowych. Zastosowano środki ochrony przed szkodliwym oprogramowaniem. Wdrożono urządzenie UTM (Unified Threat Management) do ochrony dostępu do sieci komputerowej. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco. Zastosowano środki bezpieczeństwa na poziomie wysokim.

	zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	

Administrator Danych Osobowych

WÓJT GMINY

.....Dariusz Zwolinski.....

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

REJESTR CZYNNOŚCI PRZETWARZANIA

SWO.142.3.2020.WS

Gmina Nadarzyn

Imię i nazwisko lub nazwa administratora .....

ul. Mszczonowska 24, 05-830 Nadarzyn, tel. 22 729 81 85, fax. 22 729 81 75

Dane kontaktowe administratora .....

nie dotyczy

Dane współadministratorów .....

Wiesław Sobczyński, wsobczynski@nadarzyn.pl, tel. 22 729 81 85 wew. 197

Dane inspektora ochrony danych .....

Cel przetwarzania	Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych oraz do wykonania zadania realizowanego w interesie publicznym: **Nabór kandydatów na rachmistrzów** - art. 20 ustawy z dnia 31 lipca 2019 r. o powszechnym spisie rolnym w 2020 r. (Dz. U. z 2019 r. poz. 1728).	
Opis kategorii osób, których dane dotyczą	Kandydaci na rachmistrza spisowego	Nazwisko i imię (imiona); adres zamieszkania; nr telefonu, adres e-mail; data urodzenia; wykształcenie
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione	Dane będą udostępniane na każdorazowo uzasadniony wniosek odbiorcy. Odbiorcą będą organy publiczne, jednostki które mogą otrzymywać dane w ramach wypełniania obowiązku ustawowego.	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w państwach trzecich	**nie dotyczy**	
Kategorie odbiorców, którym dane zostały lub zostaną ujawnione w organizacjach międzynarodowych	**nie dotyczy**	
Planowane terminy usunięcia poszczególnych kategorii danych	Dane osobowe będą przechowywane przez czas określony w szczegółowych przepisach prawa.	

Opis środków bezpieczeństwa	techniczne	organizacyjne
	Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) w zamkniętych nie metalowych szafach. Kopie zapasowe (archiwalne) przechowywane są w zamkniętym sejfie lub kasie pancernej. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek. Zastosowano urządzenia typu UPS i wydzieloną sieć elektroenergetyczną, chroniącą system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatorów i haseł. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł. Zastosowano system rejestracji dostępu do zbiorów danych osobowych. Zastosowano środki ochrony przed szkodliwym oprogramowaniem. Wdrożono urządzenie UTM (Unified Threat Management) do ochrony dostępu do sieci komputerowej. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco. Zastosowano środki bezpieczeństwa na poziomie wysokim.

	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	

Administrator Danych Osobowych

Dariusz Zyskowski

.....

GMINA NADARZYN
ul. Mszczonowska 24, 05-830 Nadarzyn
NIP: 534-22-54-841
tel. 22 729-81-85

SWO.142.3.2018.WS

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	GMINA NADARZYN
Adres	ul. Mszczonowska 24, 05-830 Nadarzyn
Email	gmina@nadarzyn.pl
Telefon	22 729 81 85

Inspektor Ochrony Danych	
Nazwa	Wiesław Sobczyński
Adres	ul. Mszczonowska 24, 05-830 Nadarzyn
Email	wsobczynski@nadarzyn.pl
Telefon	500 091 842

LP.	Cel przetwarzania powierzonych Danych	Kategorie osób, których dotyczą Dane i rodzaj powierzonych Danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Charakter przetwarzania	Miejsce przetwarzania Danych	Administrator Danych Osobowych Nazwa i dane kontaktowe administratora	Czas trwania przetwarzania
1	2	3	4	5	6	7	8
1.	Powierzone Dane będą przetwarzane przez Podmiot Przetwarzający w następujących celach: a)przekazanie deklaracji do OPL	Zbiór Danych Abonentów Usług Telekomunikacyjnych Orange Polska S.A. Administrator powierza Podmiotowi Przetwarzającemu do przetwarzania następujące rodzaje danych osobowych: a) imię i nazwisko, b) miejscowość, c) kod pocztowy, d) ulica, e) numer domu, f) pesel, g) numer telefonu, h) adres e-mail.	Podmiot Przetwarzający zapewnia bezpieczeństwo Danych stosując środki organizacyjne i techniczne mające na celu należyte zabezpieczenie Danych, odpowiednie do zagrożeń oraz kategorii powierzonych Danych, w szczególności zobowiązuje się zabezpieczyć Dane przed ich ujawnieniem osobom nieupoważnionym lub dostępem do nich osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem z	Przetwarzanie przez Podmiot Przetwarzający będzie miało następujący charakter: - częściowo zautomatyzowany i/lub manualny, -przetwarzanie nie będzie obejmowało profilowania. W ramach przetwarzania Danych Podmiot Przetwarzający nie będzie komunikował się w imieniu Administratora bezpośrednio z osobami, których Dane dotyczą.	Powierzone Dane będą przez Podmiot Przetwarzający przetwarzane w 05-830 Nadarzyn, ul. Mszczonowska 24. Powierzone Dane będą przetwarzane przez Podmiot Przetwarzający w systemie teleinformatycznym stanowiącym własność Orange Polska S.A., Dane będą przetwarzane w następujących systemach teleinformatycznych Orange Polska: ,,Włącz się'' Podmiot Przetwarzający nie jest upoważniony do przetwarzania Danych poza Europejskim Obszarem Gospodarczym.	Orange Polska Spółka Akcyjna, z siedzibą w Warszawie Al. Jerozolimskie 160 02-326 Warszawa	Na podstawie Postanowień Podmiot Przetwarzający będzie przetwarzać powierzone Dane przez czas trwania Umowy lub przez czas niezbędny do realizacji celu powierzenia przetwarzania Danych, w zależności od tego, który z tych terminów upłynie jako pierwszy, a w przypadku określonym w ust. 13 pkt. 2 - wyłącznie przez okres niezbędny do usunięcia lub wydania Administratorowi Danych. W trakcie trwania Umowy Administrator poprzez Koordynatora może wskazywać Podmiotowi Przetwarzającemu inne lub dodatkowe instrukcje dotyczące okresu przetwarzania Danych niż wskazane wyżej, w szczególności w sytuacjach związanych z koniecznością usunięcia lub ograniczenia przetwarzania tych Danych.

			naruszeniem aktualnie obowiązujących przepisów prawa w zakresie przetwarzania danych osobowych, zmianą, utratą, uszkodzeniem). m.in. poprzez zapewnienie: 1.zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, 2.zdolności do szybkiego przywrócenia dostępności Danych i dostępu do nich w razie incydentu fizycznego lub technicznego, 3.regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i		O planowanym użyciu innych systemów teleinformatycznych, które nie stanowią własności Podmiotu Przetwarzającego, Podmiot Przetwarzający poinformuje Administratora z wyprzedzeniem 5 dni roboczych. Taka zmiana będzie wymagała akceptacji Administratora. W szczególności Administrator, jeśli uzna, że zmiany planowane przez Podmiot Przetwarzający mogą wpływać w istotny sposób na przetwarzanie Danych, może przeprowadzić ocenę ryzyka takiej zmiany (w tym przeprowadzić ocenę skutków dla ochrony Danych) i w razie stwierdzenia, że planowane przetwarzanie powodowałoby wysokie ryzyko,		

			organizacyjnych mających zapewnić bezpieczeństwo przetwarzania		gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, Administrator może nie zgodzić się na planowane przez Podmiot Przetwarzający zmiany.		

Przetwarzający Dane

Z up. Wójta Gminy
ZASTĘPCA WÓJTA
mgr inż. Janusz Rajkowski

Wykonał: Wiesław Sobczyński

22 729 81 85 w. 197

Załącznik Nr 12 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

....., dnia .....

.....

.....

Dane osoby wnoszącej o sprostowanie

Rada Gminy Nadarzyn

ul. Mszczonowska 24, 05-830 Nadarzyn

Wniosek o sprostowanie danych osobowych

Na podstawie art. 16 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (DZ. U. UE. z 2016 r., L119/1), zwracam się do administratora danych osobowych z żądaniem **sprostowania moich danych**

w zakresie :

.....

.....

Jednocześnie oświadczam, że podane dane są prawdziwe i jestem świadoma/my odpowiedzialności karnej za złożenie fałszywego oświadczenia*.

.....

Podpis osoby składającej wniosek

* Kto, składając zeznanie mające służyć za dowód w postępowaniu sądowym lub w innym postępowaniu prowadzonym na podstawie ustawy, zeznaje nieprawdę lub zataja prawdę, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. (Art. 233. § 1 U stawy z dnia 6 czerwca 1997 r. Kodeks karny). Przepisy § 1 stosuje się odpowiednio do osoby, która składa fałszywe oświadczenie, jeżeli przepis ustawy przewiduje możliwość odebrania oświadczenia pod rygorem odpowiedzialności karnej (Art. 233. § 6)

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

Załącznik Nr 13 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

SWO.142.1.2019.WS

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

L. p.	Nazwa zbioru danych osobowych	Numer pomieszczenia	Kondygnacja	Uwagi
1.	Rejestr korespondencji	100, 200	parter, I piętro	
2.	Ewidencja licencji na krajowy transport drogowy taksówką	104, 105,106	parter	
3.	Ewidencja zezwoleń na sprzedaż napojów alkoholowych	104, 105,106	parter	
4.	Uzależnienia	104, 105,106	parter	
5.	Ewidencja obiektów hotelarskich innych	104, 105,106	parter	
6.	Wnioski o udostępnienie informacji publicznej	104, 105,106	parter	
7.	Karta Nadarzyniaka	107, 108, 109	parter	
8.	Sprawy obronne	107, 108, 109	parter	
9.	Przedstawiciele Wójta Gminy Nadarzyn do sprawowania stałego, zewnętrznego dozoru lokali wyborczych	107, 108, 109		
10.	Monitoring wizyjny	107, 108, 109	parter	
11.	Wnioski o udostępnienie informacji publicznej	107, 108, 109	parter	
12.	Ewidencja nadanych numerów porządkowych posesjom	110, 111, 112, 113, 114	parter	
13.	Ewidencja użytkowników wieczystych	110, 111, 112, 113, 114	parter	
14.	Ewidencja wydanych decyzji podziału gruntów	110, 111, 112, 113, 114	parter	
15.	Ewidencja wydanych decyzji przekształcenia prawa użytkowania wieczystego w prawo własności	110, 111, 112, 113, 114	parter	

16.	Ewidencja wydanych decyzji w sprawie rozgraniczenia nieruchomości	110, 111, 112, 113, 114	parter	
17.	Ewidencja wydanych decyzji w sprawie odszkodowania za działkę, która przeszła z mocy prawa na własność gminy	110, 111, 112, 113, 114	parter	
18.	Rejestr decyzji i postanowień z zakresu urbanistyki i zagospodarowania przestrzennego	110, 111, 112, 113, 114	parter	
19.	Rejestr wypisów z miejscowego planu zagospodarowania przestrzennego	110, 111, 112, 113, 114	parter	
20.	Rejestr zaświadczeń z zakresu urbanistyki i zagospodarowania przestrzennego	110, 111, 112, 113, 114	parter	
21.	Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów	110, 111, 112, 113, 114	parter	
22.	Wnioski o udostępnienie informacji publicznej	110, 111, 112, 113, 114	parter	
23.	Monitoring wizyjny	124	parter	
24.	Rejestr skarg i wniosków do Biura Rady Gminy	130,131, 132, 134	parter	
25.	Oświadczenia majątkowe radnych	130,131, 132, 134	parter	
26.	Archiwum	130,131, 132, 134	parter	
27.	Wnioski o udostępnienie informacji publicznej	130,131, 132, 134	parter	
28.	Rejestr skarg i wniosków do Wójta Gminy	201	I piętro	
29.	Oświadczenia majątkowe	201	I piętro	
30.	Wnioski o udostępnienie informacji publicznej	201	I piętro	
31.	Rekrutacja i konkursy na stanowiska	205	I piętro	
32.	Wnioski o udostępnienie informacji publicznej	205	I piętro	
33.	Kadry, płace	202, 203, 204, 210	I piętro	
34.	Zakładowy Fundusz Świadczeń Socjalnych	202, 203, 204, 210	I piętro	
35.	Ewidencja sprzedaży dla celów rozliczenia podatku VAT	202, 203, 204, 210	I piętro	
36.	Ewidencja opłat rocznych z tytułu użytkowania wieczystego	206, 207, 208, 209	I piętro	
37.	Ewidencja podatków i opłat od osób fizycznych	206, 207, 208, 209	I piętro	
38.	Ewidencja podatników, płatników i dłużników	206, 207, 208, 209	I piętro	

39.	Wnioski o udostępnienie informacji publicznej	206, 207, 208, 209	I piętro	
40.	Ewidencja decyzji środowiskowych	222, 223, 224, 228	I piętro	
41.	Informacje o wyrobach zawierających azbest	222, 223, 224, 228	I piętro	
42.	Rejestr osób składających deklaracje na wywóz odpadów komunalnych	222, 223, 224, 228	I piętro	
43.	Rejestr pozwoleń na usunięcie drzew i krzewów	222, 223, 224, 228	I piętro	
44.	Rejestr umów na wywóz nieczystości stałych i płynnych	222, 223, 224, 228	I piętro	
45.	Ewidencja zbiorników bezodpływowych i oczyszczalni przydomowych	222, 223, 224, 228	I piętro	
46.	Zbiór wydanych przez starostę pozwoleń o dopuszczalność emisji do środowiska	222, 223, 224, 228	I piętro	
47.	Rejestr zezwoleń na chów psów ras niebezpiecznych dla osób postronnych	222, 223, 224, 228	I piętro	
48.	Rejestr decyzji wydanych do projektów robót geologicznych	222, 223, 224, 228	I piętro	
49.	Ewidencja podmiotów gospodarczych prowadzących działalność, w wyniku której powstają odpady niebezpieczne oraz nie zaliczone do niebezpiecznych	222, 223, 224, 228	I piętro	
50.	Ewidencja opłat za zmniejszoną naturalną retencję terenową	222, 223, 224, 228	I piętro	
51.	Postępowania w sprawie zmiany stanu wody na gruncie	222, 223, 224, 228	I piętro	
52.	Produkcja roślinna	222, 223, 224, 228	I piętro	
53.	Wnioski o udostępnienie informacji publicznej	222, 223, 224, 228	I piętro	
54.	Akta Urzędu Stanu Cywilnego (księgi urodzeń, zgonów, zaślubin)	222, 223, 224, 228	I piętro	
55.	Rejestr mieszkańców	225, 226	I piętro	
56.	Zmiana imion i nazwisk	225, 226	I piętro	
57.	Wnioski o udostępnienie informacji publicznej	225, 226	I piętro	
58.	Zamówienia publiczne	232, 229, 230	I piętro	
59.	Realizacja projektów dofinansowania z funduszy zewnętrznych	232	I piętro	
60.	Wnioski o udostępnienie informacji publicznej	232	I piętro	
61.	Sprawy dotyczące pasa drogowego	229, 230	I piętro	
62.	Wnioski o udostępnienie informacji publicznej	238, 239	I piętro	
63.	Wnioski o udostępnienie informacji publicznej	240	I piętro	

Administrator Danych Osobowych

WÓJT GMINY

.....

Dariusz Żwoliński

Wykonał: W. Sobczyński

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

SWO.142.1.2019.WS

Załącznik Nr 13 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

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

L. p.	Nazwa zbioru danych osobowych	Nazwa i numer pomieszczenia	Kondygnacja	Uwagi
1.	Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów.	Referat Geodezji i Gospodarki Przestrzennej– 110, 111, 112, 113, 114	parter	

Administrator Danych Osobowych

WÓJT GMINY

.....

Dariusz [illegible]ński

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn

SWO.142.1.2019.WS

Załącznik Nr 14 do Polityki Bezpieczeństwa Przetwarzania Danych Osobowych

Wykaz zbiorów danych osobowych

Lp.	Nazwa zbioru danych osobowych	Programy zastosowane do przetwarzania	Lokalizacja zbioru/ miejsce przetwarzania danych
1	1) Rejestr korespondencji.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL.	Kancelaria – 100; Sekretariat – 200
2	2) Ewidencja licencji na krajowy transport drogowy taksówką; 3) Ewidencja zezwoleń na sprzedaż napojów alkoholowych; 4) Uzależnienia; 5) Ewidencja obiektów hotelarskich innych.	EZD; CEIDG; EWIDENCJA DZIAŁALNOŚCI GOSPODARCZEJ; zezwolenia na sprzedaż napojów alkoholowych; licencje na taxi; rejestr innych obiektów hotelarskich; zezwolenia na transport drogowy osób; KONTO UŻYTKOWNIKA, KONTO EMAIL.	Referat Działalności Gospodarczej – 104, 105,106
3	6) Karta Nadarzyniaka; 7) Przedstawiciele Wójta Gminy Nadarzyn do sprawowania stałego, zewnętrznego dozoru lokali wyborczych. 8) Sprawy obronne. 9) Monitoring wizyjny	EZD; 4 SECID; 4 SECID_ZTM; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Organizacyjny– 107, 108, 109
4	10) Ewidencja nadanych numerów porządkowych posesjom; 11) Ewidencja użytkowników wieczystych; 12) Ewidencja wydanych decyzji podziału gruntów; 13) Ewidencja wydanych decyzji przekształcenia prawa użytkowania wieczystego w prawo własności; 14) Ewidencja wydanych decyzji w sprawie rozgraniczenia nieruchomości; 15) Ewidencja wydanych decyzji w sprawie odszkodowania za działkę, która przeszła z mocy prawa na własność gminy; 16) Rejestr decyzji i postanowień z zakresu urbanistyki i zagospodarowania przestrzennego; 17) Rejestr wypisów z miejscowego planu zagospodarowania przestrzennego;	EZD; EWOPIS;EWMAPA; EDOŚ; GROSZEK - UŻYTKOWANIE; GEO-SYSTEM; NUMERACJA PORZĄDKOWA; Kszob; Dzierżawy; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Geodezji i Gospodarki Przestrzennej– 110, 111, 112, 113, 114

	18) Rejestr zaświadczeń z zakresu urbanistyki i zagospodarowania przestrzennego; 19) Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów.	GEO-SYSTEM-MIENIE;	
5	20) Zbiór danych osobowych z monitoringu wizyjnego w Urzędzie Gminy Nadarzyn.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Organizacyjny– 107, 108, 109;
		Wgląd	Portier/Monitoring/Pomieszczenie do przechowywania kluczy zapasowych – 124
6	21) Rejestr skarg i wniosków do Biura Rady Gminy; 22) Oświadczenia majątkowe Radnych; 23) Archiwum.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL	Biuro Rady Gminy i Archiwum – 130,131, 132, 134
7	24) Rejestr skarg i wniosków do Wójta Gminy; 25) Oświadczenia majątkowe pracowników.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL	Sekretarz Gminy – 201
8	26) Konkursy na stanowiska w urzędach; 27) Kadry, płace;	EZD; Kadry Płace; Płatnik; Stare Kadry; KONTO UŻYTKOWNIKA, KONTO EMAIL	Samodzielne Stanowisko ds. Kadrowych – 205
9	28) Zakładowy Fundusz Świadczeń Socjalnych; 29) Kadry, płace; 30) Ewidencja sprzedaży dla celów rozliczenia podatku VAT.	EZD; beSTi@ ;Kadry Płace; Kszob eBank Biznes; PFRON; płatnik płace stare; Bank; Rejestr VAT KASA; KONTO; KSIĘGOWOŚĆ BUDŻETOWA; KONTO; DocuSafe UPK; K i P-TENSOFT, KADRY i PŁACE – INFOSYSTEM ; ŚRODKI TRWAŁE; BANKOWOŚĆ ELEKTRONICZNA; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Realizacji Budżetu – 202, 203, 204, 210
10	31) Ewidencja opłat rocznych z tytułu użytkowania wieczystego; 32) Ewidencja podatków i opłat od osób fizycznych; 33) Ewidencja podatników, płatników i dłużników.	EZD; księgowość budżetowa; BeSTi@; podatki; EWOPIS KASA; PODATKI, OPŁATY LOKALNE, KSIĘGOWOŚĆ ZOBOWIĄZAŃ., W. UŻYTKOWANIE; E-MANDAT – WINDYKACJA; AUTA-OS. FIZYCZNE I PRAWNE (JGU); KONTO UŻYTKOWNIKA, KONTO EMAIL; KSZOb; BUDŻET; GOMIG; UPK I KSIĘGOWOŚĆ JGU; EGZEKUCJA	Referat Realizacji Podatków i Opłat – 206, 207, 208, 209

11	34) Akta Urzędu Stanu Cywilnego (księgi urodzeń, zgonów, zaślubin); 35) Rejestr mieszkańców; 36) Zmiana imion i nazwisk.	EZD; USC WIN;SELWIN;SWDO; EWOPIS; Rejestry: dowodów osobistych, PESEL, mieszkańców, zamieszkania cudzoziemców; KONTO UŻYTKOWNIKA, KONTO EMAIL	Urząd Stanu Cywilnego – 225, 226
12	37) Realizacja projektów dofinansowania z funduszy zewnętrznych.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL;EWOPIS;EWMAPA; MEWA.SI2014, UZP, UPUE;	Referat Zamówień Publicznych i Funduszy Zewnętrznych – 232
13	38) Ewidencja decyzji środowiskowych; 39) Informacje o wyrobach zawierających azbest; 40) Rejestr osób składających deklaracje na wywóz odpadów komunalnych; 41) Rejestr pozwoleń na usunięcie drzew i krzewów; 42) Rejestr umów na wywóz nieczystości stałych i płynnych; 43) Ewidencja zbiorników bezodpływowych i oczyszczalni przydomowych; 44) Zbiór wydanych przez starostę pozwoleń o dopuszczalność emisji do środowiska; 45) Rejestr zezwoleń na chów psów ras niebezpiecznych dla osób postronnych; 46) Rejestr decyzji wydanych do projektów robót geologicznych; 47) Ewidencja podmiotów gospodarczych prowadzących działalność, w wyniku której powstają odpady niebezpieczne oraz nie zaliczone do niebezpiecznych; 48) Ewidencja opłat za zmniejszoną naturalną retencję terenową; 49) Postępowania w sprawie zmiany stanu wody na gruncie; 50) Produkcja roślinna;	EZD; EWOPIS;EWMAPA; GOMIG; TAXI+; KSZOB; EDOŚ; OPŁATY LOKALNE; bazaazbestowa; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Rolnictwa, Ochrony Środowiska i Gospodarki – 222, 223, 224, 228
14	51) Zamówienia publiczne.	EZD; EWOPIS;EWMAPA; MEWA.SI2014, UZP, UPUE; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Inwestycji – 229, 230; Referat Zamówień Publicznych i Funduszy Zewnętrznych – 232
15	52) Sprawy dotyczące pasa drogowego.	EZD; EWOPIS; EWMAPA; KSzob-Opłaty lokalne; NORMA; ePODGiK, KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Inwestycji – 229, 230

16	53) Wnioski o udostępnienie informacji publicznej.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL.	Referat Działalności Gospodarczej – 104, 105,106; Referat Geodezji i Gospodarki Przestrzennej– 110, 111, 112, 113, 114; Referat Organizacyjny– 107, 108, 109; Biuro Rady Gminy i Archiwum – 130,131, 132, 134; Sekretarz Gminy – 201; Samodzielne Stanowisko ds. Kadrowych – 205; Referat Realizacji Budżetu – 202, 203, 204, 210; Referat Realizacji Podatków i Opłat – 206, 207, 208, 209; Urząd Stanu Cywilnego – 225, 226; Referat Zamówień Publicznych i Funduszy Zewnętrznych – 232; Referat Rolnictwa, Ochrony Środowiska i Gospodarki – 222, 223, 224, 228; Referat Inwestycji – 229, 230; Samodzielne stanowisko ds. administrowania siecią - 240

Administrator Danych Osobowych

WÓJT GMINY

.....

Dariusz Żukowski

Wykonał:
W. Sobczyński

SWO.142.1.2019.WS

Załącznik Nr 14 do Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych

Wykaz zbiorów danych osobowych

Lp.	Nazwa zbioru danych osobowych	Programy zastosowane do przetwarzania	Lokalizacja zbioru/ miejsce przetwarzania
1.	Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów.	EZD; EWOPIS;EWMAPA; GROSZEK-UŻYTKOWANIE; GEO-SYSTEM-MIENIE; KONTO UŻYTKOWNIKA, KONTO EMAIL	Referat Geodezji i Gospodarki Przestrzennej– 110, 111, 112, 113, 114

Administrator Danych Osobowych

WÓJT GMINY
Dariusz Żupiński
.....

Wykonał:
W. Sobczyński

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

Urząd Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn

SWO.142.1.2019.WS

Załącznik Nr 15 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Lp.	Nazwa zbioru danych osobowych	Określenie zakresu danych (nazwa tablicy)	Programy służące do przetwarzania	Uwagi
1.	1) Rejestr korespondencji.	Nazwiska i imiona, adres zamieszkania lub pobytu, przedmiot sprawy.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL.	
2.	2) Ewidencja licencji na krajowy transport drogowy taksówką;	Imię, nazwisko, adres zamieszkania, Numer Identyfikacji Podatkowej, numer Certyfikatu Kompetencji Zawodowych.	EZD; CEIDG; EWIDENCJA DZIAŁALNOŚCI GOSPODARCZEJ; zezwolenia na sprzedaż napojów alkoholowych; licencje na taxi; rejestr innych obiektów hotelarskich; zezwolenia na transport drogowy osób; KONTO UŻYTKOWNIKA, KONTO EMAIL.	
	3) Ewidencja zezwoleń na sprzedaż napojów alkoholowych;	Nazwiska i imiona, adres zamieszkania lub pobytu, Numer Identyfikacji Podatkowej, oznaczenie rodzaju zezwolenia, oznaczenie przedsiębiorcy, jego siedzibę i adres, w przypadku stanowienia pełnomocników ich imiona, nazwiska i adres zamieszkania, przedmiot działalności gospodarczej, adres punktu sprzedaży, adres punktu składowania napojów alkoholowych (magazynu dystrybucyjnego), dokument potwierdzający tytuł prawny wnioskodawcy do lokalu stanowiącego punkt sprzedaży napojów alkoholowych, pisemna zgoda właściciela, użytkownika, zarządcy lub administratora budynku, jeżeli punkt sprzedaży będzie zlokalizowany w budynku mieszkalnym wielorodzinnym.		
	4) Uzależnienia.	Nazwiska i imiona, adres zamieszkania, informacje dotyczące członków rodziny osoby uzależnionej, nałogi.		
	5) Ewidencja obiektów hotelarskich innych.	Imię i nazwisko, miejsce zamieszkania, nazwa obiektu jeżeli usługi będą świadczone z użyciem nazwy własnej, położenie wraz z podaniem jego adresu.		

3.	6) Karta Nadarzyniaka;	Imię, nazwisko, adres zamieszkania, Nr PESEL, adres e-mail, nr telefonu.	EZD; 4 SECID; 4 SECID_ZTM; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	7) Przedstawiciele Wójta Gminy Nadarzyn do sprawowania stałego, zewnętrznego dozoru lokali wyborczych.	Imiona, nazwiska, adresy zamieszkania, numery dowodów osobistych, numery telefonów.		
	8) Sprawy obronne.	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, miejsce urodzenia, kategoria zdolności do czynnej służby wojskowej, stopień, wojskowy, specjalność wojskowa, adres siedziby firmy, numer rejestracyjny pojazdu, marka pojazdu, numer książeczki wojskowej.		
	9) Monitoring wizyjny	Wizerunek		
4.	10) Ewidencja nadanych numerów porządkowych posesjom;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, położenie działki.	EZD; EWOPIS;EWMAPA; EDOŚ; GROSZEK - UŻYTKOWANIE; GEO-SYSTEM; NUMERACJA PORZĄDKOWA; Kszob;	
	11) Ewidencja użytkowników wieczystych;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, powierzchnia działki, położenie działki.		
	12) Ewidencja wydanych decyzji podziału gruntów;	Imię, nazwisko, adres zamieszkania, data urodzenia, PESEL, imiona rodziców, miejsce urodzenia, numer dowodu osobistego, siedziba firmy, NIP, Regon, numer księgi wieczystej, numer aktu własności, numer działki, położenie działki, powierzchnia działki.		
	13) Ewidencja wydanych decyzji przekształcenia prawa użytkowania wieczystego w prawo własności;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu, numer działki, położenie działki, powierzchnia działki.		
	14) Ewidencja wydanych decyzji w sprawie rozgraniczenia nieruchomości;	Nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer działki, położenie działki, powierzchnia działki.		

	15) Ewidencja wydanych decyzji w sprawie odszkodowania za działkę, która przeszła z mocy prawa na własność gminy;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu, numer działki, położenie działki, powierzchnia działki.	Dzierżawy; KONTO UŻYTKOWNIKA, KONTO EMAIL GEO-SYSTEM-MIENIE;	
	16) Rejestr decyzji i postanowień z zakresu urbanistyki i zagospodarowania przestrzennego;	Imię i nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy, położenie działki, numer działki.		
	17) Rejestr wypisów z miejscowego planu zagospodarowania przestrzennego;	Imię i nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy.		
	18) Rejestr zaświadczeń z zakresu urbanistyki i zagospodarowania przestrzennego.	Imię i nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy, położenie działki, numer działki.		
	19) Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów	Imiona, nazwiska , adres zamieszkania, numer księgi wieczystej, numer ewidencyjny działki.		

5.	20) Rejestr skarg i wniosków do Biura Rady Gminy;	Nazwiska i imiona, adres zamieszkania lub pobytu.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	21) Oświadczenia majątkowe Radnych;	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, miejsce urodzenia, miejsce pracy, zawód, posiadane zasoby pieniężne, posiadane nieruchomości, posiadane udziały w spółkach, posiadane akcje w spółkach, działalność gospodarcza, funkcje w spółkach, inne dochody, składniki mienia ruchomego o wartości powyżej 10 000 PLN, zobowiązania pieniężne o wartości powyżej 10 000 PLN.		
	22) Archiwum.	Nazwiska i imiona, adresy zamieszkania, przedmiot sprawy.		
6.	23) Rejestr skarg i wniosków do Wójta Gminy;	Nazwiska i imiona, adres zamieszkania lub pobytu.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	24) Oświadczenia majątkowe	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, miejsce urodzenia, miejsce pracy, zawód, posiadane zasoby pieniężne, posiadane nieruchomości, posiadane udziały w spółkach, posiadane akcje w spółkach, działalność gospodarcza, funkcje w spółkach, inne dochody, składniki mienia ruchomego o wartości powyżej 10 000 PLN, zobowiązania pieniężne o wartości powyżej 10 000 PLN.		
7.	25) Konkursy na stanowiska w urzędach;	Nazwiska i imiona, miejsce pracy, data urodzenia, zawód, miejsce urodzenia, wykształcenie, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer PESEL, numer telefonu, inne dane osobowe, przetwarzane w zbiorze: adres poczty elektronicznej, motywacja i zainteresowania osoby, orzeczenie o stopniu niepełnosprawności. Dane przetwarzane w zbiorze ujawniają bezpośrednio lub w kontekście stan zdrowia, orzeczenia o ukaraniu.	EZD; Kadry Płace; Płatnik; Stare Kadry; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	26) Kadry, płace;	Nazwiska i imiona, miejsce pracy, data urodzenia, zawód, miejsce urodzenia, wykształcenie, adres zamieszkania lub pobytu, seria i numer dowodu osobistego, numer PESEL, numer telefonu, inne dane osobowe, przetwarzane w zbiorze: adres poczty elektronicznej, motywacja i zainteresowania osoby, orzeczenie o stopniu niepełnosprawności. Dane przetwarzane w zbiorze ujawniają bezpośrednio lub w kontekście stan zdrowia, orzeczenia o ukaraniu.		

8.	27) Zakładowy Fundusz Świadczeń Socjalnych;	Nazwiska i imiona, PESEL, data i miejsce urodzenia, miejsce zamieszkania lub pobytu, stan cywilny, pełna informacja o rodzinie, sytuacja zawodowa pracownika, emeryta.	EZD; beSTi@ ;Kadry Płace; Kszob eBank Biznes; PFRON; płatnik; płace stare; Bank; Rejestr VAT; KASA; KONTO; KSIĘGOWOŚĆ BUDŻETOWA; KONTO; DocuSafe; UPK; K i P-TENSOFT, KADRY i PŁACE – INFOSYSTEM ; ŚRODKI TRWAŁE; BANKOWOŚĆ ELEKTRONICZNA; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	28) Ewidencja sprzedaży dla celów rozliczenia podatku VAT.	Imiona, nazwiska, adres zamieszkania lub pobytu, NIP.		
9.	29) Ewidencja opłat rocznych z tytułu użytkowania wieczystego;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, powierzchnia i nr działki.	EZD; księgowość budżetowa; BeSTi@; podatki; EWOPIS KASA; PODATKI, OPŁATY LOKALNE, KSIĘGOWOŚĆ ZOBOWIĄZAŃ., W. UŻYTKOWANIE; E-MANDAT – WINDYKACJA; AUTA-OS. FIZYCZNE I PRAWNE (JGU); KONTO UŻYTKOWNIKA, KONTO EMAIL; KSZOb; BUDŻET; GOMIG; UPK I KSIĘGOWOŚĆ JGU; EGZEKUCJA	
	30) Ewidencja podatków i opłat od osób fizycznych;	Imię i nazwisko, data urodzenia, imię ojca i matki, nr PESEL, adres zamieszkania oraz dane dotyczące nieruchomości tzn. miejsce położenia przedmiotu opodatkowania oraz nr działki, nr księgi wieczystej.		
	31) Ewidencja podatników, płatników i dłużników.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, numer ewidencyjny PESEL, adres zamieszkania lub pobytu, miejsce pracy, seria i numer dowodu osobistego, księga wieczysta, numer ewid. działki, powierzchnia działki, powierzchnia budynku, dane o powierzchni lasu, nieruchomości, dochody roczne z gospodarstw rolnych, hektary przeliczeniowe, dane identyfikujące pojazd lub nieruchomość, tytuł prawny do przedmiotów opodatkowania, identyfikatory działek ewidencyjnych, dane dotyczące środków transportowych.		
10.	32) Akta Urzędu Stanu Cywilnego (księgi urodzeń, zgonów, zaślubin);	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego, , numer telefonu, nazwisko, imię (imiona) i płeć dziecka, miejsce i datę urodzenia dziecka, nazwiska, nazwiska rodowe rodziców, miejsce zamieszkania każdego z rodziców w chwili urodzenia się dziecka, płeć, nazwisko, imię i miejsce zamieszkania zgłaszającego, numer aktu urodzenia i USC sporządzającego akt, dane zawarte w zgłoszeniu urodzenia dziecka, nazwiska i imiona osób	EZD; USC WIN;SELWIN;SWDO;	

		zawierających małżeństwo, nazwisko panieńskie, nazwisko z poprzedniego małżeństwa star cywilny, miejsce i datę zawarcia małżeństwa, nazwiska i imiona świadków, nazwisko (nazwiska) które będą nosić osoby zawierające małżeństwo po jego zawarciu, oraz nazwisko, które będą nosić dzieci zrodzone z tego małżeństwa, numer aktu małżeństwa i USC sporządzającego akt, informacje zawarte w zezwoleniu na zawarcie małżeństwa, godzina oraz miejsce zgonu lub znalezienia zwłok, okoliczność znalezienia zwłok, przypuszczalny rok urodzenia zmarłego, znaki szczególne zmarłego, opis odzieży oraz innych przedmiotów znalezionych przy zmarłym, nazwisko, imię (imiona) oraz nazwisko rodowe małżonka osoby zmarłej, stan cywilny, nazwiska rodowe i imiona rodziców zmarłego, nazwisko, imię (imiona) osoby zgłaszającej zgon, dane dotyczące szpitala lub zakładu, adnotacje o rozwodzie, separacji oraz o zniesieniu separacji, data rozwiązania małżeństwa, oznaczenie sądu i numer orzeczenia, data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, orzekającego przysposobienie, adopcję, data unieważnienia aktu małżeństwa, urodzenia, zgonu, oznaczenie sądu orzekającego oraz numer orzeczenia. Innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.	EWOPIS; Rejestry: dowodów osobistych, PESEL, mieszkańców, zamieszkania cudzoziemców; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	33) Rejestr mieszkańców;	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu , numer ewidencyjny PESEL, seria i numer dowodu osobistego, adres zameldowania, nazwiska rodowe rodziców, kraj urodzenia, stan cywilny, płeć, obywatelstwo, imię i nazwisko rodowe małżonka oraz numer PESEL jeśli był nadany.		
	34) Zmiana imion i nazwisk.	Nazwiska i imiona, PESEL jeśli został nadany, imiona rodziców, adres zamieszkania lub pobytu, nazwisko rodowe, ważne względy uzasadniające wniosek o zmianę nazwiska lub imienia, części (człony), z jakich składa się nazwisko, forma pisowni imienia lub nazwiska. Innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.		
11.	35) Realizacja projektów dofinansowania z funduszy zewnętrznych.	Imię, nazwisko, płeć, wiek w chwili przystąpienia do projektu, PESEL, wykształcenie, potwierdzenie bądź zaprzeczenie zatrudnienia, potwierdzenie bądź zaprzeczenie niepełnosprawności adres zamieszkania, telefon, adres poczty elektronicznej.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL;EWOPIS;EWMAPA; MEWA.SI2014, UZP;UPUE	
12.	36) Ewidencja decyzji środowiskowych;	Imię, nazwisko, adres zamieszkania, nazwa firmy, siedziba firmy.	EZD; EWOPIS;EWMAPA;	

	37) Informacje o wyrobach zawierających azbest;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer działki, adres działki.	GOMIG; TAXI+; KSZOB; EDOŚ; OPŁATY LOKALNE; bazaazbestowa; KONTO UŻYTKOWNIKA, KONTO EMAIL	
	38) Rejestr osób składających deklaracje na wywóz odpadów komunalnych;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer telefonu, e-mail.		
	39) Rejestr pozwoleń na usunięcie drzew i krzewów;	Imiona, nazwiska, adres zamieszkania, nazwa firmy, siedziba firmy, numer działki.		
	40) Rejestr umów na wywóz nieczystości stałych i płynnych;	Nazwiska i imiona, adres zamieszkania lub pobytu, nazwa firmy, siedziba firmy, numer zawartej umowy.		
	41) Ewidencja zbiorników bezodpływowych i oczyszczalni przydomowych;	Nazwisko, imię, adres zamieszkania, adres i nr działki na której prowadzona jest eksploatacja przydomowej oczyszczalni ścieków, numer telefonu.		
	42) Zbiór wydanych przez starostę pozwoleń o dopuszczalność emisji do środowiska;	Imiona, nazwiska, adres zamieszkania, nazwa firmy, siedziba firmy.		
	43) Rejestr zezwoleń na chów psów ras niebezpiecznych dla osób postronnych;	Nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu, metryka psa, w której podaje się imię, nazwisko i adres hodowcy.		
	44) Rejestr decyzji wydanych do projektów robót geologicznych;	Imię, nazwisko, nazwa firmy, adres zamieszkania, siedziba firmy, numer działki.		

	45) Ewidencja podmiotów gospodarczych prowadzących działalność, w wyniku której powstają odpady niebezpieczne oraz nie zaliczone do niebezpiecznych;	Imię i nazwisko, adres zamieszkania, nazwa firmy, siedziba firmy, zakres działania.		
	46) Ewidencja opłat za zmniejszoną naturalną retencję terenową;	Imię, nazwisko, adres zamieszkania, nr telefonu.		
	47) Postępowania w sprawie zmiany stanu wody na gruncie;	Imię, nazwisko, adres zamieszkania, nr telefonu.		
	48) Produkcja roślinna.	Imię, nazwisko, adres zamieszkania, nr telefonu.		
13.	49) Zamówienia publiczne.	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, informacje na temat przeciętnej liczby zatrudnionych pracowników oraz liczebności personelu kierowniczego, wykaz niezbędnych do wykonania zamówienia narzędzi i urządzeń, jakie posiada wykonawca, wykaz osób i podmiotów, które będą wykonywać zamówienie lub będą uczestniczyć w wykonywaniu zamówienia, wraz z informacjami na temat ich kwalifikacji niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nich czynności, wykaz wykonanych w okresie ostatnich pięciu lat robót budowlanych, wykaz wykonanych w okresie ostatnich trzech lat dostaw lub usług, informacje banku, w którym wykonawca posiada podstawowy rachunek bankowy, potwierdzające wysokość posiadanych środków finansowych lub zdolność kredytową wykonawcy, polisa lub inny dokument ubezpieczenia potwierdzające, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej, koncesje, zezwolenia lub licencje, aktualne zaświadczenia właściwego naczelnika urzędu skarbowego oraz właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia	EZD; EWOPIS;EWMAPA; MEWA.SI2014, UZP, UPUE; KONTO UŻYTKOWNIKA, KONTO EMAIL	

		Społecznego potwierdzające odpowiednio, że wykonawca nie zalega z opłacaniem podatków, opłat oraz składek na ubezpieczenie zdrowotne lub społeczne, lub zaświadczenia, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu, dokumenty stwierdzające, że osoby, które będą wykonywać zamówienie, posiadają wymagane uprawnienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień, dane dotyczące skazań.		
14.	50) Sprawy dotyczące pasa drogowego.	Nazwiska i imiona, adres zamieszkania lub pobytu, cel zajęcia pasa drogowego, powierzchnia zajmowanego pasa drogowego lub powierzchnia reklamy, okres zajęcia pasa drogowego, wysokość opłaty za zajęcie pasa drogowego oraz sposób jej uiszczania, sposób zabezpieczenia zajmowanego pasa drogowego, warunki przywracania pasa drogowego do poprzedniego stanu użyteczności, zakres i technologia robót przywracających stan użyteczności, sposób odbioru przedmiotowego odcinka pasa drogowego, zasady usuwania usterek i wad technicznych.	EZD; EWOPIS; EWMAPA; KSzob-Opłaty lokalne; NORMA; ePODGiK, KONTO UŻYTKOWNIKA, KONTO EMAIL	
15.	51) Wnioski o udostępnienie informacji publicznej.	Nazwiska i imiona, adres zamieszkania, numer telefonu, adres e-mail, nazwa firmy, siedziba firmy.	EZD; KONTO UŻYTKOWNIKA, KONTO EMAIL.	Dotyczy wszystkich referatów – zbiór rozproszony

Administrator Danych osobowych

WÓJT GMINY
Dariusz Zdaliński

.....

Wyk. W. Sobczyński

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-85, fax 22 729-81-75

SWO.142.1.2019.WS

Załącznik Nr 15 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Lp.	Nazwa zbioru danych osobowych	Określenie zakresu danych (nazwa tablicy)	Programy służące do przetwarzania	Uwagi
1.	Ewidencja wydanych zaświadczeń o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów.	Imiona, nazwiska , adres zamieszkania, numer księgi wieczystej, numer ewidencyjny działki.	EZD; EWOPIS;EWMAPA; GROSZEK- UŻYTKOWANIE; GEO-SYSTEM- MIENIE; KONTO UŻYTKOWNIKA, KONTO EMAIL	

WÓJT GMINY
Dariusz Dwornicki

Administrator Danych Osobowych

.....

Wykonał:
W. Sobczyński

Załącznik Nr 17 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

Nadarzyn, dnia ..... r.

.....

(miejscowość, data)

.....

(imię i nazwisko pracownika)

.....

(stanowisko)

OŚWIADCZENIE O ZACHOWANIU W TAJEMNICY PRZETWARZANIA DANYCH OSOBOWYCH

W związku z udzielonym mi w dniu ..... r. upoważnieniem do przetwarzania danych osobowych, niniejszym zobowiązuje się do:

1. zachowania w tajemnicy wszelkich danych osobowych, do których mam dostęp w związku z wykonywaniem zadań służbowych;
2. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, do których mam dostęp w związku z wykonywaniem zadań służbowych.

Powyższej tajemnicy zobowiązuje się dochować również po ustaniu zatrudnienia.

.....

(podpis)

_____, _____ r.

(miejscowość, data)

Załącznik Nr 18 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

WYREJESTROWANIE UPRAWNIEŃ

dostępu do systemów informatycznych

Z dniem.....odbieram Pani/Panu .....uprawnienia dostępu do systemów informatycznych. Wyrejestrowanie następuję przez zablokowanie konta użytkownika i ma charakter czasowy/trwały.

.....

/podpis osoby upoważnionej/

.....

/data i podpis osoby wyrejestrowanej/

Załącznik Nr 19 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

UPOWAŻNIENIE

dla osoby odpowiedzialnej za przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych

Z dniem.....upoważniam Panią/Pana ..... do przetwarzania w systemie teleinformatycznym danych przetwarzanych w zbiorach danych utworzonych przez Urząd Gminy Nadarzyn w ramach powierzonych obowiązków oraz do **przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.**

Upoważnienie ważne jest.....

Załącznik Nr 20 do Polityki Bezpieczeństwa

Przetwarzania Danych Osobowych

SWO.142.3.2018.WS

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

W

Urzędzie Gminy Nadarzyn,
ul. Mszczonowska 24, 05-830 Nadarzyn

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
GMINA NADARZYN ul. Mszczonowska 24, 05-830 Nadarzyn NIP: 534-22-54-841 tel. 22 729-81-85	WÓJT GMINY Dariusz Żwoliński	25 maja 2018

Spis treści

Cel i zakres stosowania instrukcji 3
Postanowienia ogólne 3
Definicje 3
Obowiązki w zakresie ochrony danych osobowych 4
Obowiązki inspektora ochrony danych (IOD) 4
Obowiązki inspektora ds. administrowania siecią - informatyka 5
Obowiązki użytkowników 5
Poziom bezpieczeństwa 6
Bezpieczna eksploatacja systemów informatycznych 7
Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym 8
Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem 9
Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu oraz tworzenia kopii zapasowych 10
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego 13
Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych 13
Przetwarzanie, udostępniane i likwidacja danych osobowych 14
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych 15
Naprawy urządzeń komputerowych z chronionymi danymi osobowymi 15
Wymagania dotyczące sprzętu i oprogramowania 15
Procedura utrzymania ciągłości działania systemów informatycznych 16
Postanowienia końcowe 19
HISTORIA DOKUMENTU 20

§ 1 Cel i zakres stosowania instrukcji

Instrukcja określa sposób zarządzania systemami informatycznymi, wykorzystywanymi do przetwarzania danych osobowych, przez administratora danych – w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych.

§ 2 Postanowienia ogólne

1. Instrukcja została opracowana zgodnie z wymogami 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 (ogólne rozporządzenie o ochronie danych), (DZ. U. UE. z 2016 r., L119/1) zwanym dalej „Rozporządzeniem".
2. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
3. Inspektor ds. administrowania siecią - informatyk powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.

§ 3 Definicje

1. Ilekroć w instrukcji jest mowa o:
   1) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   2) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
   3) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
   4) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
   5) **identyfikatorze** – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   6) **publicznej sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – prawo telekomunikacyjne (j.t. Dz. U. z 2014 r., poz. 243);

związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

§ 6 Obowiązki inspektora ds. administrowania siecią - informatyka

Do obowiązków inspektora ds. administrowania siecią - informatyka w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych;

2) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;

3) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym;

4) zarządzanie stosowanymi w systemach informatycznych środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków złożonych przez osobę do tego upoważnioną;

5) utrzymanie systemu w należytej sprawności technicznej;

6) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania, oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych;

7) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

§ 7 Obowiązki użytkowników

Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności:

1) przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych;
2) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
3) udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania;
4) uniemożliwienie dostępu do danych osobowych w systemie lub ich podglądu przez osoby nieupoważnione;
5) informowanie Inspektora ochrony danych o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

11) inspektor ds. administrowania siecią - informatyk monitoruje wdrożone zabezpieczenia systemu informatycznego;

12) urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar przetwarzania danych, zabezpiecza się w sposób zapewniający poufność i integralność tych danych;

13) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;

14) w przypadku zastosowania logicznych zabezpieczeń obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną,

b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

15) wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony.

§ 9 Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona poprzez przestrzeganie następujących zasad:

1) użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie;

2) użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;

3) użytkownikom nie wolno we własnym zakresie instalować nowego lub aktualizować już zainstalowanego oprogramowania;

4) użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych;

5) użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona;

6) użytkownikom nie wolno bez uzyskania zgody Inspektora ochrony danych lub osób przez niego upoważnionych przenosić aplikacji oraz zasobów zlokalizowanych na zasobach sieciowych na dyski lokalne oraz przenośne nośniki danych;

zarejestrowana jako użytkownik w tym systemie przez Inspektora ds. administrowania siecią - informatyka , na pisemny wniosek Administratora Danych, określającego zakres uprawnień pracownika.

11) Rejestracja użytkownika polega na nadaniu identyfikatora i przydzieleniu jednorazowego hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu. Podczas pierwszego logowania, użytkownik dokonuje zmiany hasła na nowe, znane tylko jemu.

12) Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

13) Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

14) Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

15) Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązuje się do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

2. Wyrejestrowywanie uprawnień

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje Inspektor ds. administrowania siecią - informatyk na wniosek przełożonego.

2) Wyrejestrowanie, o którym mowa w pkt 1, może mieć charakter czasowy lub trwały.

3) Wyrejestrowanie następuje poprzez:

   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

§ 11 Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Identyfikator

1) Identyfikator nadaje Inspektor ds. administrowania siecią – informatyk.

2) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. Hasło użytkownika

1) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

2) Użytkownicy powinni stosować hasła, które:

   a) są łatwe do zapamiętania, a trudne do odgadnięcia,

   b) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko,

6) Obowiązuje zakaz robienia kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez inspektora ds. administrowania siecią - informatyka lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
7) Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne, po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii, dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
8) Jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami administratora danych a komputerami przenośnymi użytkowników tylko po ich zaszyfrowaniu.
9) Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
10) Obowiązuje zakaz wynoszenia poza obszar przetwarzania danych na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej.
11) Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak by zapobiec ich utracie.
12) Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary zasobów sieciowych, a następnie prawidłowym wylogowaniu się przez użytkownika i wyłączeniu komputera.
13) Przed opuszczeniem pokoju należy:
    a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    b) schować do zamykanych na klucz szaf wszelkie dokumenty zawierające dane osobowe,
    c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    d) zamknąć okna,
    e) opuszczając pokój należy zamknąć za sobą drzwi na klucz.

2. Tryb pracy na komputerach przenośnych.

1) O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji, dotyczące pracy na komputerach stacjonarnych.
2) Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu.
3) Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
4) Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
5) Użytkownicy zmieniają hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni;
6) Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane i opatrzone hasłem dostępu.
7) Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych

§ 13 Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez inspektora ds. administrowania siecią – informatyka.
2) Oprogramowanie, o którym mowa w pkt 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3) Niezależnie od ciągłego nadzoru, o którym mowa w pkt. 2, inspektor ds. administrowania siecią - informatyk nie rzadziej niż raz na miesiąc przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
4) Do obowiązków inspektora ds. administrowania siecią - informatyka należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie.
5) Użytkownik niezwłocznie powiadamia inspektora ds. administrowania siecią - informatyka o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
6) Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym Firewall.

§ 14 Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1) System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.
2) 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.
3) Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione.
4) W przypadku zgłoszenia sprzeciwu o którym mowa w „Rozporządzeniu", wobec przetwarzania danych osobowych, system powinien zapewniać odnotowywanie tej informacji.
5) Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i wydrukowanie:

7) Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.

8) W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych.

9) Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.

§ 16 Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1) Przeglądu i konserwacji systemu dokonuje inspektor ds. administrowania siecią - informatyk doraźnie.

2) Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale inspektor ds. administrowania siecią - informatyk nie rzadziej niż raz na kwartał.

§ 17 Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1) Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzane są – o ile to możliwe – przez inspektora ds. administrowania siecią - informatyka.

2) Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane przez serwisanta prowadzone są pod nadzorem inspektora ds. administrowania siecią - informatyka w siedzibie administratora danych (jeśli to możliwe) lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umowy powierzenia przetwarzania danych osobowych.

3) Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce.

§ 18 Wymagania dotyczące sprzętu i oprogramowania

1) Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

2) Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty inspektora ds. administrowania siecią - informatyka.

3) Przed zainstalowaniem nowego oprogramowania inspektor ds. administrowania siecią - informatyk lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.

4) Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna

d) Gomig-Odpady, EDOŚ (lokalny serwer/sieć lokalna),

e) Poczta elektroniczna (połączenie internetowe),

f) System plików użytkowników (lokalny serwer/sieć lokalna),

g) Aplikacja bankowa (połączenie internetowe).

5. Odtwarzanie serwerów (sieć lokalna – pomieszczenie serwerowe).

1) Jeśli usterka nie wymaga nakładu pracy większego niż 1 dzień lub wymagane i możliwe jest przywrócenie serwera z momentu tuż przed awarią: kontakt z pomocą techniczną i wymiana uszkodzonego elementu.

2) Jeśli usterka wymaga większego nakładu pracy większego niż 1 dzień lub nie jest możliwe przywrócenie stanu systemu z przed awarii: przywrócenie systemu na zapasowy serwer. Dla zapewnienia funkcjonowania minimalnego zakresu systemów informatycznych konieczny jest min. 1 serwer. Wszystkie dostępne obecnie na rynku serwery spełniają minimalne wymagania. Należy jedynie zwrócić uwagę na pojemność dysków. Dyski o łącznej pojemności min. 2 TB.

6. Odtwarzanie połączenia Internetowego.

1) Dla zapewnienia funkcjonowania krytycznego systemu komunikacji internetowej konieczne jest zapewnienie prawidłowego funkcjonowania urządzeń połączeniowych typu router, jak i właściwego funkcjonowania samego łącza internetowego. W przypadku wystąpienia przerw w dostępie do połączeń internetowych należy zwrócić się do następujących osób/firm:
   a) Orange Polska S.A., ul. Jagiellońska 34, opiekun klienta: Jakub Flaszczyński tel. 510-068-189,
   b) Lokalny radiowy operator internetowy.
2) Przewidywany czas odtwarzania (zależny od przyczyny braku komunikacji internetowej) – od 2 godzin do 96 godzin.
3) W przypadku uszkodzenia routera należy uruchomić procedurę gwarancyjną, a następie przywrócić z konfiguracją urządzenia z kopii zapasowej.

7. Odtwarzanie urządzeń sieciowych (sieć lokalna – pomieszczenie serwerowe).

1) Dla zapewnienia funkcjonowania minimalnego zakresu systemów informatycznych konieczne są przynajmniej dwa urządzenia przełączające SWITCH o 24 portach 10/100/1000 Mb/s. Pozwala to zapewnić pracę w krytycznych z punktu widzenia urzędu działach: np.:
   a) Referat Realizacji Podatków i Opłat (4 stanowiska),
   b) Referat Geodezji i Gospodarki Przestrzennej (4 stanowiska),
   c) Urząd Stanu Cywilnego (2 stanowiska),
   d) Samodzielne stanowisko ds. obsługi Biura Rady Gminy i Archiwum (1 stanowisko),
   e) Samodzielne stanowisko ds. audytu (1 stanowisko),
   f) Samodzielne stanowisko ds. kadrowych (1 stanowisko),
   g) Samodzielne stanowisko ds. ochrony informacji niejawnych, bezpieczeństwa informacji oraz obronnych i wojskowych (1 stanowisko),
   h) Samodzielne stanowiska ds. kancelaryjno-sekretarskich (2 stanowiska),

Gomig-Odpady, EDOŚ: pomoc techniczna tel. 42 648 03 30
Aplikacja bankowa: Michał Pawlak, tel. 22 727 90 01

10. Alternatywna lokalizacja

W przypadku wystąpienia katastrofy (pożar, powódź itp.) koniecznym może okazać się zmiana lokalizacji biura. Pomieszczeniem, które jako pierwsze powinno zostać zaadaptowane na biuro jest pomieszczenie w Nadarzynie przy Placu Poniatowskiego 42. W tym przypadku należy kontaktować się z następującymi osobami: Dyrektor Nadarzyńskiego Ośrodka Kultury, tel. 22 729 89 15

11. Powiadamianie.

1) W przypadku wystąpienia katastrofy (pożar, powódź, kradzież itp.) następujące osoby w firmie powinny zostać natychmiast powiadomione o zaistniałych faktach, bieżącej sytuacji i podjętych lub planowanych działaniach mających na celu powrót do normalnej działalności:
   a) Wójt Gminy Nadarzyn,
   b) Inspektor Ochrony Danych (IOD),
   c) Inspektor ds. administrowania siecią – Informatyk.

2) W przypadku wystąpienia zagrożenia dla zdrowia lub życia pracowników bezwzględny priorytet maja wszelkie akcje mające na celu zapewnienie bezpiecznej ewakuacji pracowników, a później ochrony mienia. W tym przypadku należy bezwzględnie powiadomić właściwe służby:
   a) Straż pożarna, 998 lub 112;
   b) Pogotowie ratunkowe, 999 lub 112;
   c) Policja 997 lub 112.

§ 20 Postanowienia końcowe

1) W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2) Każda osoba upoważniona do przetwarzania danych osobowych jest zapoznawana przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz składa pisemne oświadczenie, potwierdzające znajomość jej treści.
3) Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

HISTORIA DOKUMENTU

Numer zmiany	Numer strony/ Rozdziały	Opis	Akcja Np. utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie	Data	Zatwierdził Podpis

URZĄD GMINY NADARZYN
05-830 Nadarzyn
ul. Mszczonowska 24
województwo mazowieckie
tel. 22 729-81-65, fax 22 729-81-75

REGULAMIN ZARZĄDZANIA SYSTEMEM MONITORINGU WIZYJNEGO

W Urzędzie Gminy Nadarzyn

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot:	Gmina Nadarzyn
Wersja:	Nr 1
z dnia:	2019-04-01
Zatwierdził(a):	WÓJT GMINY Dariusz Żwoliński ..... podpis Administratora Danych

§ 1

Regulamin określa zasady funkcjonowania monitoringu wizyjnego w budynkach wraz z ich otoczeniem pozostających w zasobach Gminy Nadarzyn, reguły rejestracji i zapisu informacji oraz sposób zabezpieczania i udostępniania zgromadzonych danych.

§ 2
OGÓLNE POSTANOWIENIA

1. Administrator danych Gmina Nadarzyn z reprezentacją w osobie **Dariusza Zwolińskiego – Wójta Gminy Nadarzyn** w zakresie zastosowania monitoringu kieruje się zasadą adekwatności tj.: Administrator danych osobowych może pozyskiwać jedynie te dane, co do których istnieje uzasadnienie formalnoprawne ich pobierania oraz zasadą proporcjonalności tj.: doboru stosownej technologii monitoringu.

2. Przyjęte definicje

- *Administrator Danych* (AD)- Gmina Nadarzyn

- *dane osobowe* - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). *Odnosząc się do zakresu danych osobowych przetwarzanych przez monitoring właściwym jest wskazanie w szczególności wizerunku, cech szczególnych osób i numerów identyfikacyjnych (np. numery tablic rejestracyjnych i numery boczne pojazdów);*

- *naruszenie bezpieczeństwa informacji* – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych;

- *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;

- *odbiorca danych* – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem powszechnie obowiązującym, 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. Przy czym przez sformułowanie ,, „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

- *osoba upoważniona do przetwarzania danych osobowych* – osoba, która złożyła Administratorowi oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez Administratora, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;

- *podmiot przetwarzający* – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

- *przetwarzanie* - 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. *W przypadku monitoringu wizyjnego będą to operacje polegające w szczególności na zapisywaniu, przeglądaniu, udostępnianiu i usuwaniu nagrań zarejestrowanych zdarzeń i osób niezależnie od charakteru nośnika, w którym są przechowywane (dyski twarde systemu, nagrania zapisane w pamięci urządzenia umożliwiającego zdalny dostęp;*

- *poufność danych* - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

- *rozliczalność danych* - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

- *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 (ogólne rozporządzenie o ochronie danych);

- *usuwanie danych* – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

- *uwierzytelnianie* – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

- *użytkownik/pracownik (w tym podmiotu trzeciego)* - osoba przetwarzająca dane w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia u Administratora lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

- *zgoda na przetwarzanie danych osobowych* - oświadczenie woli osoby, której dane są przetwarzane przez Administratora danych, w której wyraża swoją aprobatę dla tego procesu;

3. Przed instalacją monitoringu przeanalizowano następujące aspekty:
   a) nadzór eksploatacyjny,
   b) bezpieczeństwo fizyczne oprogramowania jak i urządzeń systemu monitorującego,
   c) szkolenia personelu zajmującego się systemem monitorującym,
   d) zapewnienia adekwatnych środków technicznych i organizacyjnych w celu bezpiecznego przechowywania oraz archiwizacji nagrań z monitoringu,

4. Regulamin funkcjonowania monitoringu wizyjnego określa:
   a) zasady stosowania systemu monitoringu,
   b) zakres stosowania systemu monitoringu,
   c) zasady rejestracji, zapisu oraz zabezpieczenia monitoringu,
   d) regulacje związane z udostępnieniem zapisu z monitoringu.

2. Administrator informuje pracowników na piśmie, o wprowadzeniu monitoringu, jego celach, zakresie, sposobie zastosowania co pracownik potwierdza własnoręcznym podpisem.

§ 3
PODSTAWA PRAWNA

Przesłanki umożliwiające funkcjonowanie monitoringu na terenie Gminy Nadarzyn mają odzwierciedlenie w następujących podstawach prawnych:

a) 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),

b) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000 z dnia 24.05.2018 r.),
c) Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2016r. poz. 1432 z późn. zm.),
d) Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. Z 2018 r. poz 917),
e) Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. Z 2018 r. poz. 994).

Wójt Gminy Nadarzyn ma świadomość, że zapis z monitoringu nie zawsze stanowi zbiór danych osobowych sensu stricto, co nie zwalnia jednocześnie placówki z obowiązku zabezpieczania takowych informacji przed dostępem osób nieuprawnionych.
Monitoring nie stanowi środka nadzoru nad jakością wykonywania pracy przez pracowników placówki.

§ 4
CEL ZASTOSOWANIA MONITORINGU

1. Celem zastosowania systemu monitoringu jest:
   a) zapewnienie bezpieczeństwa pracowników, a także ochrony mienia i zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Zapis monitoringu ma na celu wyłącznie zwiększenie bezpieczeństwa pracy, pracowników oraz umożliwienie wykrywania zachowań szkodzących Administratorowi, pracownikom lub narażających Administratora na straty i nie zostanie wykorzystany w żadnym innym celu;
   b) wypełnienie obowiązku prawnego ciążącego na Administratorze,
   c) wykonanie zadania realizowanego w interesie publicznym.

§ 5
ZAKRES STOSOWANIA MONITORINGU

1. System monitoringu składa się z następujących elementów:
   a) kamer rejestrujących zdarzenie – Zał. Nr 1
   b) urządzenia rejestrujące oraz zapisujące materiał wideo na urządzeniu twardo dyskowym lub nośniku zewnętrznym (magnetyczny, optyczny, magnetooptyczny i półprzewodnikowy) – Zał. Nr 1
   c) kamery w Sali konferencyjnej
2. Zakres możliwie przetwarzanych informacji w powiązaniu z wizerunkiem utrwalonym na urządzeniu monitorującym jednostkę:
   a) Imię i nazwisko,
   b) Nr rejestracyjny pojazdu,
   c) Czas i miejsce zdarzenia objętego monitoringiem,

3. Rejestracja i zapisanie materiału wideo na urządzeniu twardo dyskowym lub nośniku zewnętrznym (magnetyczny, optyczny, magnetooptyczny i półprzewodnikowy) polega na zapisie wyłącznie obrazu.

4. Monitoring funkcjonuje całodobowo, a zapis z monitoringu przechowywany jest na elektronicznym nośniku przez okres 29 dni. Zaznaczyć należy, że okres ten nie powinien być dłuższy niż 30 dni, chyba, że zajdzie uzasadniona konieczność przechowywania zapisu z monitoringu dla celów dowodowych w zakresie postępowania przygotowawczego prowadzonego przez stosowne organy. Niszczenie nagrania następuje po 29 dniach automatycznie, bez udziału osób trzecich, poprzez nadpisanie kolejnych nagrań.

5. Udostępnianie kopii zapisów z systemu monitoringu odbywa się na zasadach ściśle określonych w przepisach prawa.

§ 6
ZASADY STOSOWANIA MONITORINGU

Administrator, podejmując decyzję o stosowaniu monitoringu, zweryfikował, czy realizowane przez niego cele uzasadniają obserwację osób. Administrator ma w świadomości zasadę ograniczenia celu zgodnie z art. 5 ust. 1 lit. b RODO, i bierze pod uwagę potrzebę ochrony prawa do prywatności i ochrony danych osobowych, oraz ich ograniczanie tylko w niezbędnym zakresie. Administrator podejmie starania, aby dane przetwarzane były zgodnie z zasadami:

1. Zgodność z prawem, rzetelność i przejrzystość - dane przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2. Ograniczenie celu - dane zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, nieprzetwarzane w sposób niezgodny z tymi celami ;
3. Minimalizacja danych – dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4. Prawidłowość – dane prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane;
5. Ograniczenie przechowywania – dane przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
6. Integralność i poufność – dane przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

§ 7
MIEJSCA STOSOWANIA MONITORINGU

1. Miejsca objęte monitoringiem:
   a) Części zewnętrzne infrastruktury Gminy Nadarzyn – Zał. Nr 1
   b) Części wewnętrzne infrastruktury Gminy Nadarzyn – Zał. Nr 1
   c) Sala konferencyjna – jedna kamera.

2. Zasady ograniczenia celu i minimalizacji wymagają ograniczenia obszaru monitorowania do niezbędnego zasięgu. Administrator ma na uwadze, że jego interesy nie mogą w sposób nadmierny ograniczać prawa do ochrony danych oraz uzasadnionego oczekiwania osób obserwowanych co do zapewnienia prywatności. Dlatego Administrator nie prowadzi monitoringu w obszarach wrażliwych, takich jak:

   - pomieszczenia przeznaczone do odpoczynku i rekreacji pracowników,
   - obiekty socjalne,
   - pomieszczenia sanitarne,
   - szatnie, stołówki oraz palarnie,
   - pomieszczenia udostępniane zakładowej organizacji związkowej.

3. Zastosowanie systemu monitoringu w podmiocie powinno być zawsze przemyślane i ograniczone do obszarów, gdzie jest to niezbędne z punktu widzenia bezpieczeństwa oraz stosowane z uwzględnieniem wpływu na prywatność osób przebywających w obszarze monitoringu.

§ 8
OBOWIĄZEK INFORMACYJNY

1. Obowiązek informacyjny względem osób, których dane osobowe zostały pozyskane za pomocą monitoringu, jest spełniany względem tych osób za pomocą tablic informujących o zainstalowanym monitoringu. Tablice są zamieszczone w miejscu na tyle widocznym, że spełnienie obowiązku informacyjnego po stronie Administratora nie budzi wątpliwości. Dodatkowo, jednostka zamieszcza graficzny znak informujący o stosowaniu monitoringu w obszarze jej siedziby tj. piktogram kamery.

2. Osoby przebywające na terenie objętym monitoringiem wyrażają jednocześnie zgodę na przetwarzanie ich wizerunku oraz wykonywanych czynności /zachowań, które zostaną zarejestrowane przez kamery systemu monitorującego.

3. Biorąc pod uwagę art. 47 Konstytucji RP, który stanowi, iż każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, jednostka stosuje monitoring z uwzględnieniem poszanowania prawa do prywatności pracowników. Administrator ma obowiązek informacyjny również względem pracowników zatrudnionych w placówce, w ramach której stosuje się urządzenia monitorujące.

§ 9
UDOSTĘPNIANIE ZAPISU Z MONITORINGU OBIEKTU

1. Administrator może zlecić prowadzenie monitoringu profesjonalnym podmiotom na postawie zawartej umowy. Podmiot przetwarzający musi zapewnić gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Osobami upoważnionymi do zasobów monitoringu są:
   1) Arkadiusz Wencel, inspektor ds. organizacyjnych, obronnych i wojskowych
   2) Monika Kosakowska – Ludwiniak , inspektor ds. organizacyjnych
   3) Mateusz Sielski, inspektor ds. inwestycji
3. Zapis monitoringu może być udostępniony, na podstawie pisemnego wniosku, za zgodą Administratora danych tylko:
   a) osobom działającym z upoważnienia Administratora, w celu zwiększenia bezpieczeństwa oraz podjęcia właściwych oddziaływań w tym zakresie,
   b) innym osobom trzecim, które udowodnią swój interes prawny, co do otrzymania wyżej wymienionego zapisu (interes realizowany przez stronę trzecią np. osobom poszkodowanym w sytuacjach zarejestrowanych przez monitoring).
   c) osoby upoważnione przez podmiot przetwarzający.
   d) Wnioski wniesione od innych osób niż wymienione w ust. 2 nie będą rozpatrywane.
4. Osoba, której dane zostaną zebrane poprzez system monitoringu, może korzystać z praw osoby, której dane dotyczą, ujętych w rozporządzeniu. Realizacja uprawnień osoby obserwowanej wiąże się z koniecznością przedstawienia przez nią informacji o sytuacjach, w których mogła znaleźć się w obszarze działania monitoringu (np. okresy czasu, sytuacje, szczegóły jej ubioru). Administrator ma możliwość zażądania, przez podanie informacji, by osoba, której dane dotyczą sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie. Udostępniany materiał nie może obejmować danych innych osób niezaangażowanych w zdarzenie.
5. W przypadku wniosków o dostęp do zapisu monitoringu kierowanych przez organy publiczne i służby porządkowe, powinny być one związane z realizacją zadań tych podmiotów i zgodne z obowiązującymi je zasadami pozyskiwania danych.
6. Sytuacje dotyczące udostępnienia powinny być udokumentowane w myśl zasady rozliczalności.
7. Dane zarejestrowane w ramach monitoringu wizyjnego nie stanowią informacji publicznej i nie podlegają udostępnieniu na podstawie przepisów ustawy o informacji publicznej.

§ 10
ZABEZPIECZENIE DANYCH

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa uwzględniający stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych. Środki techniczne i organizacyjne służące zabezpieczeniu danych osobowych opisane zostały w Polityce Bezpieczeństwa Informacji.

WÓJT GMINY
Dariusz Żwaliński

Nadarzyn, dn. 2019-04-01 .....

podpis Administratora Danych

Wykonał: Wiesław Sobczyński

Opis obszaru i infrastruktury systemu monitoringu

CCTV jest oparty o cyfrowy rejestrator video, audio (HIKVISION).
- Budynek Urzędu Gminy System nr 1 – 16 kamer System HIKVISION. Kamery rejestrują obraz z prędkością 12 lub 25 kl./s. System o rozdzielczości 3 Mpix

HIKVISION

l.p.	Obszar nadzorowany
1	Wejście do budynku lewa strona
2	Wejście do budynku prawa strona
3	Parking z tyłu budynku
4	Wejście główne
5	Kasa
6	Wejście Kancelaria
7	Hol parter
8	Hol piętro
9	Korytarz GOPS
10	Korytarz Audyt
11	Wjazd główny
12	Parking z przodu budynku zbliżenie na miejsca przy budynku
13	Dojście z parkingu do wejścia z prawej strony
14	Podejście do Paczkomatu front budynku
15	Parking z przodu budynku
16	Wjazd na parking od ul. Granicznej

System INTROX. Kamera D/N, 1/3" CCD , rozdzielczość kolor 550 linii, B/W 580 linii, czułość 0 lux (IR LED zał.), synchronizacja wewnętrzna, stosunek S/N ponad 48 dB (AGC wył.), AES, ARW, ABB, FL, AWB, BL, 3,8-9,5 mm

INTROX

l.p.	Obszar nadzorowany
1	Parking z przodu budynku
2	Wejście główne
3	Przejazd po lewej stronie budynku widok od frontu
4	Przejazd po lewej stronie budynku widok od budynku gospodarczego
5	Przejazd na tyłach budynku róg od ul. Granicznej
6	Parking z tyłu budynku widok na miejsca dla niepełnosprawnych
7	Widok na przejście prawy róg budynku (trawnik)
8	Widok na teren zielony przed budynkiem (prawa strona)
9	Parking na tyłach budynku widok na miejsca Poczty Polskiej
10	Hol budynku parter
11	Korytarz I piętro USC, Serwerownia
12	Klatka schodowa strona lewa
13	Klatka schodowa strona prawa
14	Wejście prawe wewnątrz
15	Wejście lewe wewnątrz
16	Poczta Polska

Białe pola wypełnia wnioskodawca DRUKOWANYMI literami. Szare pola wypełnia Administrator Danych.	..... miejscowość i data
..... Oznaczenie Administratora Danych	..... numer kolejny wniosku

WNIOSEK O UDOSTĘPNIENIE NAGRAŃ Z MONITORINGU WIZYJNEGO

1. Dane osoby wnioskującej

imię/imiona:	.....
Nazwisko:	.....
Adres zamieszkania:	.....
inna dana pozwalająca na identyfikację np. nr dowodu osobistego/PESEL:	.....

2. Informacje o sytuacji/zdarzeniu (np. data, godzina, miejsce zdarzenia, szczegóły ubioru), oraz krótki opis zdarzenia.

.....
.....
.....
.....
.....
.....

3. Wskazanie celu otrzymania nagrania z monitoringu, podać komu zostanie przekazane np.: policja, sąd

.....
.....
.....
.....
.....
.....

.....
podpis wnioskodawcy

5. Informacje dotyczące przychylenia/ odrzucenia wniosku:

□ Administrator przychyla się do wniosku	□ Administrator odrzuca wniosek

Uzasadnienie decyzji Administratora

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

data i podpis AD

Potwierdzam odbiór nagrania i oświadczam, że otrzymane materiały zostaną wykorzystane wyłącznie w celu wskazanym we wniosku i nie zostaną wykorzystane do celów prywatnych.

.....

data i czytelny podpis osoby wnioskującej

EWIDENCJA WNIOSKÓW O UDOSTĘPNIENIE NAGRAŃ Z MONITORINGU WIZYJNEGO

Lp.	*data*	*numer kolejny wniosku*	*dane osoby wnioskującej*	*Informacje dotyczące przychylenia/ odrzucenia wniosku*	*Data przekazania nagrania*

EWIDENCJA PRACOWNIKÓW UPOWAŻNIONYCH DO PRACY Z SYSTEMEM MONITORINGU

Lp.	*nazwisko i imię upoważnionego*	*stanowisko*	*data udzielenia upoważnienia*	*data wygaśnięcia upoważnienia*
1.	WENCEL ARKADIUSZ	inspektor ds. organizacyjnych, obronnych i wojskowych	2017-02-24	
2.	KOSAKOWSKA – LUDWINIAK MONIKA	Inspektor ds. organizacyjnych	2019-04-01	
3.	SIELSKI MATEUSZ	Inspektor ds. inwestycji	2019-04-01	
4.	SIELSKI BOGUSŁAW	Portier	2018-05-07	

WÓJT GMINY

Dariusz Żmoliński

.....

podpis Administratora Danych

Załącznik nr 5

.....
Miejscowość, data

.....
(imię i nazwisko pracownika)

.....
(nazwa stanowiska pracy)

Wójt Gminy Nadarzyn
ul. Mszczonowska 24
05-830 Nadarzyn
.....
(oznaczenie Administratora)

OŚWIADCZENIE
o zapoznaniu się z Regulaminem Zarządzania Systemem Monitoringu Wizyjnego w Urzędzie Gminy Nadarzyn

Ja niżej podpisany(a) ....., zatrudniony(a) w Urzędzie Gminy Nadarzyn,
(imię i nazwisko)

ul. Mszczonowska 24, 05-830 Nadarzyn, potwierdzam, że zapoznałem(am) się z treścią obowiązującego Regulaminu Zarządzania Systemem Monitoringu Wizyjnego, co potwierdzam własnoręcznym podpisem. Oświadczam, że treść dokumentu jest dla mnie zrozumiała i nie budzi wątpliwości.

.....
(podpis pracownika)

KLAUZULA INFORMACYJNA MONITORING

do przetwarzania danych osobowych

Na podstawie art. 13 ust. 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 (ogólne rozporządzenie o ochronie danych), zwane dalej RODO, informuję Pana/Panią, że:

1. Administratorem Pana/i Danych jest: Gmina Nadarzyn, Mszczonowska 24, 05-830 Nadarzyn

2. Został powołany Inspektor Ochrony Danych, z którym można się skontaktować pod adresem e-mail: rodo@nadarzyn.pl w każdej sprawie dotyczącej danych.

3. Pani/Pana dane w postaci wizerunku przetwarzane będą w celu:

- zapewnienia bezpieczeństwa osób przebywających na terenie Urzędu Gminy Nadarzyn, ul. Mszczonowska 24, 05-830 Nadarzyn oraz zabezpieczenia mienia na podstawie art. 6 RODO, wypełnienie obowiązku prawnego ciążącego na Administratorze, wykonanie zadania realizowanego w interesie publicznym.

4. Podstawą do przetwarzania Pani/Pana danych osobowych jest:

- Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. Z 2018 r. poz. 994),
- 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 RODO).

5. Informacja o przekazywaniu danych do innych podmiotów:

Podane przez Panią/Pana dane osobowe będą udostępniane podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa oraz umów. Pani/Pana dane nie będą przekazywane do państwa trzeciego, ani żadnej organizacji międzynarodowej.

6. Okres przechowywania danych:

- Pani/Pana dane osobowe będą przechowywane przez okres 30 dni.

7. W granicach określonych w przepisach prawa ma Pani/Pan prawo do:

- dostępu do swoich danych oraz możliwość ich sprostowania,
- usunięcia lub ograniczenia przetwarzania swoich danych,
- wniesienia sprzeciwu wobec przetwarzania,
- przenoszenia danych,
- cofnięcia wyrażonej zgody na przetwarzanie danych,
- wniesienia skargi do organu nadzorczego.

8. Podanie przez Pana/Panią danych osobowych jest dobrowolne. Przebywanie na terenie Gminy Nadarzyn jest równoznaczne z wyrażeniem zgody na podanie danych osobowych w zakresie wskazanym w pkt. 3. Konsekwencją odmowy udostępnienia tych danych jest brak uprawnienia do przebywania na terenie Gminy Nadarzyn

9. Pani/Pana dane będą przetwarzane w sposób zautomatyzowany – kamery monitoringu nagrywają obraz w sposób ciągły, po upływie 29 dni zapis jest automatycznie nadpisywany. Pani /Pana dane nie podlegają profilowaniu i zautomatyzowanemu systemowi podejmowania decyzji.