

**ZARZĄDZENIE NR ON. 120.20.2020**  
**STAROSTY SIERPECKIEGO**  
z dnia 20.08.2020 r.

**w sprawie wprowadzenia polityki ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Sierpcu .**

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym ( t.j. Dz. U. z 2020 r. poz. 920 z późniejszymi zmianami) oraz art. 24 ust. 2 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. L.2016.119.1 z dnia 4.05.2016 r.) zarządzam co następuje:

**§1.1.** Wprowadzam Politykę ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Sierpcu stanowiącą załącznik do niniejszego zarządzenia.

**2.** Polityka o której mowa w ust. 1 obowiązuje wszystkich pracowników zatrudnionych na stanowiskach urzędniczych, pomocniczych i obsługi, a także osób odbywających staże oraz praktyki zawodowe w Starostwie Powiatowym w Sierpcu.

**3.** Polityka ochrony danych osobowych stanowiąca załącznik do Zarządzenia jest dokumentem wewnętrznym i nie podlega publikacji.

**§ 2.1.** Na stanowisko Administratora Systemów Informatycznych powołuję Pana Michała Chiczewskiego – Starszego Informatyka w Wydziale Organizacji i Nadzoru.

**2.** Do zastępowania Administratora Systemów Informatycznych oraz pomocy w obsłudze administracyjnej Inspektora Ochrony Danych Osobowych wyznaczam podinspektora w Wydziale Organizacji i Nadzoru Pana Łukasza Szpakowskiego.

**§ 3.** Traci moc Zarządzenie Starosty Sierpeckiego Nr ON.120.32.2018 z dnia 24 maja 2018 roku w sprawie dokumentacji przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu.

**§ 4.** Wykonanie Zarządzenia powierza się Inspektorowi Ochrony Danych Osobowych oraz Administratorowi Systemów Informatycznych.

**§ 5.** Zarządzenie wchodzi w życie z dniem podjęcia z mocą obowiązującą od 1 września 2020 roku.

**STAROSTA**  
*Mariusz Turalski*

Jarosław Dołhun  
**ADWOKAT**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100



Załącznik do Zarządzenia  
Nr ON.120. 40 .2020  
Starosty Sierpeckiego  
z dnia 20. 08 2020 roku

ZATWIERDZAM:

  
**STAROSTA**  
*Mariusz Turalski*

**POLITYKA  
OCHRONY DANYCH OSOBOWYCH  
w Starostwie Powiatowym w Sierpcu**

## Spis treści

I.	Spis treści.....	2
II.	Definicje.....	4
III.	Wstęp.....	8
IV.	Określenie obowiązków.....	9
V.	Odpowiedzialność .....	13
VI.	Zapewnienie poufności, integralności oraz rozliczalności danych osobowych...	14
VII.	Zapewnienie realizacji praw i wolności osób, których dane dotyczą.....	17
VIII.	Procedura monitorowania sposobu używania sprzętu i oprogramowania.....	22
IX.	Procedura nadawania i odbierania upoważnień lub uprawnień.....	24
X.	Procedura dostępu do danych osobowych.....	26
XI.	Procedura zabezpieczenia systemu informatycznego.....	28
XII.	Procedura tworzenia kopii zapasowych.....	29
XIII.	Procedura przechowywania elektronicznych nośników informacji.....	30
XIV.	Procedura wykonywania przeglądów i konserwacji.....	31
XV.	Procedura dostępu fizycznego do pomieszczeń.....	32
XVI.	Procedura udostępnienia danych.....	33
XVII.	Procedura powierzenia przetwarzania danych osobowych.....	34
XVIII.	Procedura przeprowadzania szkoleń pracowników.....	36
XIX.	Procedura zgłaszania incydentów.....	37
XX.	Procedura zarządzania ryzykiem.....	41
XXI.	Procedura oceny skutków.....	53
XXII.	Procedura prowadzenia wykazu i rejestrów.....	62
XXIII.	Procedura przeprowadzania audytów zgodności.....	63
XXIV.	Postanowienia końcowe.....	65

## ZAŁĄCZNIKI

Załącznik 1	Wykaz kategorii osób oraz kategorii danych osobowych	66
Załącznik 2	Wzór informacji podawanych w przypadku zbierania danych osobowych	81
Załącznik 3	Wzór informacji podawanych w przypadku pozyskiwania danych osobowych	89
Załącznik 4	Wzór oświadczenia o zachowaniu danych osobowych w poufności	90
Załącznik 5	Wzór nadania upoważnienia do przetwarzania danych osobowych	92
Załącznik 6	Wzór cofnięcia upoważnienia do przetwarzania danych osobowych	93
Załącznik 7	Wzór wniosku o nadanie, zmianę lub odebranie uprawnień w systemie	94
Załącznik 8	Wzór ewidencji osób uprawnionych	97
Załącznik 9	Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych	98
Załącznik 10	Wzór umowy powierzenia przetwarzania danych osobowych	99
Załącznik 11	Wzór rejestru incydentów	106
Załącznik 12	Wzór wykazu podmiotów przetwarzających	107
Załącznik 13	Wzór rejestru czynności przetwarzania danych osobowych	108
Załącznik 14	Wzór rejestru wszystkich kategorii czynności przetwarzania	109
Załącznik 15	Wzór formularza oceny skutków	110

## II. Definicje

<b>Pojęcie adekwatność lub minimalizacja danych</b>	<b>Znaczenie</b> Zasada dotycząca przetwarzania danych osobowych polegająca na tym, że administrator danych powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne do realizacji celu dla którego dane są zbierane;
<b>administrator</b>	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji ochrony danych osobowych przez administratora danych rozumie się Starostwo Powiatowe w Sierpcu;
<b>analiza ryzyka</b>	Proces identyfikacji ryzyka, określania jego wartości i identyfikowanie niezbędnych zabezpieczeń;
<b>anonimizacja</b>	przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań;
<b>audyt zgodności</b>	czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami RODO oraz innymi przepisami o ochronie danych osobowych, a także czynności mające na celu monitorowanie przestrzegania polityki ochrony danych osobowych;
<b>dane biometryczne</b>	dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
<b>dane dotyczące zdrowia</b>	dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;
<b>dane genetyczne</b>	dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
<b>dane osobowe</b>	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;
<b>dane poufne</b>	dane, które nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom;
<b>docelowy poziom ryzyka</b>	docelowy poziom pojedynczego ryzyka, jaki administrator zamierza osiągnąć w odniesieniu do konkretnego ryzyka;
<b>dostępność</b>	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
<b>działania zaradcze</b>	środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;

<b>hasło</b>	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
<b>identyfikator</b>	ciąg znaków literowych, cyfrowych lub innych znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
<b>incydent</b>	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;
<b>integralność</b>	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób;
<b>Inspektor</b>	osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO
<b>istotność ryzyka</b>	ilość i prawdopodobieństwo i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiągnięcie przez administratora zamierzonych celów;
<b>legalność</b>	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane zgodnie z prawem, po spełnieniu przynajmniej jednego z warunków określonych w art. 6 ust. 1 lub art. 9 ust. 2 RODO;
<b>mapa ryzyka</b>	graficzne zestawienie ryzyka z punktu widzenia ich istotności, lub innych kryteriów;
<b>ocena ryzyka</b>	proces porównywania ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka;
<b>odbiorca</b>	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego;
<b>ograniczenie celu</b>	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
<b>okresowość</b>	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane są przetwarzane;
<b>organ nadzorczy</b>	niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolność osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w Unii Europejskiej, zgodnie z art. 51 RODO;
<b>osoba upoważniona</b>	osoba upoważniona przez administratora do przetwarzania danych osobowych nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
<b>podmiot przetwarzający</b>	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
<b>Polityka</b>	niniejszy dokument, tj. Polityka ochrony danych osobowych;
<b>poufność</b>	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
<b>Naczelnik wydziału</b>	osoby pełniące funkcje Naczelników poszczególnych Wydziałów oraz pracowników zatrudnionych na samodzielnych stanowiskach;

<b>komórka właściwa ds. IT</b>	osoba zatrudniona na stanowisku informatyka pracująca w wydziale Organizacji i Nadzoru.
<b>pracownik lub współpracownik</b>	osoba zatrudniona przez Starostwo na podstawie umowy o pracę oraz osoba świadcząca na rzecz Starostwa usługi na podstawie umów cywilnoprawnych, a także praktykanci, wolontariusze, stażyści i studenci;
<b>prawdopodobieństwo</b>	oczekiwana częstość materializacji danego ryzyka;
<b>przetwarzanie</b>	operacja 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;
<b>pseudonimizacja</b>	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;
<b>raport zgodności</b>	dokument opracowywany przez Inspektora Ochrony Danych po dokonaniu audytu zgodności zawierający opis niezgodności przetwarzania danych osobowych z przepisami RODO, innymi przepisami o ochronie danych osobowych oraz Polityką, a także zawierający ogólną ocenę poziomu ochrony danych osobowych;
<b>rejestr czynności przetwarzania danych osobowych</b>	dokument, o którym mowa w art. 30 ust. 1 RODO, prowadzony w formie pisemnej przez administratora, udostępniany organowi nadzorczemu na jego żądanie;
<b>rejestr wszystkich kategorii czynności przetwarzania</b>	dokument, o którym mowa w art. 30 ust. 2 RODO, prowadzony w formie pisemnej przez podmiot przetwarzający, udostępniany organowi nadzorczemu na jego żądanie;
<b>RODO</b>	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
<b>rozliczalność przetwarzania</b>	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
<b>ryzyko</b>	kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji. Ryzyko związane z bezpieczeństwem danych osobowych to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów;
<b>rzetelność</b>	zasada dotycząca przetwarzania danych osobowych zapewniająca merytoryczną poprawność danych osobowych poprzez ich zgodność ze stanem faktycznym, kompletność i aktualność;
<b>skutek</b>	efekt materializacji ryzyka;
<b>Starostwo</b>	Starostwo Powiatowe w Sierpcu ul. w Sierpcu ul. Świętokrzyska 2A 09-200 Sierpc;
	osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż

<b>strona trzecia lub osoba trzecia</b>	osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
<b>system informatyczny</b>	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
<b>szacowanie ryzyka</b>	całościowy proces analizy i oceny ryzyka;
<b>właściciel ryzyka</b>	osoba, która ze względu na zajmowane stanowisko i przydział odpowiedzialności zarządza głównymi czynnikami ryzyka, przypisanego do niej. Właścicielami ryzyka mogą być Starosta, Sekretarz Powiatu, Skarbnik Powiatu, Naczelnicy, kierownicy, samodzielne stanowiska lub pełnomocnicy odpowiadający za zarządzane przez nich procesy przetwarzania danych osobowych;
<b>wpływ</b>	potencjalne skutki materializacji ryzyka;
<b>upoważnienie</b>	oświadczenie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych przez tę osobę;
<b>uwierzytelnianie</b>	działanie, którego celem jest weryfikacja deklarowanej tożsamości, osoby upoważnionej;
<b>zabezpieczenie</b>	środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;
<b>zagrożenie</b>	niepożądane zdarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę;
<b>zarządzanie ryzykiem</b>	skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń;
<b>zbiór danych</b>	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

### III. Wstęp

Tworzy się niniejszą Politykę ochrony danych osobowych celem realizacji obowiązków wynikających z powszechnie obowiązującego prawa, w szczególności 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 lub RODO).

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Aby móc to wykazać administrator wdraża niniejszą Politykę.

Aby przetwarzanie odbywało się w sposób zapewniający należyłą ochronę danych osobowych będących w zasobach administratora, przetwarzanie odbywa się z zachowaniem następujących zasad:

1. zgodności z prawem;
2. rzetelności, przejrzystości i ograniczoności celu;
3. adekwatności, prawidłowości i okresowości przetwarzanych danych;
4. poufności, integralności i rozliczalności danych;
5. odpowiedzialności administratora danych .

Polityka ochrony danych osobowych jest aktualizowana w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych lub w związku ze zmianą stanu faktycznego, które wpływają na treść dokumentu.

Zakres podmiotowy stosowania niniejszej Polityki obejmuje wszystkich pracowników lub współpracowników mających dostęp do danych osobowych.

Żadna procedura ani regulacja wewnętrzna obowiązująca u administratora nie może naruszać zasad określonych w niniejszej Polityce.

Administrator, zgodnie z treścią art. 37 ust. 1 RODO, wyznaczył Inspektora Ochrony Danych, który wykonując zadania zgodnie z art. 39 RODO, podlega bezpośrednio Staroście Sierpeckiemu.

Dane osobowe chronione niniejszą Polityką przetwarzane są w siedzibie administratora danych mieszczącej się w Sierpcu, adres: ul. Świętokrzyska 2a, 09-200 Sierpc, a także w siedzibach podmiotów przetwarzających dane osobowe wskazanych w wykazie podmiotów przetwarzających dane osobowe w imieniu administratora, prowadzonym zgodnie ze wzorem stanowiącym **załącznik nr 12 do niniejszej Polityki**.

## IV. Określenie obowiązków

Administrator jest zobowiązany do:

1. zapewnienia niezbędnych środków do stworzenia i funkcjonowania systemu ochrony danych osobowych;
2. wdrożenia niezbędnych środków organizacyjnych i technicznych zapewniających rozliczalność, integralność oraz poufność przetwarzanych danych osobowych;
3. zapewnienia, by systemy informatyczne wykorzystywane do przetwarzania danych spełniały odpowiednie środki techniczne, zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane są przetwarzane;
4. wdrożenia odpowiednich środków organizacyjnych, zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych;
5. zapewnienia, aby osoby dopuszczone do przetwarzania danych osobowych przestrzegały przepisy o ochronie danych osobowych;
6. zapewnienia, by dostęp do danych osobowych udzielany był wyłącznie osobom upoważnionym do ich przetwarzania;
7. podejmowania odpowiednich środków, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania;
8. zapewniania, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
9. zapewniania, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania przez niego zadań;
10. zatwierdzania Polityki ochrony danych osobowych oraz dokumentów opracowanych na jej podstawie.

**Inspektor Ochrony Danych jest zobowiązany do:**

1. informowania administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisach o ochronie danych osobowych i doradzania im w tym zakresie;
2. monitorowania przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz Polityki administratora poprzez wykonywanie audytów zgodności;
3. opracowywania, po każdorazowym przeprowadzeniu audytu zgodności, raportu dla administratora;
4. nadzorowania wdrażania zabezpieczeń będących wynikiem audytu zgodności oraz analizy ryzyka;
5. podejmowania działań zwiększających świadomość z zakresu ochrony danych osobowych, w tym informowanie o zagrożeniach związanych z dostępem do danych osobowych;
6. szkolenia pracowników uczestniczących w operacjach przetwarzania ;
7. udzielania na żądanie, zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania zgodnie z art. 35 RODO;
8. współpracy z organem nadzorczym;
9. pełnienia roli punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
10. pełnienie roli punktu kontaktowego dla osób, których dane dotyczą;
11. reagowania na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych, analizowanie ich przyczyn oraz kierowanie wniosków dotyczących usprawnienia ochrony danych osobowych i ukarania winnych naruszeń;
12. prowadzenia rejestru incydentów;
13. aktualizacji Polityki ochrony danych osobowych;
14. prowadzenia wykazu podmiotów przetwarzających dane;
15. prowadzenia rejestru czynności przetwarzania danych osobowych;
16. prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu podmiotu powierzającego;
17. przygotowania i bieżącej aktualizacji treści informacji podawanych w przypadku zbierania danych od osoby, której dane dotyczą;
18. przygotowania i bieżącej aktualizacji treści informacji podawanych w przypadku zbierania danych od osobowych w sposób inny niż od osoby, której dane dotyczą.

**Komórka właściwa ds. IT** jest zobowiązana do:

1. nadzorowania stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemie informatycznym;
2. bieżącego utrzymania systemów informatycznych służących do przetwarzania danych osobowych i ich funkcjonowania, zapewniającego ich poufność, integralność i dostępność, m. in. poprzez właściwą aktualizację tych systemów;
3. zarządzania systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji w sposób zapewniający bezpieczeństwo wymiany danych;
4. nadzorowania funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym oraz kontroli dostępu do danych osobowych;
5. wykonywania kopii bezpieczeństwa elektronicznych zbiorów danych osobowych;
6. okresowego sprawdzania kopii bezpieczeństwa pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
7. prowadzenia depozytu kopii bezpieczeństwa i logów danych;
8. przydzielania użytkownikom indywidualnych identyfikatorów i haseł do systemu informatycznego oraz dokonywania ewentualnych modyfikacji uprawnień, a także usuwania kont użytkowników;
9. okresowego zmieniania haseł dostępu użytkowników do systemu informatycznego w przypadkach, gdy system informatyczny nie wymusza okresowej zmiany haseł użytkowników;
10. prowadzenia bieżącej ewidencji wszystkich użytkowników systemów informatycznych uprawnionych do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym **załącznik nr 8 do niniejszej Polityki** ;
11. osobistego wykonywania lub sprawowania nadzoru na wykonaniu napraw, konserwacji oraz likwidacji urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe;
12. uczestniczenia w procesie zakupów aplikacji oraz oprogramowania zatwierdzonego do włączenia do sytemu informatycznego służącego do przetwarzania danych osobowych;
13. zapewnienia legalności oprogramowania wykorzystywanego w systemie informatycznym służącym do przetwarzania danych osobowych oraz zarządzania licencjami do odpowiednich elementów systemu informatycznego;
14. zapewnienia właściwej konfiguracji systemów zarządzania hasłami;
15. inwentaryzacji sprzętu komputerowego oraz systemów informatycznych;
16. bieżącej inwentaryzacji przepływów danych osobowych pomiędzy systemami służącymi do przetwarzania danych osobowych;
17. prowadzenie, przy współpracy z Inspektorem, postępowania wyjaśniającego w sytuacji wystąpienia naruszenia ochrony danych osobowych.

**Osoba upoważniona do przetwarzania danych, która otrzymała polecenie przetwarzania danych z chwilą podpisania umowy o pracę i zakresu czynności, uprawnień i obowiązków jest zobowiązana do:**

1. przestrzegania przyjętych u administratora zasad ochrony danych osobowych ze szczególnym uwzględnieniem zasady bezpieczeństwa;
2. informowania bezpośredniego przełożonego lub komórkę właściwą ds. IT o incydentach godzących w bezpieczeństwo danych osobowych;
3. dochowywania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane są przetwarzane;
4. zachowania w poufności przetwarzanych danych osobowych oraz sposobów ich zabezpieczania;
5. usuwania danych osobowych, które administrator pozyskuje lub są na rzecz administratora przekazywane, zawsze wtedy, gdy administrator nie posiada interesu prawnego i faktycznego w przetwarzaniu (w tym archiwizacji) tych danych. W razie wątpliwości, co do obowiązku usunięcia danych osobowych, osoba upoważniona powinna zwrócić się o opinię do Inspektora;
6. uporządkowania swojego stanowiska pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności: zabezpieczenia komputerów i wszelkich nośników danych, wyłączenia wszystkich urządzeń elektrycznych (niewymagających stałego zasilania), zamknięcia okien i drzwi oraz zdania kluczy po zakończeniu pracy.

## V. Odpowiedzialność

**Administrator** za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83 lub 84 RODO.

**Podmiot przetwarzający** za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83 i 84 RODO.

**Osoba upoważniona** za naruszenie ochrony danych osobowych może ponieść odpowiednio odpowiedzialność wskazaną w art. 52 lub 208 kodeksu pracy albo odpowiedzialność kontraktową przewidzianą w art. 471 kodeksu cywilnego. Osoba upoważniona może także ponieść odpowiedzialność karną przewidzianą w art. 266 kodeksu karnego.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki, potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku wykrycia incydentu lub uzasadnionego podejrzenia, powstania incydentu nie podjęła działania określonego w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie udokumentowała takiego przypadku, może zostać wszczęte postępowanie dyscyplinarne.

Kara dyscyplinarna nałożona na osobę uchylającą się od powiadomienia, o którym mowa powyżej, nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości kierowania wobec takiej osoby roszczeń cywilnych przez administratora o zrekompensowanie poniesionych strat .

## **VI. Zapewnienie poufności, integralności oraz rozliczalności danych osobowych**

Administrator zapewnia poufność, integralność oraz rozliczalność przetwarzanych danych osobowych, poprzez zastosowanie niezbędnych środków organizacyjnych oraz technicznych.

Dobór powyższych środków ma na celu obniżyć poziom ryzyka wystąpienia incydentów, związanych z bezpieczeństwem przetwarzania danych osobowych, do poziomu akceptowalnego przez administratora.

Wprowadzenie omawianych środków, zostało poprzedzone przeprowadzeniem analizy kosztów ich wdrożenia w odniesieniu do stopnia bezpieczeństwa przetwarzania danych osobowych, jaki administrator zamierza osiągnąć po ich wdrożeniu.

**W ramach grupy środków organizacyjnych wprowadza się, w szczególności:**

1. monitorowanie przestrzegania niniejszej Polityki przez wyznaczonego Inspektora Ochrony Danych;
2. nadzór środowiska informatycznego przez kierownika komórki właściwej ds. IT;
3. upoważnienia do przetwarzania danych osobowych, które są wydawane każdemu pracownikowi zgodnie z zakresem obowiązków;
4. ewidencję upoważnień do przetwarzania danych osobowych;
5. oświadczenia o zachowaniu w poufności danych osobowych i sposobów zabezpieczenia danych, które są zbierane od osób upoważnionych;
6. szkolenia dla osób upoważnionych z zasad bezpiecznego przetwarzania danych osobowych;
7. umowy powierzenia w rozumieniu art. 28 ust. 3 RODO, zawierane z podmiotami przetwarzającymi dane w imieniu administratora danych;
8. ewidencję umów powierzenia;
9. rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 RODO;
10. zasadę, zgodnie z którą osoby trzecie przebywają w obszarze przetwarzania danych wyłącznie w obecności osoby upoważnionej. Osoby trzecie mogą w wyjątkowych okolicznościach przebywać bez obecności osoby upoważnionej - w obszarze przetwarzania danych - po uprzednim wydaniu na to zgody przez administratora danych.

Ponadto, została określona odpowiedzialność pracownika lub podmiotu przetwarzającego za działania związane z naruszeniem bezpieczeństwa przetwarzania danych osobowych.

**W ramach grupy środków technicznych, wprowadza się w szczególności:**

1. zabezpieczenia techniczne zapewniające poufność przetwarzanych danych osobowych:
  - 1) nadzór Agencji Ochrony – realizacja po wystąpieniu alarmu;
  - 2) obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych lub kart wejściowych;
  - 3) dane osobowe przetrzymywane w formie papierowej są przechowywane w zamkniętych szafkach, szafach lub szufladach;
  - 4) dostęp do danych w systemie informatycznym jest możliwy wyłącznie po udanym uwierzytelnieniu użytkownika;
  - 5) hasła składają się z min. 8 znaków (małe, wielkie litery, przynajmniej jedna cyfra lub znak specjalny);
  - 6) hasła są zmieniane nie rzadziej niż co 30 dni;
  - 7) na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
  - 8) monitorowanie działania systemu informatycznego;
  - 9) logiczna i fizyczna separacja sieci;
  - 10) logiczny dostęp do danych osobowych z sieci publicznej ograniczony jest przez zastosowanie zapory ogniowej (firewall). Chroni ona wszystkie systemy informatyczne przed nieuprawnionym dostępem i atakami z zewnątrz.
  
2. zabezpieczenia techniczne zapewniające integralność przetwarzanych danych osobowych:
  - 1) ochrona przed nieautoryzowanym dostępem;
  - 2) na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
  - 3) awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS;
  - 4) właściwe okablowanie sieci;
  - 5) cykliczna weryfikacja integralności baz danych poprzez odtwarzanie danych zawartych na kopiach zapasowych.
  
3. zabezpieczenia techniczne zapewniające rozliczalność przetwarzanych danych osobowych:
  1. dostęp do danych w systemie informatycznym, możliwy wyłącznie po udanym uwierzytelnieniu użytkownika;
  2. awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS;
  3. zapis zdarzeń w systemach informatycznych.

**Przetwarzanie danych osobowych poza obszarem przetwarzania dopuszczalne jest wyłącznie po spełnieniu poniższych przesłanek:**

1. zachowanie szczególnej ostrożności podczas transportu, przechowywania i użytkowania nośników zawierających dane osobowe;
2. stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych;
3. zakaz pozostawiania nośników zawierających dane osobowe w miejscach powszechnie dostępnych;
4. wykorzystywanie nośników wyłącznie w celach służbowych.

**Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:**

1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie;
3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób umożliwiający ich odzyskanie.

## VII. Zapewnienie realizacji praw i wolności osób, których dane dotyczą.

Administrator ma świadomość, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach.

Administrator zapewniając realizację praw i wolności osób, których dane dotyczą, podjął odpowiednie, środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania.

Zapewniając realizację praw i wolności osób, których dane dotyczą administrator ustala następujące zasady:

1. Informacji udziela się na piśmie lub w inny sposób, w tym elektronicznie.
2. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
3. Informacji udziela się bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – osobie, której dane dotyczą, udziela się informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO.
4. Jeżeli osoba wskazana do udzielenia informacji ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21, powinna zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
5. W przypadku przetwarzania niewymagającego identyfikacji, tam gdzie administrator nie jest w stanie zidentyfikować podmiotu danych, można odmówić podjęcia żądanego działania.
6. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, przedstawia się tej osobie klauzule informacyjne o treści i w miejscach lub dokumentach wskazanych w **załączniku nr 2 do niniejszej Polityki**.
7. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, przedstawia się jej klauzule informacyjne o treści i w miejscach lub dokumentach wskazanych w **załączniku nr 3 do niniejszej Polityki**.
8. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane zostały pozyskane, przed dalszym przetwarzaniem informuje osobę której dane dotyczą o tym innym celu oraz udziela jej wszelkich innych stosowanych informacji, o których mowa odpowiednio w pkt. 6 lub 7.
9. Administrator, bez zbędnej zwłoki, informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
10. Administrator zapewnia realizację następujących praw i wolności osób, których dane dotyczą:

## **Prawo dostępu przysługujące osobie, której dane dotyczą**

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz uzyskania informacji, określających:

- 1) cele przetwarzania;
- 2) kategorie odnośnych danych osobowych;
- 3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- 4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- 5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- 6) informacje o prawie wniesienia skargi do organu nadzorczego;
- 7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
- 8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.

Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w wysokości wynikającej z kosztów administracyjnych.

Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną równocześnie nie wskazując formy ich przekazania, informacji udziela się drogą elektroniczną.

## **Prawo do sprostowania danych**

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

## **Prawo do bycia zapomnianym**

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania jej danych osobowych;
3. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
4. dane osobowe były przetwarzane niezgodnie z prawem;
5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator;
6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Jeżeli administrator upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Prawo do usunięcia danych nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

1. do korzystania z prawa do wolności wypowiedzi i informacji;
2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do bycia zapomnianym, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
5. do ustalenia, dochodzenia lub obrony roszczeń.

## **Prawo do ograniczenia przetwarzania**

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

1. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
4. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli zgodnie z żądaniem przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Przed uchycieniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia przetwarzania.

### **Prawo do przenoszenia danych**

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

1. przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; oraz
2. przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku prawa do bycia zapomnianym. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Administrator odmawia realizacji prawa do przenoszenia danych w sytuacji, gdy realizacja tego prawa może niekorzystnie wpływać na prawa i wolności innych osób.

## Prawo do sprzeciwu

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczącego jej danych osobowych, gdy:

1. przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
2. przetwarzanie danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, 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.

Administratorowi nie wolno już przetwarzać danych osobowych w sytuacji skorzystania z prawa do sprzeciwu, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wnieśli sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

## VIII. Procedura monitorowania sposobu używania sprzętu i oprogramowania

Celem niniejszej procedury jest określenie zasad korzystania ze sprzętu i oprogramowania, które administrator powierzył pracownikom, w celu niezbędnym do prawidłowego wykonywania powierzonych zadań.

1. Administrator wyposażył pracownika w sprzęt, w tym sprzęt komputerowy (dalej „Sprzęt”) i oprogramowanie komputerowe (dalej „Oprogramowanie”) niezbędne do prawidłowego wykonywania powierzonych zadań. Pracownik w trakcie wykonywania tych zadań może mieć dostęp do informacji stanowiących: tajemnicę, dane osobowe, dane poufne lub dane, co do których administrator zobowiązał się do ich zabezpieczenia przed nieuprawnionym ujawnieniem.
2. Pracownik może korzystać ze Sprzętu i Oprogramowania wyłącznie w celu wykonywania powierzonych obowiązków, zgodnie z obowiązującymi przepisami prawa. Powyższy obowiązek należy do podstawowych obowiązków pracowniczych z uwagi na konieczność dbałości o mienie administratora.
3. Pracownik jest zobowiązany do:
  - 1) niekorzystania z jakiegokolwiek oprogramowania komputerowego innego niż Oprogramowanie, w szczególności niedokonywania instalacji takiego oprogramowania na Sprzęcie;
  - 2) niekorzystania ze Sprzętu i Oprogramowania w celach prywatnych, w szczególności poprzez prowadzenie korespondencji e-mail niezwiązanej ze świadczeniem pracy, poprzez korzystanie z komunikatorów, portali społecznościowych, witryn www, innych niż konieczne do wykonywania obowiązków pracowniczych;
  - 3) niekorzystania z Oprogramowania w sposób mogący naruszyć prawa osób trzecich, w tym niekopiowania i nierozpowszechniania Oprogramowania;
  - 4) niezwłocznego udostępniania administratorowi, na każde żądanie, Sprzętu i Oprogramowania celem umożliwienia wykonania kontroli, o której mowa w pkt 4 niniejszej Procedury.
4. Administrator może przeprowadzić sprawdzenie należytego wykonania niniejszej polityki. Sprawdzenie może być wykonane przez wyznaczonego pracownika komórki właściwej ds. IT, lub Inspektora poprzez:
  - 1) monitoring operacji wykonywanych na Sprzęcie;
  - 2) sprawdzanie wykazu połączeń telefonicznych;
  - 3) kontrolę zainstalowanego Oprogramowania i sposobu korzystania z niego;
  - 4) kontrolę czasu pracy przy wykorzystaniu Sprzętu i Oprogramowania;
  - 5) kontrolę aktywności w sieci Internet;
  - 6) kontrolę wysyłanej poczty służbowej;
  - 7) kontrolę przeprowadza się osobiście lub przez wykorzystanie odpowiedniego oprogramowania
5. Bezwzględnie zabronione jest wykorzystywanie Sprzętu lub Oprogramowania w celach niezgodnych z prawem lub zasadami obowiązującymi u administratora, a w szczególności w celach:
  - 1) korzystania z treści pornograficznych;
  - 2) naruszania praw autorskich (nielegalnego pobierania bądź udostępniania plików);
  - 3) infekowania sieci komputerowej wirusami pobieranymi z plikami z Internetu;

- 4) korzystania ze służbowej poczty elektronicznej w sprawach prywatnych.
6. W związku z naruszeniem zasad niniejszej polityki pracownik może podlegać odpowiedzialności karnej, o której stanowi ustawa z dnia 6 czerwca 1997 r. Kodeks karny oraz odpowiedzialności karnej i cywilnej przewidzianej w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania oraz odpowiedzialności karnej określonej w art. 51 ustawy.
7. Naruszenie przez pracownika jego obowiązków pracowniczych w zakresie wskazanym w niniejszej Polityce może stanowić podstawę do podjęcia przez Starostwo przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą wypowiedzenie przez Starostwo umowy o pracę łączącej Starostwo z pracownikiem lub wymierzenie kary porządkowej przewidzianej przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy

## IX. Procedura nadawania i odbierania upoważnień lub uprawnień

Celem niniejszej procedury jest określenie zasad nadawania upoważnień do przetwarzania danych osobowych oraz uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych.


1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, użytkownikom nadaje komórka właściwa ds. IT,
2. Przed nadaniem użytkownikowi dostępu do systemu informatycznego:
  - 1) Sekretarz Powiatu zapoznaje pracownika z przepisami RODO oraz regulacjami wewnętrznymi administratora danych w obszarze przetwarzania danych, w tym Polityki ochrony danych osobowych, odbiera od pracownika( stażysty, praktykanta ) oświadczenie o zachowaniu danych w poufności wg wzoru stanowiącego **załącznik Nr 4** do Polityki i przekazuje do Wydziału Organizacji i Nadzoru,
  - 2) wyznaczony do wydawania upoważnień pracownik Wydziału Organizacji i Nadzoru odbiera od użytkownika oświadczenie o zachowaniu danych osobowych w poufności,
3. Wydział Organizacji i Nadzoru przygotowuje upoważnienie do przetwarzania danych, którego **wzór stanowi załącznik nr 5 do niniejszej Polityki**, w zakresie wynikającym z zajmowanego stanowiska.
4. Upoważnienie do przetwarzania danych podpisuje administrator lub osoba posiadająca odrębne pełnomocnictwo administratora.
5. Wydział Organizacji i Nadzoru prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, **której wzór stanowi załącznik nr 9 do niniejszej Polityki**.
6. Wydział Organizacji i Nadzoru jest obowiązany niezwłocznie odnotować fakt cofnięcia upoważnienia w ewidencji osób upoważnionych do przetwarzania danych osobowych.
7. Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru. Egzemplarz z potwierdzeniem odbioru wraz z oświadczeniem o zachowaniu danych osobowych w poufności pracownik ds. kadr załącza do akt osobowych pracownika.
8. Naczelnik wydziału, po podpisaniu upoważnienia przez administratora, składa do komórki właściwej ds. IT wniosek o nadanie uprawnień w systemie, **którego wzór stanowi załącznik nr 7 do niniejszej Polityki**.
9. Komórka właściwa ds. IT, niezwłocznie po otrzymaniu wniosku o nadanie uprawnień, przyznaje dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe.
10. Nadanie uprawnień do systemu informatycznego polega na przydzieleniu unikalnego identyfikatora i hasła.
11. Komórka właściwa ds. IT prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w systemie informatycznym, **której wzór stanowi załącznik nr 8 do niniejszej Polityki**. Ewidencja zawiera w szczególności: identyfikator użytkownika systemu, datę nadania oraz odebrania uprawnień.

12. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych, możliwy jest wyłącznie po podaniu unikalnego identyfikatora i hasła. Nadane przez komórkę właściwą ds. IT hasło jest hasłem startowym, które użytkownik jest zobowiązany zmienić na hasło spełniające wymagania, o których mowa w rozdziale „Procedura dostępu do danych osobowych”.
13. Użytkownik odbiera identyfikator i hasło startowe osobiście od komórki właściwej ds. IT - legitymując się dokumentem ze zdjęciem.
14. Procedurę nadania uprawnień stosuje się odpowiednio w przypadku zmiany uprawnień, przy czym wniosek o nadanie uprawnień zastępuje wniosek o zmianę uprawnień, którego **wzór stanowi załącznik nr 7 do niniejszej Polityki**.
15. Zmiana uprawnień, w tym odebranie uprawnień może mieć charakter czasowy lub trwały.
16. Odebranie uprawnień następuje przez:
  - 1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (odebranie uprawnień czasowe),
  - 2) usunięcie danych użytkownika z bazy użytkowników systemu (odebranie uprawnień trwałe).
17. Identyfikator osoby, której odebrano uprawnienia trwale, należy niezwłocznie usunąć oraz unieważnić jej hasło.

## **X. Procedura dostępu do danych osobowych**

Celem niniejszej procedury jest określenie zasad dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz obowiązków związanych z rozpoczęciem, zawieszeniem i zakończeniem pracy.

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu indywidualnego identyfikatora i właściwego hasła. W identyfikatorze pomija się znaki diakrytyczne.
2. W przypadku trzech nieudanych prób uwierzytelnienia hasła, celem zabezpieczenia systemu przed próbą włamania, następuje automatyczne zablokowanie dostępu użytkownika do systemu. Odblokowanie dostępu użytkownika do systemu wymaga interwencji pracownika komórki właściwej ds. IT, który nadaje użytkownikowi nowe hasło startowe.
3. W systemie stosuje się uwierzytelnianie przynajmniej jednostopniowe: na poziomie dostępu do sieci lokalnej. Tam gdzie to możliwe stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji lub programu.
4. Identyfikator użytkownika w aplikacji lub programie (o ile działanie aplikacji lub programu na to pozwala) powinien być tożsamy z tym, jaki jest mu przydzielony w sieci lokalnej.
5. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni.
6. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po odebraniu uprawnień użytkownika w systemie informatycznym nie powinien być przydzielony innej osobie.
7. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł. Zabronione jest udostępnianie przez użytkownika swojego identyfikatora i hasła innym osobom, a także korzystanie z identyfikatora i hasła innego użytkownika. Zabrania się również przechowywania haseł w miejscach dostępnych innym osobom, np. pod klawiaturą, na monitorze lub w niezabezpieczonej szafce.
8. Hasło należy wprowadzać do systemu informatycznego w sposób, który uniemożliwia innym osobom jego poznanie.
9. W sytuacji, gdy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do samodzielnej zmiany hasła i powiadomienia o tym incydencie komórki właściwej ds. IT.
10. Hasło powinno składać się z zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika w jakiegokolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani jego imieniem lub nazwiskiem.
11. Niedozwolone jest stosowanie haseł, którymi użytkownik posługiwał się uprzednio w okresie minionego roku.

12. Kombinacja hasła nie powinna zawierać ogólnie dostępnych informacji o użytkowniku, np. imienia i nazwiska, numeru telefonu, numeru rejestracyjnego samochodu, marki samochodu lub przewidywanych sekwencji z klawiatury (np.: „QWERTY” i „12345” itp.).
13. Nie należy korzystać z opcji zapamiętywania hasła w systemie.
14. Komórka właściwa ds. IT jest odpowiedzialna za sprawdzenie, a następnie usuwanie lub blokowanie zbędnych identyfikatorów użytkowników.
15. Naczelnik wydziału z chwilą powzięcia informacji o rozwiązaniu umowy z pracownikiem zobowiązany jest niezwłocznie - nie później niż tego samego dnia co jej rozwiązanie - przekazać komórce właściwej ds. IT wniosek o odebranie uprawnień w systemie, **którego wzór stanowi załącznik nr 7 do niniejszej Polityki**.
16. Po otrzymaniu wniosku o odebranie uprawnień od kierownika komórki organizacyjnej, komórka właściwa ds. IT z dniem rozwiązania umowy lub zmiany stanowiska z pracownikiem, odpowiednio odbiera lub zmienia uprawnienia w systemie informatycznym.
17. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w szafie metalowej, do której mają dostęp wyłącznie: Starosta, Wicestarosta, Sekretarz Powiatu oraz pracownik komórki właściwej ds. IT, lub w inny sposób, umożliwiający dostęp do niego wyłącznie Staroście, Wicestarości, Sekretarzowi Powiatu oraz pracownikowi komórki właściwej ds. IT.
18. Rozpoczęcie pracy na stacji roboczej odbywa się po prawidłowym uwierzytelnieniu użytkownika.
19. Każdorazowe zaprzestanie pracy w systemie informatycznym, wymaga zabezpieczenia systemu przed nieuprawnionym dostępem, np. poprzez zablokowanie stacji roboczej przy użyciu komendy „Ctrl+Alt+Del i Zablokuj” lub „+L”. Użytkownik jest zobowiązany wyłączyć monitor w sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć osoba nieuprawniona. Na komputerze użytkownika nie wykonujących żadnych czynności przez 10 minut zostanie automatycznie uruchomiony wygaszacz ekranu, którego odblokowanie odbywa się po wpisaniu hasła.
20. Użytkownik przed wyłączeniem stacji roboczej i opuszczeniem stanowiska pracy powinien wylogować się z systemu informatycznego oraz sprawdzić, czy nie zostały pozostawione niezabezpieczone elektroniczne nośniki zawierające dane osobowe.
21. Użytkownik udostępniający stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązany jest wylogować się z systemu.
22. Przy przetwarzaniu danych osobowych na komputerach przenośnych stosuje się procedury określone powyżej. Użytkownicy korzystający z komputerów przenośnych zobowiązani są do ochrony ich przed kradzieżą i dostępem osób nieuprawnionych.

## **XI. Procedura zabezpieczenia systemu informatycznego**

Celem niniejszej procedury jest określenie zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi.

1. Na każdej stacji roboczej, komputerze przenośnym i serwerze musi być zainstalowane oprogramowanie antywirusowe, które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
2. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak, aby przynajmniej raz w tygodniu sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
7. Przeprowadza się cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co 3 miesiące.
8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości, zgłoszonych przez użytkownika, w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa, oraz wszystkie posiadane przez użytkownika nośniki.
10. Użytkownik jest obowiązany zawiadomić komórkę właściwą ds. IT o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
11. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
12. Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym Firewall.

## **XII. Procedura tworzenia kopii zapasowych**

Celem niniejszej procedury jest określenie zasad tworzenia kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym służącym do przetwarzania danych osobowych.

1. Odpowiedzialnym za tworzenie i przechowywanie u administratora kopii zapasowych danych osobowych przetwarzanych w zbiorach danych w sposób zgodny z przepisami prawa oraz poniższymi zasadami jest pracownik komórki właściwej ds. IT.
2. Kopie zapasowe danych osobowych wykonywane są codziennie, w sposób automatyczny i zawierają pełny obraz danych osobowych.
3. Kopie zapasowe przechowuje się odpowiednio zabezpieczone przed dostępem osób nieuprawnionych w innych pomieszczeniach niż serwerownia przez okres 7 dni wstecz.
4. Kopie zapasowe testuje się okresowo, nie rzadziej niż co pół roku.
5. Kopie zapasowe danych osobowych przetwarzanych po ustaniu ich użyteczności są bezzwłocznie usuwane.
6. Kopie zapasowe przetwarzanych danych osobowych, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.
7. Dostęp do kopii zapasowych ma Naczelnik komórki właściwej ds. IT oraz inne osoby wskazane przez Naczelnika komórki właściwej ds. IT.
8. Użytkownicy stacji roboczej są zobowiązani do samodzielnego wykonywania kopii zapasowych danych osobowych zapisanych na dysku stacji roboczej. Kopie wykonywane są na imiennym katalogu umieszczonym na zasobie sieciowym.
9. Niniejsza procedura nie ma zastosowania do systemu informatycznego służącego do przetwarzania danych osobowych z użyciem sieci publicznej, oraz których serwery zlokalizowane są poza siedzibą administratora. W takim jednak wypadku konfiguracja ww. serwerów powinna zapewniać wykonywanie kopii zapasowych.

### **XIII. Procedura przechowywania elektronicznych nośników informacji**

Celem niniejszej procedury jest określenie zasad przechowywania elektronicznych nośników informacji takich jak: pendrive, dyskietka, dysk magnetoptyczny, dysk twardy lub komputer przenośny.

1. Nośniki danych osobowych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetoptycznych czy dyskach twardych nie są wynoszone poza siedzibę administratora. Nie dotyczy to komputerów przenośnych, które mogą być wynoszone poza siedzibę administratora.
3. Po zakończeniu pracy przez użytkowników systemu wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób mechaniczny uniemożliwiający ich odczytanie.
6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.
7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych.
8. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.
9. W przypadku konieczności przechowywania wydruków zawierających dane osobowe, należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
10. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

## **XIV. Procedura wykonywania przeglądów i konserwacji**

Celem niniejszej procedury jest określenie zasad wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

1. Za bezawaryjną pracę systemu IT, w szczególności serwerów, stacji roboczych, aplikacji serwerowych, baz danych, poczty e-mail – odpowiada komórka właściwa ds. IT.
2. Przeglądu lub konserwacji systemu dokonuje doraźnie komórka właściwa ds. IT.
3. Przegląd lub konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
4. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada komórka właściwa ds. IT.
5. Nieprawidłowości ujawnione w trakcie dokonywania przeglądu lub konserwacji powinny być niezwłocznie usunięte, a ich przyczyny powinny być przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Inspektora.
6. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji, oprogramowania lub systemów serwerowych (log systemowy) komórka właściwa ds. IT dokonuje nie rzadziej niż raz na miesiąc lub przy wykorzystaniu oprogramowania.
7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać na zasadach określonych w umowie zawartej pomiędzy administratorem a podmiotem zewnętrznym.
8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nieposiadające upoważnień do przetwarzania danych osobowych (np. specjalistów z firm zewnętrznych), muszą być wykonywane wyłącznie pod nadzorem osób upoważnionych do przetwarzania danych osobowych.

## XV. Procedura dostępu fizycznego do pomieszczeń

Celem niniejszej procedury jest określenie zasad pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe.

1. Obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych.
2. Kluczy do pomieszczeń, w których przetwarzane są dane osobowe powinny być pobierane przed rozpoczęciem pracy oraz zdawane po jej zakończeniu z przeznaczonej do tego gabloty.
3. Klucze do pomieszczeń przechowywane są w sposób uporządkowany w zamkniętej gablocie.
4. Klucze zapasowe i kody do pomieszczeń przechowywane są w zamkniętej gablocie przeznaczonej na zapasowe klucze.
5. Odpowiedzialni za klucze od momentu pobrania do zdania są naczelnicy wydziałów, kierownicy, pracownicy zatrudnieni na samodzielnych stanowiskach.
6. Wydanie kluczy zapasowych oraz kodów dostępu do pomieszczeń wyposażonych w instalacje alarmową i innych kluczy zapasowych do pomieszczeń biurowych, może nastąpić tylko w sytuacjach awaryjnych/ kryzysowych na polecenie:
  - 1) Starosty
  - 2) Wicestarosty
  - 3) Sekretarza
  - 4) Naczelnika Wydziału ( w ramach podległego mu wydziału).
7. Komórka właściwa ds. organizacyjnych zobowiązana jest do sporządzenia notatki służbowej w sytuacji wydania kluczy zapasowych lub kodów dostępu do pomieszczeń wyposażonych w instalację alarmową.
8. Każdy przypadek utraty, uszkodzenia lub zniszczenia klucza wymaga zgłoszenia Sekretarzowi Powiatu.
9. Zabrania się:
  - 1) dorabiania kluczy do pomieszczeń bez zgody Sekretarza Powiatu,
  - 2) udostępniania kluczy oraz kodów dostępu do pomieszczeń wyposażonych w instalację alarmową osobom nieupoważnionym,
  - 3) pozostawiania otwartych pomieszczeń lub kluczy bez dozoru.
10. Każdy przypadek utraty, uszkodzenia lub zniszczenia klucza wymaga zgłoszenia Sekretarzowi Powiatu.

## **XVI. Procedura udostępnienia danych**

Celem niniejszej procedury jest określenie zasad udostępniania danych osobom, których dane dotyczą, a także organom publicznym, które wnioskuje o udostępnienie danych osobowych w ramach prowadzonego przez te organy postępowania.

1. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.
2. W przypadku wniosku o udostępnienie danych, każda osoba, do której wpłynie taki wniosek, a która ma uzasadnione wątpliwości czy udostępnienie danych będzie zgodne z przepisami prawa, jest zobowiązana przekazać wniosek do Inspektora.
3. Inspektor rozpatruje przekazany wniosek oraz ustala czy wniosek o udostępnienie:
  - 1) jest sporządzony w formie pisemnej;
  - 2) wystarczająco identyfikuje osobę, której dane mają być udostępnione;
  - 3) wskazuje odpowiednią podstawę prawną udostępnienia danych;
  - 4) określa zakres danych osobowych, których wniosek o udostępnienie danych osobowych dotyczy.
4. Inspektor ocenia, czy można legalnie udostępnić dane osobowe i podejmuje decyzję, którą następnie administrator przekazuje odbiorcy wniosku.
5. W razie braków formalnych wniosku o udostępnienie danych osobowych, administrator zwraca się do wnioskodawcy o ich usunięcie we wskazanym terminie pod rygorem pozostawienia wniosku bez rozpoznania.
6. Po uzyskaniu pozytywnej opinii od Inspektora w przedmiocie dopuszczalności udostępnienia danych osobowych, administrator bez zbędnej zwłoki udostępnia dane osobowe.
7. Dane osobowe powinny być udostępnione w sposób zapewniający ich poufność wobec osób postronnych.
8. Po uzyskaniu negatywnej opinii od Inspektora w przedmiocie dopuszczalności udostępnienia danych osobowych, administrator nie udostępnia danych osobowych.

## **XVII. Procedura powierzenia przetwarzania danych osobowych**

Celem niniejszej procedury jest określenie zasad i zapewnienie, że administrator korzysta z usług podmiotów przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.

1. Administrator dokłada należytej staranności, by przetwarzanie danych osobowych przez podmiot przetwarzający odbywało się na podstawie pisemnej umowy między administratorem a podmiotem przetwarzającym, **której wzór stanowi załącznik nr 10 do niniejszej Polityki.**
2. Podmiot przetwarzający, któremu administrator powierzył przetwarzanie danych osobowych, nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora.
3. W umowie powierzenia przetwarzania danych osobowych należy zastrzec, że podmiot przetwarzający ma obowiązek poinformować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, która określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
5. Umowa powierzenia przetwarzania danych osobowych stanowi w szczególności, że podmiot przetwarzający:
  - 1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
  - 2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
  - 3) podejmuje wszelkie środki by uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku;
  - 4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego;
  - 5) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
  - 6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków nałożonych na administratora w RODO; po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazuje przechowywanie danych osobowych;

- 7) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w umowie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
6. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający na mocy umowy powinny zostać nałożone te same obowiązki ochrony danych jak w umowie między administratorem a podmiotem przetwarzającym.
7. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego powinna spoczywać na pierwotnym podmiocie przetwarzającym.

## **XVIII. Procedura przeprowadzania szkoleń pracowniczych**

Celem niniejszej procedury jest określenie zapewnienia realizacji zadania Inspektora Ochrony Danych jakim jest informowanie pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów z zakresu ochrony danych osobowych, a także na mocy niniejszej Polityki.

1. Każda osoba upoważniona do przetwarzania danych osobowych, przed dopuszczeniem do pracy, jest poddawana szkoleniu „stanowiskowemu”, które przeprowadza jego bezpośredni przełożony lub osoba wyznaczona przez bezpośredniego przełożonego.
2. Szkolenie stanowiskowe obejmuje zaznajomienie pracownika z regulacjami wewnętrznymi obowiązującymi u administratora, w tym z niniejszą Polityką, a także omówienie sposobu bezpiecznego postępowania z danymi osobowymi, przetwarzanymi w związku z wykonywaniem zadań wynikających z umowy o pracę i powierzonych w zakresie czynności .
3. Przynajmniej raz w roku Inspektor przeprowadza szkolenia grupowe dla wszystkich pracowników, którzy przetwarzają dane osobowe. Szkolenie obejmuje swym zakresem omówienie obowiązków spoczywających na pracownikach przetwarzających dane osobowe na mocy RODO oraz innych przepisów z zakresu ochrony danych osobowych, a także na mocy niniejszej Polityki.
4. Administrator zapewnia odpowiednie warunki do przeprowadzenia szkoleń grupowych.
5. Pracownicy potwierdzają swój udział w szkoleniu własnoręcznym podpisem na liście obecności, którą przechowuje Inspektor.

## **XIX. Procedura zgłaszania incydentów**

Procedura definiuje katalog zagrożeń i incydentów mogących prowadzić do naruszenia bezpieczeństwa danych osobowych przetwarzanych przez administratora (również tych danych, które zostały powierzone na rzecz administratora przez inny podmiot) oraz sposób reagowania na ww. zagrożenia i incydenty.

Celem opracowania procedury jest ograniczenie skutków wystąpienia incydentów godzących w bezpieczeństwo przetwarzania danych osobowych oraz zmniejszenie ryzyka ich powstania w przyszłości.

Procedura dzieli się na:

1. Postępowanie wewnętrzne;
2. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu;
3. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

### **Postępowanie wewnętrzne**

1. Każdy pracownik administratora, w przypadku stwierdzenia zagrożenia lub podejrzenia naruszenia zasad ochrony danych osobowych, zobowiązany jest do niezwłocznego zgłoszenia o ww. okolicznościach bezpośredniego przełożonego lub komórkę właściwą ds. IT. Bezpośredni przełożony lub pracownik komórki właściwej ds. IT w przypadku powzięcia powyższej informacji zobowiązany jest do jej niezwłocznego przekazania Inspektorowi.
2. Rodzaje najczęściej występujących zagrożeń bezpieczeństwa danych osobowych:
  - 1) niewłaściwe zabezpieczenie stacji roboczych, komputerów przenośnych, tabletów, smartphonów, nośników przenośnych oraz oprogramowania IT przed kradzieżą, zniszczeniem lub utratą danych osobowych;
  - 2) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń oraz dokumentów;
  - 3) nieprzestrzeganie przyjętych zasad ochrony danych osobowych przez upoważnione osoby.
3. Przykładowe incydenty naruszające zasadę bezpieczeństwa danych osobowych:
  - 1) incydenty losowe zewnętrzne np. pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
  - 2) incydenty losowe wewnętrzne np. awarie stacji roboczych, awarie serwera, awarie oprogramowania, utrata lub zgubienie danych zawartych na nośnikach przenośnych;
  - 3) incydenty umyślne np. ataki hakerskie, włamania do pomieszczeń, celowe i świadome zniszczenie dokumentów, szkodliwe oprogramowanie.
4. W przypadku podejrzenia wystąpienia zagrożenia lub incydentu Inspektor w porozumieniu z kierownikiem komórki właściwej ds. IT prowadzi postępowanie wstępne, w toku którego:
  - 1) ustala zakres i przyczyny zagrożenia lub incydentu oraz jego ewentualne skutki;

- 2) inicjuje ewentualne postępowanie dyscyplinarne;
  - 3) rekomenduje działania prewencyjne zmierzające do eliminacji podobnych zagrożeń lub incydentów w przyszłości;
  - 4) dokumentuje prowadzone postępowanie;
  - 5) przedstawia raport z przeprowadzonego postępowania administratorowi.
5. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych, Inspektor informuje administratora o konieczności zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
6. Oceny, czy występuje ryzyko naruszenia praw lub wolności człowieka, administrator dokonuje we współpracy z Inspektorem. Ocena powinna być oparta na obiektywnych kryteriach, jak dotychczasowe doświadczenie związane z podobnymi naruszeniami lub wiedza z zakresu bezpieczeństwa informacji, oraz na uwzględnieniu okoliczności samego naruszenia ochrony danych osobowych.
7. W toku dokonywania oceny, o której mowa w pkt. 6 administrator bierze pod uwagę wszelkie możliwe szkody, jak i krzywdy, które mogą wyniknąć dla osób fizycznych z danego naruszenia. Mogą one w szczególności polegać na:
- 1) utracie kontroli nad własnymi danymi osobowymi,
  - 2) negatywnych konsekwencjach wizerunkowych,
  - 3) możliwości zawierania przez inną osobę umów z wykorzystaniem danych osobowych innej osoby fizycznej,
  - 4) stratach finansowych,
  - 5) negatywnym odbiorze społecznym, który może być konsekwencją upublicznienia niektórych danych osobowych.
8. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych Inspektor, niezależnie od pkt 5, niezwłocznie rozpoczyna audyt doraźny. W ramach czynności audytowych Inspektor:
- 1) określa sposób dokumentowania audytu, a w jego ramach:
    - a) sporządza notatki z czynności audytowych, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
    - b) odbiera pisemne wyjaśnienia osoby, której czynności objęto audytem;
    - c) sporządza kopie okazanych dokumentów;
    - d) sporządza kopię obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

- e) sporządza kopie zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
- 2) zabezpiecza ewentualne dowody związane z incydem;
  - 3) ustala osoby odpowiedzialne za powstanie incydem;
  - 4) wskazuje możliwe sposoby przywrócenia stanu zgodnego z prawem;
  - 5) wnioskuje o wszczęcie postępowań dyscyplinarnych;
  - 6) przygotowuje raport dla administratora.
9. Inspektor zawiadamia administratora o rozpoczęciu audytu doraźnego przed podjęciem pierwszej czynności w toku audytu.
10. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta powinna pozwolić organowi nadzorcemu na zweryfikowanie przestrzegania niniejszej Procedury.
11. Inspektor prowadzi rejestr incydentów, którego wzór stanowi załącznik nr 11 do niniejszej Polityki.

### **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu**

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. W sytuacji, gdy naruszenie dotyczy danych osobowych osób fizycznych, których Starostwo nie jest administratorem, a podmiotem przetwarzającym, któremu na podstawie art. 28 RODO zostały dane powierzone, to po stwierdzeniu naruszenia ochrony danych osobowych Starostwo, bez zbędnej zwłoki, zgłasza naruszenie podmiotowi, który dane Starostwu powierzył.
3. Zgłoszenie, o którym mowa w pkt. 1, zawiera co najmniej:
  - 1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - 2) imię i nazwisko oraz dane kontaktowe Inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - 3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
  - 4) opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

## **Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych**

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych.
2. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:
  - 1) imię i nazwisko oraz dane kontaktowe Inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - 2) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
  - 3) opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
3. Zawiadomienie nie jest wymagane, w następujących przypadkach:
  - 1) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
  - 2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
  - 3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku administrator wyda publiczny komunikat lub zastosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

## XX. Procedura zarządzania ryzykiem

Procedura zarządzania ryzykiem to szereg skoordynowanych działań podejmowanych przez Starostę, Wicestarostę, Sekretarza Powiatu, Skarbnika Powiatu, Naczelników poszczególnych wydziałów, kierowników oddziałów, pracowników zatrudnionych na samodzielnych stanowiskach, jak i pozostałych pracowników oraz współpracowników Starostwa, którzy poprzez identyfikację i analizę ryzyka oraz określanie adekwatnych reakcji na ryzyko zwiększają poziom bezpieczeństwa przetwarzania danych osobowych w ramach poszczególnych procesów ich przetwarzania.

1. W ramach powyższych działań dla zidentyfikowanych procesów przetwarzania danych osobowych (tabela nr 1) zostaną wskazane, przeanalizowane i oszacowane:
  - 1) **Zasoby** – które będziemy chronić:
    - a) sprzęt komputerowy przechowujący dane,
    - b) dane osobowe przetwarzane w formie papierowej i elektronicznej,
    - c) prawa i wolności osób fizycznych, których dane dotyczą,
    - d) aplikacje, w których przetwarzane są dane osobowe,
    - e) pomieszczenia, w których pracują osoby upoważnione do przetwarzania danych osobowych;
  - 2) **Zastosowane środki bezpieczeństwa** – zastosowane środki techniczne i organizacyjne, opisane w niniejszej Polityce;
  - 3) **Zagrożenia** – zdarzenia, które można wyróżnić ze względu na utratę poufności, dostępności, integralności i rozliczalności przetwarzanych danych osobowych, mogące powodować wystąpienie incydentu;
  - 4) **Podatności** – słabości zasobów, które mogą być wykorzystane przez potencjalne zagrożenia;
  - 5) **Skutki** – jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.
2. Mając na uwadze powyższe administrator zapewnia warunki pracy na systemach informatycznych zapewniające poufność, dostępność, integralność i rozliczalność przetwarzanych danych osobowych.
3. Administrator jest zobowiązany dostosować środki bezpieczeństwa zarówno techniczne, fizyczne, jak i organizacyjne do wyników przeprowadzonej analizy ryzyka.
4. Zmiany związane z pkt. 3 należy każdorazowo zaktualizować w Polityce ochrony danych osobowych.
5. Administrator wykazał zidentyfikowane zagrożenia, podatności oraz skutki związane z utratą poufności, dostępności, integralności i rozliczalność przetwarzanych danych osobowych **w tabeli nr 2** do niniejszej procedury. W powyższej klasyfikacji zostały uwzględnione zagrożenia wewnętrzne (np. działanie pracownika, awaria systemu spowodowana brakiem zasilania) i zewnętrzne (np. atak hakerski) mogące być następstwem działań (umyślnych lub nieumyślnych) człowieka lub wynikające z przyczyn naturalnych (środowiskowych).
6. Zidentyfikowane zagrożenia, podatności oraz skutki, o których mowa w pkt. 5, podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka. Na potrzeby niniejszej

procedury **poziomem istotności ryzyka (tabela nr 5, która obrazuje macierz ryzyka)** jest iloczyn oceny prawdopodobieństwa wystąpienia danego ryzyka (**tabela nr 3**) oraz oceny jego skutku (**tabela nr 4**).

7. Istotność konkretnego ryzyka określa czy jego poziom jest akceptowalny (**tabela nr 6**). Ustala się, że ryzykiem:
  - 1) akceptowalnym jest ryzyko na poziomie 3 i poniżej. Przy tym poziomie ryzyka podjęcie dodatkowych działań ograniczających wystąpienie zagrożenia może nastąpić w okresie dłuższym niż w ciągu roku, w zależności od możliwości i koniecznych nakładów finansowych.
  - 2) nieakceptowalnym jest ryzyko na poziomie od 4 – 16. Przy tym poziomie ryzyka konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych (wdrażane są adekwatne, skuteczne i efektywne działania zaradcze), z uwzględnieniem sposobów postępowania określonych w pkt 8 niniejszej procedury.
8. U administratora przyjmuje się następujące sposoby postępowania z ryzykiem:
  - 1) przeniesienie ryzyka – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta, przy czym należy pamiętać, że przeniesienie ryzyka nie eliminuje go,
  - 2) akceptacja ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu administratora, w szczególności gdy koszty podjętych ewentualnych działań mogą przekroczyć przewidywane korzyści,
  - 3) redukcja ryzyka – polega na obniżeniu poziomu ryzyka do poziomu akceptowalnego poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenia skutków jego wystąpienia np. poprzez zwiększenie mechanizmów kontroli (procedury, wytyczne, zasady, nadzór),
  - 4) unikanie ryzyka – polega na unikaniu przez administratora działań, które powodują powstanie określonych zagrożeń np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do przewidywanych korzyści.
9. Identyfikację i analizę ryzyka przeprowadza się na bieżąco, jako element systematycznego działania. **Identyfikację i analizę ryzyka przeprowadza się okresowo, co najmniej raz w roku, w sposób udokumentowany, odnosząc się do obecnych oraz nowo zidentyfikowanych procesów przetwarzania danych osobowych.**
10. Za każde zidentyfikowane ryzyko, w tym za sposób postępowania odnośnie tego ryzyka odpowiedzialna jest osoba mająca uprawnienia wystarczające do zapewnienia efektywnego zarządzania ryzykiem w ramach zidentyfikowanego procesu przetwarzania, tj. właściciel ryzyka.
11. Właściciel ryzyka w zakresie wykonywanych zadań ponosi odpowiedzialność za:
  - 1) przeprowadzanie i dokumentowanie identyfikacji i analizy ryzyka,
  - 2) podejmowane decyzje o zakresie i sposobie zarządzania ryzykiem,
  - 3) bezzwłoczne zgłoszenie bezpośredniemu przełożonemu ryzyka, które nie jest akceptowane i które wymaga zastosowania dodatkowych mechanizmów kontrolnych oraz wskazania konkretnych działań zaradczych ograniczających wystąpienie ryzyka i jego skutków.
12. Inspektor w ramach niniejszej procedury odpowiada za:

- 1) nadzór nad przestrzeganiem procedury, a w szczególności nad dokumentowaniem identyfikacji i analizy ryzyka,
  - 2) rozstrzygnięcie kwestii spornych w zakresie stosowanej metodyki zarządzania ryzykiem.
13. Podstawową dokumentację identyfikacji i analizy ryzyka stanowi arkusz ryzyk zagrażających bezpieczeństwu przetwarzania danych osobowych u administratora zwany dalej „**arkuszem ryzyk**” (**tabela nr 7**).
  14. Formularz arkusza ryzyk przekazywany jest przez Inspektora do właścicieli ryzyk w postaci elektronicznej w terminach uzgodnionych z Sekretarzem Powiatu.
  15. Wypełniony przez właściciela ryzyk arkusz ryzyk przekazywany jest Inspektorowi w postaci papierowej zawierającej datę sporządzenia i podpis właściciela ryzyka.
  16. Inspektor konsoliduje wyniki analizy ryzyk i przedstawia je Staroście wraz z propozycją postępowania z ryzykiem.
  17. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka (**patrz tabela nr 6**), zgodnie z art. 35 RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane. Przy czym podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.
  18. Niniejsza procedura podlega raz na rok przeglądowi i w przypadku konieczności aktualizacji. Przeglądu i aktualizacji procedury dokonuje Inspektor przy współpracy z kierownikiem komórki właściwej ds. IT.

**Tabela nr 1 do Procedury zarządzania ryzykiem**

<b>PROCESY</b>	<b>CZYNNOŚCI</b>
Proces rekrutacji pracowników i współpracowników	Czynności związane z przeprowadzeniem rekrutacji wraz z wyłonieniem kandydata
	Czynności związane z dopuszczeniem kandydata do pracy lub nawiązaniem współpracy
	Czynności związane z archiwizacją dokumentacji
Proces obsługi pracowników i współpracowników, w tym byłych pracowników i współpracowników	Czynności związane z nawiązaniem zatrudnienia lub podpisaniem umowy o współpracę
	Czynności związane z bieżącą obsługą pracowników
	Czynności związane z bieżącą obsługą współpracowników
	Czynności związane z bieżącą obsługą byłych pracowników
	Czynności związane z bieżącą obsługą byłych współpracowników
	Czynności związane z realizacją świadczeń socjalnych
	Czynności związane z archiwizacją dokumentacji
Proces realizacji dostawy usług świadczonych na rzecz administratora	Czynności związane z szacowaniem wartości zamówienia
	Czynności związane z zawarciem umowy
	Czynności związane z realizacją umowy
	Czynności związane z dochodzeniem roszczeń
	Czynności związane z archiwizacją dokumentacji
Proces obsługi korespondencji i osób kontaktujących się z administratorem	Czynność rejestracji korespondencji przychodzącej i wychodzącej
	Czynności związane z obiegiem dokumentów
	Czynności związane z telefoniczną obsługą osób kontaktujących się
	Czynności związane z archiwizacją dokumentacji
Proces obsługi finansowej i księgowej	Czynności związane z realizacją zobowiązań finansowych
	Czynności związane z windykacją należności
	Czynności związane z archiwizacją dokumentacji
Proces obsługi klienta	Czynności związane z przeprowadzeniem rekrutacji wraz z wyłonieniem kierownika jednostki organizacyjnej powiatu
	Czynności związane z bieżącą obsługą kierowników jednostki organizacyjnej powiatu
	Czynności związane z przeprowadzaniem kontroli w jednostkach organizacyjnych powiatu
	Czynności związane z ze zbieraniem i publikowaniem oświadczeń majątkowych
	Czynności związane z rejestracją pojazdów
	Czynności związane z wydawaniem prawa jazdy
	Czynności związane z wydaniem decyzji dotyczącej wpisu do rejestru przedsiębiorców prowadzących stacje kontroli pojazdów
	Czynności związane z wydaniem lub cofnięciem uprawnień do wykonywania badań technicznych pojazdów
	Czynności związane z wydawaniem legitymacji instruktorom nauki jazdy i przedłużeniem ważności legitymacji oraz wydawaniem zaświadczeń wykładowcom
Czynności związane z prowadzeniem rejestru działalności regulowanej przedsiębiorców	

prowadzących ośrodki szkolenia kierowców
Czynności związane z wydawaniem zezwoleń na wykonywanie zawodu przewoźnika drogowego, krajowego transportu drogowego, przewozów specjalnych
Czynności związane z zarządzaniem ruchem na drogach gminnych i powiatowych
Czynności związane z wydaniem pozwolenia wodnoprawnego
Czynności związane z obsługą posiadaczy żywych zwierząt
Czynności związane z wydaniem koncesji w zakresie kopalin
Czynności związane z wydaniem pozwolenie na wprowadzenie gazów lub pyłów do powietrza
Czynności związane z wydaniem karty wędkarskiej lub karty łowiectwa podwodnego
Czynności związane z rejestracją sprzętu wodnego służącego do amatorskiego połowy ryb
Czynności związane z wydaniem zezwolenia na prowadzenie działalności w zakresie odzysku lub unieszkodliwiania odpadów
Czynności związane z wydaniem zezwolenia na prowadzenie działalności w zakresie zbierania lub transportu odpadów
Czynności związane z obsługą wniosków o wycinkę drzew w lesie
Czynności związane z obsługą wniosków o zmianę przeznaczenia gruntów leśnych
Czynności związane z obsługą wniosków właścicieli lub innych osób władających gruntami leśnymi
Czynności związane z obsługą wniosków właścicieli lub innych osób władających gruntami, budynkami lub lokalami
Czynności związane z wydaniem pozwolenia na budowę
Czynności związane z obsługą osób zgłaszających budowę obiektu budowlanego lub wykonanie robót budowlanych
Czynności związane z przeprowadzaniem prac geodezyjnych i kartograficznych
Czynności związane z obsługą użytkowników wieczystych i dzierżawców
Czynności związane z wprowadzaniem danych nauczycieli do Systemu Informacji Oświatowej
Czynności związane z wprowadzaniem danych uczniów do Systemu Informacji Oświatowej
Czynności związane z przeprowadzeniem rekrutacji wraz z wyłonieniem dyrektora szkoły lub poradni
Czynności związane z bieżącą obsługą dyrektorów szkół lub poradni Czynności związane z kierowaniem nieletnich do MOW
Czynności związane z kierowaniem dzieci i młodzieży do szkół specjalnych lub MOS
Czynności związane z obsługą uczniowskich klubów sportowych
Czynności związane z prowadzeniem rejestru szkół niepublicznych o uprawnieniach publicznych
Czynności związane z przyznawaniem nagród Starosty
Czynności związane z prowadzeniem Stałego Dyżuru
Czynności związane z prowadzeniem Akcji Kurierskiej
Czynności związane z obsługą Powiatowego Zespołu ds. Zarządzania Kryzysowego

Czynności związane z procesem ewakuacji ludności
Czynności związane z kwalifikacją do zdolności do służby wojskowej
Czynności związane z formacją obrony cywilnej
Czynności związane z obsługą Stanowiska Kierowania
Czynności związane z prowadzeniem rejestru stowarzyszeń i fundacji
Czynności związane z postępowaniem w sprawie sprowadzenia zwłok ludzkich z zagranicy
Czynności związane z obsługą członków Komisji Bezpieczeństwa i Porządku
Czynności związane z obsługą kombatantów i osób represjonowanych
Czynności związane z postępowaniem z rzeczami znalezionymi lub zagubionymi
Czynności związane z obsługą repatriantów
Czynności związane udzielaniem nieodpłatnej pomocy prawne
Czynności związane z realizacją projektów
Czynności związane z prowadzeniem postępowania przez Powiatowego Rzecznika Konsumentów
Czynności związane z prowadzeniem postępowania sprawdzającego
Czynności związane z archiwizacją dokumentacji

Tabela nr 2 do Procedury zarządzania ryzykiem

	Zagrożenie	Podatności (słabości)	Skutki
POUFNOŚĆ, DOSTĘPNOŚĆ, INTEGRALNOŚĆ LUB ROZLICZALNOŚĆ	nieuprawniony dostęp do danych osobowych	<ul style="list-style-type: none"> <li>• awaria sprzętu,</li> <li>• atak wirusa,</li> <li>• odcięcie zasilania,</li> <li>• pożar,</li> <li>• zalanie,</li> <li>• kradzież nośników danych,</li> <li>• nieprzestrzeganie wewnętrznych regulacji,</li> </ul>	<ul style="list-style-type: none"> <li>• Wyciek, utrata, zniszczenie lub uszkodzenie danych osobowych,</li> <li>• straty wizerunkowe,</li> <li>• straty finansowe,</li> <li>• odpowiedzialność dyscyplinarna, karna lub kontraktowa,</li> <li>• naruszenie praw i wolności osób, których dane dotyczą,</li> <li>• przetwarzanie danych osobowych niezgodnie z prawem,</li> <li>• przetwarzanie nieaktualnych danych osobowych,</li> <li>• naruszenie zasady minimalizacji danych;</li> </ul>
	niepożądana modyfikacja danych osobowych	<ul style="list-style-type: none"> <li>• przekroczenie uprawnień,</li> <li>• brak umowy powierzenia,</li> <li>• brak okresowych szkoleń z zakresu ochrony danych osobowych,</li> <li>• brak zabezpieczeń fizycznych,</li> <li>• instalowanie nielegalnego oprogramowania,</li> <li>• niefrasobliwość pracowników lub współpracowników</li> </ul>	
	udostępnianie informacji osobom nieuprawnionym	<ul style="list-style-type: none"> <li>• brak wyciągania konsekwencji za przekroczenie uprawnień,</li> <li>• niestosowanie się do przyjętych regulacji,</li> <li>• niewystarczający poziom świadomości pracowników lub współpracowników,</li> </ul>	
	utrata danych	<ul style="list-style-type: none"> <li>• nieprzestrzeganie zasad czystego biurka i pulpitu,</li> <li>• wynoszenie nośników danych poza siedzibę administratora,</li> <li>• pozostawienie osób trzecich bez nadzoru,</li> </ul>	
	przetwarzanie danych osobowych nieadekwatnych do realizacji celu	<ul style="list-style-type: none"> <li>• brak legalnego oprogramowania,</li> <li>• brak odpowiedniego nadzoru nad oprogramowaniem,</li> <li>• brak świadomości najwyższego kierownictwa,</li> <li>• niewystarczające nakłady finansowe,</li> <li>• nienależyte niszczenie dokumentacji,</li> </ul>	
	przetwarzanie danych osobowych po upływie okresu niezbędnego do realizacji celu	<ul style="list-style-type: none"> <li>• używanie sprzętu i oprogramowania do celów prywatnych,</li> <li>• niewystarczający nadzór nad dokumentacją archiwalną,</li> <li>• brak reakcji na sprostowanie danych osobowych,</li> <li>• uniemożliwienie dostępu do danych osobowych osobom, których dane dotyczą,</li> </ul>	

Tabela nr 3 do Procedury zarządzania ryzykiem

SKALA OCEN PRAWDOPODOBIENSTWA		OPIS (pomocniczo)
NISKIE	1	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie nie wystąpiło.
ŚREDNIE	2	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie wystąpiło raz.
WYSOKIE	3	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie wystąpiło 2 lub 3 razy.
BARDZO WYSOKIE	4	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie wystąpiło częściej niż 3 razy.

Tabela nr 4 do Procedury zarządzania ryzykiem

SKALA OCEN SKUTKU		OPIS
NISKI	1	<p>Zagrożenie objęte ryzykiem <b>ma niewielki wpływ</b> na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:</p> <ul style="list-style-type: none"> <li>• w dłuższym czasie może spowodować niewielkie straty materialne,</li> <li>• nie powoduje strat lub powoduje minimalne straty lub koszty finansowe,</li> <li>• nie wpływa na prawa i wolności osób fizycznych, których dane dotyczą,</li> <li>• nie wpływa na wizerunek administratora.</li> </ul>
ŚREDNI	2	<p>Zagrożenie objęte ryzykiem <b>ma umiarkowany wpływ</b> na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:</p> <ul style="list-style-type: none"> <li>• może spowodować w okresie roku niewielkie straty materialne lub koszty finansowe,</li> <li>• stanowi naruszenie wewnętrznych regulacji,</li> <li>• ma znikomy wpływ na prawa i wolności osób fizycznych, których dane dotyczą,</li> <li>• ma niewielki wpływ na wizerunek administratora.</li> </ul>
WYSOKI	3	<p>Zagrożenie objęte ryzykiem <b>ma duży wpływ</b> na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:</p> <ul style="list-style-type: none"> <li>• może spowodować w krótkim okresie czasu znaczące straty materialne lub koszty finansowe,</li> <li>• stanowi naruszenie wewnętrznych regulacji,</li> <li>• może stanowić naruszenie przepisów prawa, a brak reakcji może rodzić odpowiedzialność administracyjną lub cywilną,</li> <li>• ma wysoki wpływ na prawa i wolności osób fizycznych, których dane dotyczą,</li> <li>• może powodować zakłócenia w funkcjonowaniu administratora,</li> <li>• ma duży wpływ na wizerunek administratora.</li> </ul>
BARDZO WYSOKI	4	<p>Zagrożenie objęte ryzykiem <b>ma bardzo duży wpływ</b> na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:</p> <ul style="list-style-type: none"> <li>• powoduje znaczące straty materialne lub koszty finansowe,</li> <li>• stanowi naruszenie przepisów prawa, a brak reakcji rodzi odpowiedzialność administracyjną, karną lub cywilną, ma bardzo wysoki wpływ na prawa i wolności osób fizycznych, których dane dotyczą,</li> <li>• destabilizuje pracę administratora,</li> <li>• wywołuje zdecydowanie negatywną reakcję publiczną w mediach w całym kraju.</li> </ul>

Tabela nr 5 do Procedury zarządzania ryzykiem

			SKUTEK			
			NISKI	ŚREDNI	WYSOKI	BARDZO WYSOKI
			1	2	3	4
PRAWDOPODOBIEŃSTWO	NISKIE	1				
	ŚREDNIE	2				
	WYSOKIE	3				
	BARDZO WYSOKIE	4				

**Tabela nr 6 do Procedury zarządzania ryzykiem**

<b>POZIOM RYZYKA</b>	<b>Opis działania</b>
<b>NISKI (N)</b>	Poziom ryzyka akceptowalny – działania mogą zostać przesunięte w czasie i nie wymaga monitorowania
<b>ŚREDNI (Ś)</b>	Poziom ryzyka nieakceptowalny – działania mogą zostać przesunięte w czasie, wymaga okresowego monitorowania
<b>WYSOKI (W)</b>	Poziom ryzyka nieakceptowalny – działania mogą zostać przesunięte w czasie, ale wymaga stałego monitorowania
<b>KRYTYCZNY (K)</b>	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania



## XXI. Procedura oceny skutków

Celem niniejszej procedury jest zapewnienie realizacji obowiązków wynikających z art. 35 RODO, tj. ustalenie zasad wykonywania oceny skutków dla ochrony danych osobowych.

1. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka (**patrz tabela nr 6 do Procedury zarządzania ryzykiem**), zgodnie z art. 35 RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.
2. Przeprowadzając ocenę skutków dla ochrony danych bierze się pod uwagę nie interesy administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.
3. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem tego przetwarzania dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
4. Dokonując oceny skutków dla ochrony danych, administrator konsultuje z Inspektorem m. in. kwestie dotyczące:
  - 1) konieczności przeprowadzenia oceny skutków dla ochrony danych;
  - 2) metodologii przeprowadzenia oceny skutków dla ochrony danych;
  - 3) decyzji, czy przeprowadzić wewnętrzną ocenę, czy też zlecić ją podmiotowi zewnętrznemu;
  - 4) zabezpieczeń, w tym środków technicznych i organizacyjnych, stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
  - 5) prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO, w szczególności czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować.
5. W sytuacji, gdy administrator nie zgadza się z zaleceniami Inspektora, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń.
6. **Ocenę skutków, której formularz stanowi załącznik nr 15 do niniejszej Polityki** – z wyłączeniem oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą – dokonuje się także w razie:
  - 1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
  - 2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa; lub
  - 3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
7. Ocena skutków zawiera co najmniej:

- 1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
  - 2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
  - 3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą; oraz
  - 4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
8. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Inspektor dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
9. Administrator ustala następujący sposób oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą:
- 1) Administrator wykazał zidentyfikowane możliwe skutki związane z naruszeniem praw lub wolności osób, których dane dotyczą **w tabeli nr 1 do niniejszej procedury.**
  - 2) Zidentyfikowane skutki podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka naruszenia praw w wolności osób, których dane dotyczą. Na potrzeby niniejszej procedury poziomem istotności ryzyka jest **iloczyn** (tabela nr 4, która obrazuje macierz ryzyka) **oceny prawdopodobieństwa wystąpienia danego ryzyka (tabela nr 2) oraz oceny jego skutku (tabela nr 3).**
  - 3) Istotność konkretnego ryzyka określa czy jego poziom jest akceptowalny (**tabela nr 5**). Ustala się, że ryzykiem:
    - a) **akceptowalnym jest ryzyko na poziomie 3 i poniżej. Przy tym poziomie ryzyka podjęcie dodatkowych działań ograniczających wystąpienie zagrożenia może nastąpić w okresie dłuższym niż w ciągu roku, w zależności od możliwości i koniecznych nakładów finansowych.**
    - b) **nieakceptowalnym jest ryzyko na poziomie od 4 – 16. Przy tym poziomie ryzyka konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych.**
  - 4) U administratora przyjmuje się następujące sposoby postępowania z ryzykiem związanym z naruszeniem praw i wolności osób, których dane dotyczą:
    - a) przeniesienie ryzyka – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta, przy czym należy pamiętać, że przeniesienie ryzyka nie eliminuje go,
    - b) akceptacja ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu administratora, w szczególności gdy koszty podjętych ewentualnych działań mogą przekroczyć przewidywane korzyści,
    - c) redukcja ryzyka – polega na obniżeniu poziomu ryzyka do poziomu akceptowalnego poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenia skutków jego wystąpienia np. poprzez zwiększenie mechanizmów kontroli (procedury, wytyczne, zasady, nadzór),
    - d) unikanie ryzyka – polega na unikaniu przez administratora działań, które powodują powstanie określonych zagrożeń np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatnych do przewidywanych korzyści.

- 5) Podstawową dokumentację identyfikacji i analizy ryzyka stanowi arkusz ryzyk zagrażających prawom i wolnościom osób, których dane dotyczą, zwany dalej „arkuszem ryzyk praw i wolności” (tabela nr 6).
10. Jeżeli wykonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.
11. Konsultując się z organem nadzorczym administrator przedstawia mu:
  - 1) gdy ma to zastosowanie – odpowiednie obowiązki administratora;
  - 2) cele i sposoby zamierzonego przetwarzania;
  - 3) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z RODO;
  - 4) dane kontaktowe inspektora ochrony danych;
  - 5) ocenę skutków dla ochrony danych, oraz
  - 6) wszelkie inne informacje, których żąda organ nadzorczy.
12. Niniejsza procedura podlega raz na rok przeglądowi i w przypadku konieczności aktualizacji.
13. Przeglądu i aktualizacji procedury dokonuje Inspektor.

**Tabela nr 1 do Procedury oceny skutków**

<b>Możliwe skutki związane z naruszenia praw lub wolności osób, których dane dotyczą</b>	
dyskryminacja	kradzież tożsamości
oszustwa dotyczące tożsamości	strata finansowa
naruszenie poufności danych osobowych chronionych tajemnicą zawodową	
nieuprawnione odwrócenie pseudonimizacji	szkoda gospodarcza
pozbawienie praw i wolności	szkoda społeczna
pozbawienie możliwości sprawowania kontroli nad swoimi danymi osobowymi	
naruszenie dobrego imienia	uszczerbek fizyczny

**Tabela nr 2 do Procedury oceny skutków**

<b>SKALA OCEN PRAWDOPODOBIENSTWA</b>		<b>OPIS (pomocniczo)</b>
<b>NISKIE</b>	<b>1</b>	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie nie wystąpiło.
<b>ŚREDNIE</b>	<b>2</b>	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie wystąpiło raz.
<b>WYSOKIE</b>	<b>3</b>	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie wystąpiło 2 lub 3 razy.
<b>BARDZO WYSOKIE</b>	<b>4</b>	Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale w ostatnim okresie wystąpiło częściej niż 3 razy.

Tabela nr 3 do Procedury oceny skutków

SKALA OCEN SKUTKU		OPIS
<b>NISKI</b>	<b>1</b>	Zagrozenie objete ryzykiem ma niewielki wplyw na prawa i wolnosci osob, ktorych dotycza.
<b>ŚREDNI</b>	<b>2</b>	Zagrozenie objete ryzykiem ma umiarkowany wplyw na prawa i wolnosci osob, ktorych dotycza.
<b>WYSOKI</b>	<b>3</b>	Zagrozenie objete ryzykiem ma duzy wplyw na prawa i wolnosci osob, ktorych dotycza.
<b>BARDZO WYSOKI</b>	<b>4</b>	Zagrozenie objete ryzykiem ma bardzo duzy wplyw na prawa i wolnosci osob, ktorych dotycza.

Tabela nr 4 do Procedury oceny skutków

			SKUTEK			
			NISKI	ŚREDNI	WYSOKI	BARDZO WYSOKI
			1	2	3	4
PRAWDOPODOBIEŃSTWO	NISKIE	1				
	ŚREDNIE	2				
	WYSOKIE	3				
	BARDZO WYSOKIE	4				

Tabela nr 5 do Procedury oceny skutków

POZIOM RYZYKA	Opis działania
NISKI (N)	Poziom ryzyka akceptowalny – działania mogą zostać przesunięte w czasie i nie wymaga monitorowania
ŚREDNI (Ś)	Poziom ryzyka nieakceptowalny – działania mogą zostać przesunięte w czasie, wymaga okresowego monitorowania
WYSOKI (W)	Poziom ryzyka nieakceptowalny – działania mogą zostać przesunięte w czasie, ale wymaga stałego monitorowania
KRYTYCZNY (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania



## XXII. Procedura prowadzenia wykazu i rejestrów

Celem niniejszej procedury jest ustalenie zasad prowadzenia przez Inspektora wykazu podmiotów przetwarzających dane w imieniu administratora, rejestru czynności przetwarzania danych osobowych oraz ewentualnego rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, które są prowadzone w celu realizacji przez administratora zasady rozliczalności.

### 1. Inspektor prowadzi:

- 1) wykaz podmiotów przetwarzających dane, którego wzór stanowi **załącznik nr 12** do niniejszej Polityki;
  - 2) rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 ust. 1 RODO, którego wzór stanowi **załącznik nr 13** do niniejszej Polityki;
  - 3) rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zgodnie z art. 30 ust. 2 RODO, którego wzór stanowi **załącznik nr 14** do niniejszej Polityki.
2. Wykaz i rejestry mają formę pisemną, w tym formę elektroniczną.
  3. Inspektor tworzy i prowadzi wykaz oraz rejestry w oparciu o dane otrzymane od naczelników wydziałów, kierownika referatu lub osób zajmujących samodzielne stanowiska pracy.
  4. Naczelnicy wydziałów lub osoby zajmujące samodzielne stanowiska pracy są zobowiązani do bieżącego przekazywania danych potrzebnych do prowadzenia wykazu i rejestru, w szczególności są zobowiązani do niezwłocznego informowania Inspektora o każdej zmianie mającej wpływ na treść wykazu i rejestrów.
  5. Administrator, w ramach współpracy z organem nadzorczym, udostępnia rejestr na żądanie tego organu nadzorczego w celu monitorowania przez organ operacji przetwarzania.

## XXIII . Procedura przeprowadzania audytów zgodności

Celem niniejszej procedury jest określenie trybu i zasad monitorowania przez Inspektora przestrzegania RODO i innych przepisów o ochronie danych osobowych, a także polityk administratora w dziedzinie ochrony danych osobowych, w tym niniejszej Polityki ochrony danych osobowych poprzez przeprowadzanie audytów zgodności przetwarzania danych osobowych.

1. Audyt zgodności jest przeprowadzany w trybie:
  - 1) audytu planowanego – przeprowadzanego przynajmniej raz w roku przez Inspektora ochrony danych osobowych lub firmę zewnętrzną posiadającą uprawnienia do badania zgodności przetwarzania danych osobowych przez Administratora z przepisami RODO ;
  - 2) audytu doraźnego – w sytuacji powzięcia przez Inspektora wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia. Audyt doraźny przeprowadza się na zasadach opisanych w rozdziale: „Procedura zgłaszania incydentów”.
2. Przynajmniej na 14 dni przed rozpoczęciem audytu planowanego Inspektor informuje administratora o przedmiocie, zakresie oraz terminie przeprowadzenia audytu.
3. Planując przeprowadzenie audytu Inspektor uwzględnia w szczególności: procesy przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych z:
  - 1) zasadami, o których mowa w art. 5, art. 12-23 i art. 28 RODO i w niniejszej Polityce;
  - 2) zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 32 RODO i w niniejszej Polityce;
  - 3) zasadami przekazywania danych osobowych, o których mowa w art. 44-49 RODO;
  - 4) obowiązkami wynikającymi z art. 33-36 RODO;
  - 5) zweryfikowanym stanem faktycznym w zakresie przetwarzania danych osobowych;
  - 6) zasadami i obowiązkami określonymi w niniejszej Polityce.
4. Inspektor lub audytor zewnętrzny dokumentuje czynności przeprowadzone w toku audytu, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych oraz do opracowania raportu.
5. Dokumentowanie czynności w toku audytu może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania danych osobowych lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonania wydruku tych danych oraz na:
  - 1) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
  - 2) odebraniu wyjaśnień osoby, której czynności objęto audytem;
  - 3) sporządzeniu kopii otrzymanego dokumentu;

- 4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania danych osobowych;
  - 5) sporządzaniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych.
6. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności Inspektora lub audytora zewnętrznego mogą być wykonywane przy udziale osób zarządzających tym systemem.
  7. Osoba, której dotyczy audyt, bierze udział w audycie lub umożliwia Inspektorowi przeprowadzenie czynności w toku audytu.
  8. Po zakończeniu audytu Inspektor lub audytor zewnętrzny przygotowuje raport zgodności sporządzony w postaci elektronicznej lub postaci papierowej.
  9. Inspektor lub audytor zewnętrzny przekazuje administratorowi raport zgodności:
    - 1) z audytu planowanego – nie później niż w terminie 30 dni od zakończenia audytu;
    - 2) z audytu doraźnego – niezwłocznie, nie później niż w terminie 7 dni od zakończenia audytu.
  10. Inspektor lub audytor zewnętrzny jest uprawniony, w każdym czasie, do przeprowadzania weryfikacji przestrzegania niniejszej Polityki, bez konieczności przeprowadzania audytu zgodności.
  11. Inspektor jest uprawniony do ustnego pouczenia osoby nieprzestrzegającej zasad określonych w niniejszej Polityce lub pisemnego zawiadomienia administratora o nieprzestrzeganiu zasad przez wskazaną osobę.

## **XXIV. Postanowienia końcowe**

1. Polityka ochrony danych osobowych jest dokumentem wewnętrznym i osoby, które uzyskały wgląd w jej treść, zobowiązane są do zachowania jej w poufności.
2. Przypadki nieuzasadnionego zaniechania obowiązków określonych w niniejszym dokumencie, traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
3. W sprawach nieuregulowanych w niniejszej Polityce ochrony danych osobowych mają zastosowanie przepisy 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 oraz inne przepisy z zakresu ochrony danych osobowych.

**STAROSTA**  
  
**Mariusz Turalski**

## Załącznik nr 1

WYKAZ KATEGORII OSÓB, KTÓRYCH DANE DOTYCZĄ ORAZ KATEGORII DANYCH OSOBOWYCH					
Lp.	Kategoria osób których dane dotyczą	Kategorie danych osobowych		Zastosowany program	Wersja papierowa
		Dane zwykłe	Dane szczególne		
1	Potencjalni pracownicy i współpracownicy	imię i nazwisko, wizerunek, data i miejsce urodzenia, adres zamieszkania, adres do korespondencji, nr telefonu, adres poczty elektronicznej, przebieg kariery, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa	Poczta elektroniczna	TAK
2	Pracownicy i współpracownicy, w tym byli pracownicy i współpracownicy oraz członkowie ich rodzin	imię i nazwisko, wizerunek, nazwa miejsca pracy, funkcja lub stanowisko, seria i nr dowodu tożsamości, data i miejsce urodzenia, miejsce zameldowania, adres zamieszkania, nr NIP, nr PESEL, nazwisko rodowe, obywatelstwo, prywatny nr telefonu, prywatny adres poczty elektronicznej, służbowy nr telefonu, służbowy adres poczty elektronicznej, imiona rodziców, stan rodzinny, imię i nazwisko oraz data urodzenia współmałżonka, data urodzenia dziecka lub dzieci pracownika, imię i nazwisko, adres oraz nr telefonu osoby, którą należy poinformować w razie wypadku pracownika, stosunek do powszechnego obowiązku obrony, przebieg kariery, czas pracy, wysokość wynagrodzenia, nagrody, premie, kwoty udzielonych pożyczek, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, informacje o oddziale Narodowego Funduszu Zdrowia, informacje o Urzędzie Skarbowym, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa	Poczta elektroniczna, Kadry i Płace Płatnik, BIP	TAK

		szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania, numery rachunku bankowego, nazwa banku, w którym prowadzony jest rachunek bankowy, firma, adres siedziby firmy, godzina i data użycia karty dostępu, imię i nazwisko osoby zgłoszonej do ubezpieczenia zdrowotnego			
3	<b>Potencjalni dostawcy oraz ich pracownicy i współpracownicy</b>	imię, nazwisko, nazwa firmy, adres e-mail, strona www, nr telefonu, dane z CEIDG, forma rozliczania, nr REGON, nr NIP, nr PESEL, seria i numer dowodu tożsamości		Poczta elektroniczna	TAK
4	<b>Dostawcy oraz ich pracownicy i współpracownicy</b>	imię, nazwisko, nazwa firmy, adres siedziby, adres dostawy, termin odstawy, adres e-mail, strona www, nr telefonu, dane z CEIDG, forma rozliczania, nr REGON, nr NIP, nr PESEL, seria i numer dowodu tożsamości, historia dostaw		Poczta elektroniczna Kasa	TAK
5	<b>Osoby składające skargi, wnioski i petycje</b>	imię, nazwisko, numer telefonu, adres poczty elektronicznej, adres do korespondencji, adres zamieszkania, treść podania, nr PESEL		Poczta elektroniczna ePUAP	TAK
6	<b>Osoby wnioskujące o udostępnienie informacji publicznej</b>	imię, nazwisko, numer telefonu, adres poczty elektronicznej, adres do korespondencji, adres zamieszkania, treść podania, nr PESEL		Poczta elektroniczna ePUAP	TAK
7	<b>Osoby znajdujące się w rejestrze korespondencji</b>	imię, nazwisko, nazwa firmy lub instytucji, adres zamieszkania, adres siedziby, informacja czego dotyczy pismo		Poczta elektroniczna ePUAP	TAK
8	<b>Osoby kontaktowe</b>	imię, nazwisko, adres poczty elektronicznej, nr telefonu, miejsce pracy		Poczta elektroniczna ePUAP	TAK
9	<b>Wierzyciele i dłużnicy</b>	imię, nazwisko, nr NIP, nr PESEL, nr rachunku bankowego, nazwa banku w którym prowadzony jest rachunek bankowy, nr REGON, nr telefonu, kwota, tytuł płatności, wysokość zadłużenia, informacje o egzekucji		Poczta elektroniczna, Kadry i Płace Kasa, Płatnik, system bankowy	TAK
10	<b>Potencjalni kierownicy jednostek organizacyjnych powiatu</b>	imię i nazwisko, wizerunek, data i miejsce urodzenia, adres zamieszkania, adres do korespondencji, nr telefonu, adres poczty elektronicznej, przebieg kariery, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, poziom		Poczta elektroniczna	TAK

		wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania			
11	<b>Kierownicy jednostek organizacyjnych powiatu</b>	imię i nazwisko, wizerunek, nazwa miejsca pracy, funkcja lub stanowisko, seria i nr dowodu tożsamości, data i miejsce urodzenia, miejsce zameldowania, adres zamieszkania, nr NIP, nr PESEL, nazwisko rodowe, obywatelstwo, prywatny nr telefonu, prywatny adres poczty elektronicznej, służbowy nr telefonu, służbowy adres poczty elektronicznej, imiona rodziców, stan rodzinny, imię i nazwisko oraz data urodzenia współmałżonka, data urodzenia dziecka lub dzieci pracownika, imię i nazwisko, adres oraz nr telefonu osoby, którą należy poinformować w razie wypadku pracownika, stosunek do powszechnego obowiązku obrony, przebieg kariery, czas pracy, wysokość wynagrodzenia, nagrody, premie, kwoty udzielonych pożyczek, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, informacje o oddziale Narodowego Funduszu Zdrowia, informacje o Urzędzie Skarbowym, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania, numery rachunku bankowego, nazwa banku, w którym prowadzony jest rachunek bankowy, firma, adres siedziby firmy, godzina i data użycia karty dostępu, imię i nazwisko osoby zgłoszonej do ubezpieczenia zdrowotnego	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa	Poczta elektroniczna, ePUAP	TAK
12	<b>Przedstawiciele kontrolowanych jednostek organizacyjnych</b>	imię, nazwisko, data i miejsce urodzenia, adres zamieszkania lub pobytu, nr PESEL, seria i numer dokumentu potwierdzającego		Poczta elektroniczna, ePUAP,	TAK

	<b>powiatu</b>	tożsamość, numer telefonu, adres poczty elektronicznej, miejsce pracy, adres do korespondencji, przebieg kariery, informacje o statusie bezrobotnego, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia			
13	<b>Osoby składające oświadczenia majątkowe</b>	imię, nazwisko, adres zamieszkania, miejsce zatrudnienia, stanowisko lub funkcja, zasoby pieniężne, posiadane nieruchomości, ich wartość i miejsce położenia, posiadane udziały w spółkach, posiadane akcje w spółkach, mienie nabyte od Skarbu Państwa, informacje dot. prowadzonej działalności gospodarczej, wysokość dochodu z tytułu prowadzenia działalności gospodarczej, informacje o pełnieniu funkcji w spółkach, wysokość dochodu z tytułu pełnionej funkcji w spółce, wysokość dochodów z tytułu stosunku pracy i diety, informacja o składnikach mienia ruchomego o wartości powyżej 10 000 zł, informacja o zobowiązaniach pieniężnych o wartości większej niż 10 000 zł		Poczta elektroniczna, BIP	TAK
14	<b>Właściciele pojazdów</b>	imię, nazwisko właściciela pojazdu, adres zamieszkania, nr PESEL, adres poczty elektronicznej, nr telefonu, informacje o pojeździe (marka, typ, model, numer podwozia/nadwozia, ramy, VIN, parametry techniczne, wydane oznaczenia i ich wtórniki), numer oraz data ważności polisy OC, termin następnego badania technicznego, informacja o zastawach celnych, skarbowych sądowych, zgłoszenia sprzedaży, wycofanie z ruchu, wyrejestrowanie pojazdu		Poczta elektroniczna, CEPiK	TAK
15	<b>Kierowcy</b>	imię, nazwisko, adres zamieszkania, seria i numer dowodu tożsamości, nr PESEL, data i miejsce urodzenia, numer telefonu, adres poczty elektronicznej, kategoria prawa jazdy, wizerunek, nr karty kierowcy, okres ważności prawa jazdy, data uzyskania prawa jazdy, ograniczenia		Poczta elektroniczna, CEPiK	TAK
16	<b>Stacje kontroli pojazdów</b>	imię, nazwisko, nr NIP, nr REGON, funkcja, firma prowadzącego działalność gospodarczą, adres		Poczta elektroniczna, CEPiK,	TAK

		zamieszkania albo siedziba przedsiębiorcy, nr w rejestrze przedsiębiorców albo w ewidencji działalności gospodarczej, informacja o złożeniu wniosku o wpis do rejestru przedsiębiorców prowadzących stacje kontroli pojazdów, adres stacji kontroli pojazdów przedsiębiorcy		rejestry papierowe	
17	<b>Diagności</b>	imię, nazwisko, nr dowodu tożsamości, nr PESEL, wykształcenie, wizerunek, numer uprawnień, informacja o złożeniu wniosku o wpis, informacja o ukończonych kursach, informacja o praktyce zawodowej, informacja o zdaniu egzaminu kwalifikacyjnego Transportowego Dozoru Technicznego		Poczta elektroniczna, CEPIK, rejestry papierowe	TAK
18	<b>Instruktorzy nauki jazdy</b>	imię, nazwisko, nr PESEL, adres poczty elektronicznej, nr telefonu, numer dokumentu tożsamości, wizerunek, wykształcenie, adres zamieszkania, informacja o uzyskanym uprawnieniu instruktora, nr uprawnień instruktora, zakres uprawnień, informacja o złożeniu wniosku o wpis do ewidencji instruktorów, informacja o braku zatrzymania prawa jazdy, informacja o okresie posiadania uprawnień do kierowania pojazdami	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa	Poczta elektroniczna, CEPIK, portal Starosty	TAK
19	<b>Pracownicy ośrodków szkolenia kierowców</b>	imię, nazwisko, firma przedsiębiorcy, nr NIP, nr REGON, numer wpisu do KRS lub do ewidencji działalności gospodarczej, adres siedziby, adres miejsca zamieszkania, nr telefonu, adres poczty elektronicznej, nr wpisu do rejestru przedsiębiorców prowadzących ośrodki szkolenia kierowców, informacja o złożeniu wniosku o wpis do rejestru przedsiębiorców prowadzących szkolenia kierowców, adres prowadzonego ośrodka, informacja o posiadanych pojazdach		Poczta elektroniczna, CEPIK, portal Starosty	TAK
20	<b>Przewoźnicy</b>	imię, nazwisko, firma przedsiębiorcy, nr NIP, nr PESEL, nr REGON, adres zamieszkania, siedziba przedsiębiorcy, numer certyfikatu kompetencji zawodowych osoby zarządzającej lub numer certyfikatu kompetencji zawodowych przedsiębiorcy, nr w rejestrze przedsiębiorców albo w ewidencji działalności gospodarczej, informacja o złożeniu wniosku, informacja o prowadzeniu przewozów drogowych, zakres	dane dotyczące wyroków skazujących i naruszeń prawa	Poczta elektroniczna, KREPTD	TAK

		przewozu, obszar przewozu, wykaz pojazdów, informacja o zatrudnieniu, informacja o rodzaju transportu drogowego, informacja o dokumentach potwierdzających zapewnienie podjęcia i prowadzenia działalności w zakresie transportu drogowego			
21	<b>Osoby wnioskujące o rekultywację terenów poeksploatacyjnych</b>	imię nazwisko, miejsce zamieszkania, decyzja o kierunku i terminie rekultywacji, zakończeniu rekultywacji terenu po eksploatacji kopaliny		Poczta elektroniczna,	TAK
22	<b>Posiadacze żywych zwierząt</b>	imię, nazwisko, adres zamieszkania, lub prowadzenia hodowli, liczba zwierząt, informacja o dokonaniu wpisu, zmiany lub wykreślenia wpisu, informacja o celu przetrzymywania lub prowadzenia hodowli zwierzęcia, nr i data wydania: zezwolenia na import zwierzęcia do kraju albo zezwolenia na schwytanie zwierzęcia w środowisku albo dokumentu wydanego przez powiatowego lekarza weterynarii, potwierdzającego urodzenie zwierzęcia w hodowli albo innego dokumentu stwierdzającego legalność pochodzenia zwierzęcia		Poczta elektroniczna, Karty Informacyjne	TAK
23	<b>Osoby wnioskujące o koncesje w zakresie kopalin</b>	imię nazwisko, adres zamieszkania, nr telefonu, adres poczty elektronicznej, siedziba prowadzonej działalności gospodarczej, nr NIP, nr REGON, nr PESEL, nr KRS, rodzaj i zakres wykonywanej działalności gospodarczej, informacja o prawie wnioskodawcy do terenu, data rozpoczęcia działalności, okres koncesji, określenie środków, informacja o złożeniu wniosku o udzielenie koncesji		Poczta elektroniczna, Karty Informacyjne, CEIDG	TAK
24	<b>Osoby wnioskujące o wprowadzanie gazów lub pyłów do powietrza</b>	imię nazwisko, adres zamieszkania, nr telefonu, adres poczty elektronicznej, nr NIP, nr PESEL, nr REGON, nr KRS, adres zakładu na terenie którego prowadzona jest eksploatacja instalacji, informacja o tytule prawnym do instalacji, informacja o rodzaju prowadzonej działalności, informacja o wydanym pozwoleniu		Poczta elektroniczna, Karty Informacyjne, CEIDG	TAK
25	<b>Posiadacze karty wędkarskiej i karty łowiectwa podwodnego</b>	imię, nazwisko, miejsce i data urodzenia, adres zamieszkania, wykształcenie, nr karty wędkarskiej, nr karty łowiectwa podwodnego, informacja o złożeniu egzaminu ze znajomości ochrony i połowu ryb		Poczta elektroniczna, Karty Informacyjne,	TAK

26	<b>Posiadacze sprzętu pływającego służącego do amatorskiego połowu ryb</b>	imię, nazwisko, adres zamieszkania, nr dowodu tożsamości, organ wydający dowód tożsamości, dane techniczne sprzętu pływającego, numer rejestracyjny sprzętu pływającego		Poczta elektroniczna, Karty Informacyjne	TAK
27	<b>Osoby zajmujące się gospodarką odpadami</b>	imię, nazwisko, adres zamieszkania, nr telefonu, informacje o instalacji, informacja o rodzaju prowadzonej działalności gospodarczej, adres prowadzonej działalności gospodarczej, nr PESEL, nr NIP, nr REGON, nr KRS, informacja o pozwoleniu na wytwarzanie odpadów, informacja o zatwierdzeniu programu gospodarki odpadami niebezpiecznymi, informacja o zezwoleniu na prowadzenie działalności w zakresie odzysku lub unieszkodliwiania odpadów, informacja o zezwoleniu na prowadzenie działalności w zakresie zbierania lub transportu odpadów, informacja o obszarze prowadzenia działalności w zakresie transportu odpadów		Poczta elektroniczna, Karty Informacyjne, CEIDG	TAK
28	<b>Osoby wnioskujące o wycinkę drzew w lesie</b>	imię, nazwisko, miejsce zamieszkania, numer telefonu, seria i numer dowodu osobistego, informacja o własności działki leśnej, informacja o zarządzaniu działką leśną, informacja o położeniu działki, informacja o złożeniu wniosku, opis taksacyjny		Poczta elektroniczna	TAK
29	<b>Osoby wnioskujące o zmianę przeznaczenia gruntów leśnych</b>	imię, nazwisko, miejsce zamieszkania, numer telefonu, seria i numer dowodu osobistego, informacja o własności działki leśnej, informacja o zarządzaniu działką leśną, informacja o położeniu działki, informacja o złożeniu wniosku, opis taksacyjny		Poczta elektroniczna	TAK
30	<b>Właściciele lub inne osoby władające gruntami leśnymi</b>	imię, nazwisko, miejsce zamieszkania, numer telefonu, seria i numer dowodu osobistego, informacja o własności działki leśnej, informacja o zarządzaniu działką leśną, informacja o położeniu działki, informacja o przyznaniu środków z budżetu państwa, informacja o przyznaniu dotacji, informacja o przyznaniu ekwiwalentu, informacja o utracie ekwiwalentu, opis taksacyjny		Poczta elektroniczna, Karty Informacyjne	TAK
31	<b>Właściciele lub inne osoby władające gruntami, budynkami lub lokalami</b>	imię, nazwisko, imiona rodziców, płeć, seria i numer dowodu tożsamości, obywatelstwo, numer telefonu, nr PESEL, nr NIP, adres poczty elektronicznej, informacje		Poczta elektroniczna, EWOPIS EWMAPA, Ośrodek,	TAK

		dot. numeru działki geodezyjnej, pola powierzchni, opisu jej konturów, użytków gruntowych i klas gleboznawczych, wartości działki, numeru księgi wieczystej lub zbioru dokumentów, numerów dróg publicznych, numerów porządkowych nieruchomości, usytuowania i opisu konturów budynków, wartości budynków, oznaczenia księgi wieczystej budynku lub wyodrębnionych w nim lokali, oznaczenia sposobu i funkcji użytkowych, informacja o opłacie za udostępnienie danych		RWDZ,	
32	<b>Osoby wnoszące o pozwolenie na budowę</b>	imię, nazwisko inwestora, adres zamieszkania, adres do korespondencji, numer telefonu, adres poczty elektronicznej, informacje o obiekcie budowlanym objętym zamierzeniem budowlanym, informacje o celu zamierzenia budowlanego, adres zamierzenia budowlanego, informacja o prawie do dysponowania nieruchomością na cele budowlane, informacje dot. decyzji o warunkach zabudowy i zagospodarowania terenu		Poczta elektroniczna, EWOPIS EWMAPA, Ośrodek, RWDZ, Karty Informacyjne	TAK
33	<b>Osoby zgłaszające budowę obiektu budowlanego lub wykonanie robót budowlanych</b>	imię, nazwisko wnioskodawcy, adres zamieszkania, numer telefonu, adres poczty elektronicznej, rodzaj obiektu, sposób, zakres i termin wykonania robót, nr działki ewidencyjnej, położenie działki, termin przystąpienia do robót, informacja o prawie do dysponowania nieruchomością na cele budowlane		Poczta elektroniczna, EWOPIS EWMAPA, Ośrodek, RWDZ, Karty Informacyjne	TAK
34	<b>Osoby przeprowadzające prace geodezyjne i kartograficzne</b>	imię, nazwisko, numer PESEL, informacja o reprezentacji podmiotu, adres zamieszkania, numer telefonu, adres poczty elektronicznej		EWMAPA, Ośrodek, RWDZ, Karty Informacyjne	TAK
35	<b>Użytkownicy wieczystości i dzierżawcy</b>	imię, nazwisko, imiona rodziców, płeć, seria i numer dowodu tożsamości, obywatelstwo, numer telefonu, nr PESEL, nr NIP, adres poczty elektronicznej, numeru księgi wieczystej		Poczta elektroniczna, EWOPIS EWMAPA, Karty Informacyjne	TAK
36	<b>Nauczyciele i nauczyciele emeryci oraz pracownicy niepedagogiczni</b>	imię, nazwisko, adres zamieszkania, miejsce pracy, wykształcenie, płeć, kraj pochodzenia, obywatelstwo, przypisanie do podmiotu (nazwa podmiotu, adres podmiotu, nr telefonu, nr faksu, strona www, adres e-mail, nr NIP, regon) stopień awansu zawodowego, rodzaj i wymiar prowadzonych zajęć, zawód, numer telefonu, nieobecności,	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa, informacje o przynależności związkowej	Poczta elektroniczna, SIO, SL2014	TAK

		informacja o złożeniu wniosku o podjęcie postępowania egzaminacyjnego na stopień awansu zawodowego nauczyciela mianowanego, informacja o nadaniu stopnia awansu zawodowego nauczyciela kontraktowego, informacja o planie rozwoju zawodowego, informacja o nauczanych przedmiocie, informacja o złożeniu sprawozdania z realizacji planu rozwoju zawodowego, ocena dorobku zawodowego za okres stażu oraz data jej dokonania, informacje o przyznanych nagrodach Starosty, informacja o złożeniu wniosku o przyznanie pomocy zdrowotnej, wysokość dochodu, wizerunek			
37	<b>Uczniowie</b>	imię, nazwisko, imiona rodziców, data i miejsce urodzenia, płeć, kraj pochodzenia, obywatelstwo, adres zamieszkania, nr PSESEL, numer telefonu, nazwa szkoły, wizerunek, przypisanie do podmiotu (nazwa podmiotu, adres podmiotu, nr telefonu, nr faksu, strona www, adres e-mail, nr NIP, regon), przypisanie do klas, okres nauki, kursy zawodowe, języki nauczania, pomoc materialna, dowożenie, orzeczenia/opinie, wypadki, spełnianie obowiązku przedszkolnego/szkolnego/nauki uczestnictwo w zajęciach pozalekcyjnych, informacja o uczestnictwie w projekcie, zawód, informacja o udziale w szkoleniach lub kursach dodatkowych, informacja o odbytych płatnych stażach lub praktykach, informacja o przyznaniu i wysokości stypendium, informacje o przyznanych nagrodach Starosty, informacja dotycząca bezrobotnych w rodzinie, zaświadczenie o dochodach	dane dotyczące zdrowia	Poczta elektroniczna, SIO, SL 2014	TAK
38	<b>Studenci</b>	imię, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PSESEL, wykształcenie, numer telefonu, nazwa uczelni, informacja o przyznaniu i wysokości stypendium, zaświadczenie o dochodach, nr albumu		Poczta elektroniczna, SIO, SL 2014	TAK
39	<b>Dyrektorzy szkół i poradni</b>	imię i nazwisko, wizerunek, data i miejsce urodzenia, adres zamieszkania, adres do korespondencji, nr telefonu, adres poczty elektronicznej, przebieg kariery, informacje o zatrudnieniu u innego pracodawcy, informacje o	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa, informacje o przynależności związkowej	Poczta elektroniczna	TAK

		statusie bezrobotnego, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania			
40	<b>Dyrektorzy szkół i poradni</b>	imię i nazwisko, wizerunek, data i miejsce urodzenia, adres zamieszkania, adres do korespondencji, nr telefonu, adres poczty elektronicznej, płeć, przebieg kariery, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania, informacja o wyborze na dyrektora szkoły, informacje o przyznanych nagrodach Starosty, informacje o przyznanych odznaczeniach Starosty, opinie i oceny Starosty	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa, informacje o przynależności związkowej	Poczta elektroniczna, SIO, SL 2014	TAK
41	<b>Nieletni kierowani do MOW</b>	imię, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, zawód, miejsce pracy, wykształcenie, numer telefonu, informacja o skierowaniu do MOW	dane dotyczące zdrowia	Poczta elektroniczna, SIO, SKORE	TAK
42	<b>Dzieci i młodzież kierowani do szkół specjalnych lub MOS</b>	imię, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, wykształcenie, numer telefonu, informacja o skierowaniu do szkoły specjalnej lub MOS	dane dotyczące zdrowia	Poczta elektroniczna, SIO, SKORE	TAK
43	<b>Członkowie uczniowskich klubów sportowych</b>	imię, nazwisko, data i miejsce urodzenia, miejsce zamieszkania, informacja o obecności na zebraniu założycielskim, informacja o przynależności do uczniowskiego klubu sportowego, informacja o przynależności do klubu sportowego		Poczta elektroniczna,	TAK
44	<b>Pracownicy szkół i placówek</b>	imię, nazwisko, miejsce zamieszkania, adres do		Poczta elektroniczna,	TAK

	<b>niepublicznych o uprawnieniach publicznych</b>	korespondencji, numer telefonu, zajmowane stanowisko, informacja o reprezentacji osoby prawnej, informacja o zgłoszeniu do ewidencji		SIO	
45	<b>Kandydaci do nagród Starosty</b>	imię, nazwisko, data i miejsce urodzenia, adres zamieszkania, numer telefonu, adres poczty elektronicznej, miejsce pracy, imiona rodziców, nazwa i dane teleadresowe wnioskodawcy, notatka biograficzna z informacją o dotychczasowej działalności oraz osiągnięciach kandydata, informacja o założeniu wniosku o przyznanie dorocznej nagrody, informacja o założeniu wniosku o przyznanie nagrody okolicznościowej, informacja o wnioskowanej wysokości i formy nagrody, informacja o przewidywanym terminie i miejsca wręczenia nagrody		Poczta elektroniczna	TAK
46	<b>Laureaci nagród Starosty</b>	imię, nazwisko, data i miejsce urodzenia, adres zamieszkania, numer telefonu, adres poczty elektronicznej, miejsce pracy, imiona rodziców, nazwa i dane teleadresowe wnioskodawcy, notatka biograficzna z informacją o dotychczasowej działalności oraz osiągnięciach kandydata, informacja o założeniu wniosku o przyznanie dorocznej nagrody, informacja o przyznaniu dorocznej nagrody, informacja o założeniu wniosku o przyznanie nagrody okolicznościowej, informacja o przyznaniu nagrody okolicznościowej, informacja o wysokości i formy nagrody, informacja o terminie i miejsca wręczenia nagrody		Poczta elektroniczna, BIP	TAK
47	<b>Członkowie Stałego Dyżuru</b>	imię, nazwisko, adres zamieszkania, numer telefonu, adres poczty elektronicznej, stanowisko, funkcja, miejsce zatrudnienia		Poczta elektroniczna	TAK
48	<b>Członkowie Akcji Kurierskiej</b>	imię, nazwisko, miejsce zamieszkania, adres do korespondencji, numer telefonu		Poczta elektroniczna	TAK
49	<b>Członkowie Powiatowego Zespołu Zarządzania Kryzysowego</b>	imię, nazwisko, adres zamieszkania, numer telefonu, adres poczty elektronicznej, stanowisko, funkcja, miejsce zatrudnienia		Poczta elektroniczna	TAK
50	<b>Osoby kierujące procesem ewakuacji ludności</b>	imię, nazwisko, adres zamieszkania, numer telefonu, adres poczty elektronicznej, stanowisko, funkcja, miejsce zatrudnienia		Poczta elektroniczna	TAK
51	<b>Osoba stająca do</b>	imię, nazwisko, data i miejsce	dane dotyczące zdrowia	Poczta	TAK

	<b>Kwalifikacji Wojskowej</b>	urodzenia, adres zamieszkania, nr PESEL, numer i seria dokumentu tożsamości, stopień zdolności do służby wojskowej		elektroniczna	
52	<b>Członkowie formacji obrony cywilnej</b>	imię, nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, miejsce zamieszkania, adres do korespondencji, numer PESEL, adres poczty elektronicznej, miejsce pracy, numer telefonu, stopień wojskowy, stan cywilny, wykształcenie, zawód ratownika, dotychczasowe miejsce pracy i zajmowane stanowiska, nazwisko, imię i adres najbliższego członka rodziny		Poczta elektroniczna	TAK
53	<b>Członkowie Stanowiska Kierowania</b>	imię, nazwisko, adres zamieszkania, numer telefonu, adres poczty elektronicznej, stanowisko, funkcja, miejsce zatrudnienia		Poczta elektroniczna	TAK
54	<b>Członkowie stowarzyszeń i fundacji</b>	imię nazwisko, miejsce zamieszkania, data i miejsce urodzenia, nr telefonu, adres poczty elektronicznej, nr PESEL, informacja o uprawnieniu do reprezentowania stowarzyszenia lub fundacji, informacja o wpisie do ewidencji stowarzyszeń lub fundacji, informacja o członkostwie stowarzyszenia lub fundacji, pełniona funkcja		Poczta elektroniczna	TAK
55	<b>Uczestnicy postępowania w sprawie sprowadzania zwłok ludzkich z zagranicy</b>	imię, nazwisko, imiona rodziców, płeć, data i miejsce urodzenia, seria i numer dowodu tożsamości, numer telefonu, informacja o pokrewieństwie wnioskodawcy do zmarłego, informacja o śmierci osoby spokrewnionej		Poczta elektroniczna	TAK
56	<b>Członkowie Komisji Bezpieczeństwa i Porządku</b>	imię, nazwisko, adres do korespondencji, adres poczty elektronicznej, miejsce pracy, numer telefonu		Poczta elektroniczna	TAK
57	<b>Kombatanci i osoby represjonowane</b>	imię, nazwisko, nazwisko rodowe, obywatelstwo, data i miejsce urodzenia, płeć, imię ojca, imię matki, nazwisko rodowe matki, obywatelstwo ojca i matki, data miejscowość i kraj urodzenia ojca i matki, informacja o stanie cywilnym, wykształcenie i zawód, nr PESEL, nr telefonu, adres poczty elektronicznej, informacja o zatrudnieniu, seria i nr dowodu osobistego		Poczta elektroniczna	TAK
58	<b>Znalazcy rzeczy oraz osoby, które rzecz zgubiły</b>	imię, nazwisko, adres zamieszkania, rodzaj i numer dokumentu tożsamości, data i organ wydający dokument tożsamości, numer telefonu, informacja o złożeniu		Poczta elektroniczna	TAK

		zawiadomienia o znalezieniu rzeczy, opis zgubionej rzeczy, czas i miejsce zgubienia rzeczy			
59	<b>Cudzoziemcy</b>	imię, nazwisko, nazwisko rodowe, imię ojca, imię matki, nazwisko rodowe matki, data urodzenia, płeć, miejsce urodzenia, państwo urodzenia, narodowość, obywatelstwo, stan cywilny, wykształcenie, wzrost, kolor oczu, znaki szczególne, numer PESEL, numer telefonu, adres poczty elektronicznej, miejsca pobytu, adres korespondencyjny, informacja o celu pobytu, informacja o unieważnieniu lub cofnięciu wizy krajowej wydanej w celu wykonywania pracy, informacja o cofnięciu zezwolenia na pobyt czasowy i pracę		Poczta elektroniczna	TAK
60	<b>Repatrianci</b>	imię, nazwisko, nazwisko rodowe, obywatelstwo, data i miejsce urodzenia, płeć, imię ojca, imię matki, nazwisko rodowe matki, obywatelstwo ojca i matki, data miejscowość i kraj urodzenia ojca i matki, informacja o stanie cywilnym, wykształcenie i zawód, znajomość języka polskiego, nr PESEL, nr telefonu, adres poczty elektronicznej, informacja o zatrudnieniu, informacja o przyznaniu pomocy na zagospodarowanie i remont lokali mieszkalnych, informacja o przyznaniu pomocy na zagospodarowanie i bieżące utrzymanie, zwrot kosztów podróży oraz naukę osób niepełnoletnich, informacja o uznaniu za repatrianta, nr i seria karty czasowego pobytu lub karty stałego pobytu, stosunek do służby wojskowej, informacja o posiadanych orderach i odznaczeniach, informacja o przynależności do organizacji polonijnych, dane dotyczące współmałżonka, dane dotyczące dzieci, seria i nr paszportu, seria i nr dowodu osobistego		Poczta elektroniczna	TAK
61	<b>Osoby korzystające z nieodpłatnej pomocy prawnej</b>	imię nazwisko, data i miejsce urodzenia, miejsce zamieszkania, adres poczty elektronicznej, nr telefonu, nr i seria dokumentu tożsamości, oświadczenie iż osoba nie jest w stanie ponieść kosztów odpłatnej pomocy prawnej		Poczta elektroniczna	TAK
62	<b>Konsumenci</b>	imię, nazwisko, adres zamieszkania, numer telefonu, nr PESEL, płeć, adres poczty elektronicznej, informacja o złożeniu wniosku,		Poczta elektroniczna	TAK

		informacja o prośbie dot. udzielenia porady lub informacji prawnej, przebieg sprawy			
63	<b>Przedsiębiorcy</b>	imię nazwisko, rodzaj prowadzonej działalności gospodarczej, nr NIP, nr REGON, nr PESEL, nr KRS, adres zamieszkania, siedziba, nr telefonu, adres poczty elektronicznej, adres strony internetowej		Poczta elektroniczna	TAK
64	<b>Uczestnicy projektów</b>	imię, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu tożsamości, numer telefonu		Poczta elektroniczna, SL 2014, SIO	TAK
65	<b>Osoby objęte postępowaniem sprawdzającym</b>	imię, nazwisko, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer PESEL, numer NIP, miejsce pracy, zawód, wykształcenie, seria i numer dokumentu potwierdzającego tożsamość, numer telefonu, adres poczty elektronicznej, nazwisko rodowe, nazwisko rodowe matki, stopień wojskowy, seria i numer książeczki wojskowej, informacja o źródle zarobkowania, informacja o wysokości wynagrodzenia, dane dotyczące rodziców, rodzeństwa, małżonka, dzieci, partnera życiowego osoby sprawdzanej	dane dotyczące zdrowia, informacje o przynależności związkowej, informacje o przynależności partyjnej, dane dotyczące wyroków skazujących i naruszeń prawa		TAK
66	<b>Osoby reklamowane od obowiązku pełnienia czynnej służby wojskowej w czasie ogłoszenia mobilizacji i w czasie wojny</b>	imię, nazwisko, imię ojca, służbowy nr telefonu, prywatny nr telefonu, PESEL, stopień wojskowy, adres zamieszkania		Poczta elektroniczna	TAK
67	<b>Osoby przeznaczone do wykonywania świadczeń osobistych i rzeczowych</b>	imię, nazwisko, imię ojca, rok urodzenia, adres zamieszkania, służbowy nr telefonu, prywatny nr telefonu, miejsce zatrudnienia, kwalifikacje, nazwa firmy		Poczta elektroniczna	TAK
68	<b>Osoby realizujące zadania wynikające z obowiązku państwa gospodarza(HNS)</b>	imię, nazwisko, służbowy nr telefonu, prywatny nr telefonu, nr fax, adres poczty elektronicznej, adres do korespondencji, firma, adres siedziby firmy, nr NIP, nr PESEL, nr REGON, zawartość baz danych na potrzeby HNS		Poczta elektroniczna	TAK
69	<b>Osoby uwzględnione w bazach niezbędnych w procesie zarządzania</b>	imię, nazwisko, wizerunek, adres zamieszkania, miejsce zameldowania, stanowisko, funkcja, miejsce zatrudnienia, adres do korespondencji, służbowy nr telefonu, nr fax, służbowy adres		Poczta elektroniczna	TAK

	<b>kryzysowego i planowania cywilnego</b>	poczty elektronicznej, prywatny nr telefonu, prywatny adres poczty elektronicznej, nazwa firmy (zakładu) i instytucji (jednostki), adres i nr telefonu oraz fax siedziby firmy (zakładu) lub instytucji (jednostki), nr NIP, nr PESEL, nr REGON, zawartość baz danych			
--	---	---	--	--	--

**STAROSTA**  
*Mariusz Turalski*

## Załącznik nr 2

Wzór informacji podawanych w przypadku zbierania danych od osoby, której dane dotyczą	
Wzór informacji podawanej w przypadku zbierania danych od Klientów	
Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• strona internetowa</li> <li>• wnioski składane przez Klienta</li> <li>• pismo wszczynające postępowaniem</li> <li>• tablica ogłoszeń</li> </ul>	<p style="text-align: center;"><b>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</b></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li> <li>3. administrator będzie przetwarzał Państwa dane osobowe na podstawie art.6 ust. 1 lit. c) RODO, tj. w celu wypełnienia obowiązku prawnego ciążącego na administratorze, co wynika z ustawy z dnia 5 czerwca 1998 r o samorządzie powiatowym oraz ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego;</li> <li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora</li> </ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe będą przechowywane przez okres wynikający z przepisów prawa, tj. z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) w przypadku realizacji zadań ustawowych podanie danych jest obligatoryjne, w pozostałych przypadkach podanie danych osobowych ma charakter dobrowolny. Konsekwencją niepodania danych będzie odmowa załatwienia sprawy przez administratora;</li> <li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li> </ol>

## Wzór informacji podawanych w przypadku zbierania danych od pracowników

Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• Umowa o pracę</li> <li>• formularz osoby zatrudnionej</li> <li>• oświadczenie o zachowaniu danych w poufności</li> </ul>	<p style="text-align: center;"><b>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</b></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych Pracowników jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li> <li>3. administrator będzie przetwarzał Państwa dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Dane osobowe pracowników są przetwarzane na podstawie art. 6 ust. 1 lit. b) oraz art. 9 ust. 2 lit. b) RODO w zw. z realizacją obowiązków wynikających z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych oraz ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy, a także ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych;</li> <li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li> </ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w ustawie z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy o pracę;</li> <li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li> </ol>

## Wzór informacji podawanych w przypadku zbierania danych od osób ubiegających się o zatrudnienie

Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• ogłoszenie o pracę</li> <li>• formularz osoby ubiegającej się o zatrudnienie</li> </ul>	<p style="text-align: center;"><b>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</b></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych osób ubiegających się o zatrudnienie jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li> <li>3. administrator będzie przetwarzał Państwa dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Dane osobowe pracowników są przetwarzane na podstawie art. 6 ust. 1 lit. c) oraz art. 9 ust. 2 lit. b) RODO w zw. z realizacją obowiązków wynikających z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, a także ustawy z dnia 21 listopada 2008r. o pracownikach samorządowych oraz Regulaminu naboru pracowników na stanowiska urzędnicze;</li> <li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li> </ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe zawarte w dokumentach aplikacyjnych będą przechowywane do czasu ustania celu aplikacyjnego. W przypadku zatrudnienia kandydata wyłonionego w drodze konkursu, dane osobowe w pozostałych dokumentach aplikacyjnych mogą zostać usunięte po upływie 3 miesięcy od zatrudnienia. Natomiast dane osobowe kandydata z którym została zawarta umowa o pracę, mogą być przechowywane do momentu upływu okresu przewidzianego w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu</li> </ol>

ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy o pracę;  
4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.

**STAROSTA**  
*Mariusz Turalski*

## Wzór informacji podawanych w przypadku zbierania danych od wykonawców lub zleceniobiorców

Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• umowa;</li> <li>• formularz oferty;</li> <li>• formularz oświadczenia zleceniobiorcy do celów podatkowych i ubezpieczenia społecznego;</li> <li>• formularz oświadczenia wykonawcy dzieła do celów podatkowych</li> </ul>	<p><b>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</b></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych Wykonawców lub Zleceniobiorców jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li> <li>3. administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. b) RODO, tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;</li> <li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li> </ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy o pracę;</li> <li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li> </ol>

**STAROSTA**  
  
**Mariusz Turalski**

## Wzór informacji podawanych w przypadku zbierania danych od osób składających skargi i wnioski

Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"><li>• Strona internetowa</li><li>• formularz skargi i wniosku</li><li>• tablica ogłoszeń</li></ul>	<p><b>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</b></p> <ol style="list-style-type: none"><li>1. administratorem Państwa danych osobowych osób składających skargi i wnioski jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li><li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li><li>3. administrator będzie przetwarzał Państwa dane osobowe w celu rozpatrzenia skargi lub wniosku. Państwa dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. c) RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego z ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego;</li><li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li><li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li><li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li></ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"><li>1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li><li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li><li>3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości prawnej rozpatrzenia skargi</li><li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li></ol>

**Wzór informacji podawanej w przypadku zbierania danych od osób ubiegających się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych**

Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• regulamin Zakładowego Funduszu Świadczeń Socjalnych;</li> <li>• wniosek o przyznanie Świadczenia z ZFŚS.</li> </ul>	<p align="center"><i>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych osób ubiegających się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li> <li>3. administrator będzie przetwarzał Państwa dane osobowe w celu związanym z rozpatrzeniem i realizacją wniosku o przyznanie świadczenia z Zakładowego Funduszu Świadczeń Socjalnych. Państwa dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. c) RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego z ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych;</li> <li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li> </ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji należnych świadczeń socjalnych wynikających z umowy o pracę;</li> <li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li> </ol>

**Wzór informacji podawanej w przypadku zbierania danych od osób składających wnioski o udostępnienie informacji publicznej**

Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• strona internetowa</li> </ul>	<p align="center"><i>Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych osób wnoszących o udostępnienie informacji publicznej jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej <a href="mailto:ido@powiat.sierpc.pl">ido@powiat.sierpc.pl</a></li> <li>3. administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. c) RODO, tj. w celu wypełnienia obowiązku prawnego ciążącego na administratorze przewidzianego w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej;</li> <li>4. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>5. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>6. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li> </ol> <p><i>Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości udzielenia informacji publicznej w żądanym zakresie ;</li> <li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li> </ol>

**STAROSTA**  
*Mariusz Turalski*

### Załącznik nr 3

Wzór informacji podawanych w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą	
Wzór informacji podawanej w przypadku zbierania danych wykonawców z Internetu	
Miejsce umieszczenia	Treść informacji
<ul style="list-style-type: none"> <li>• treść wiadomości elektronicznej skierowanej do potencjalnego wykonawcy,</li> <li>• formularz oferty wysyłany do potencjalnego wykonawcy</li> </ul>	<p><b>Zgodnie z art. 14 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:</b></p> <ol style="list-style-type: none"> <li>1. administratorem Państwa danych osobowych jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc,</li> <li>2. administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej ido@powiat.sierpc.pl</li> <li>3. administrator będzie przetwarzał Państwa dane osobowe w celu związanych z oszacowaniem wartości zamówienia oraz ewentualnym zawarciem i realizacją umowy o współpracy na podstawie. Dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. b) RODO, tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;</li> <li>4. administrator przetwarza jedynie Państwa dane kontaktowe;</li> <li>5. dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. laboratorium zewnętrznym, kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);</li> <li>6. administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;</li> <li>7. mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.</li> </ol> <p><i>Dodatkowo zgodnie z art. 14 ust. 2 RODO informujemy, że:</i></p> <ol style="list-style-type: none"> <li>1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przedawnienia wynikającego z ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny;</li> <li>2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego;</li> <li>3) dane osobowe zostały pozyskane z publicznie dostępnego źródła, tj. z Internetu;</li> <li>4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.</li> </ol>

## Załącznik nr 4

Wzór oświadczenia o zachowaniu danych osobowych w poufności:

Sierpc .....

imię: \_\_\_\_\_

nazwisko: \_\_\_\_\_

stanowisko: \_\_\_\_\_

wydział: \_\_\_\_\_

### OŚWIADCZENIE

o zachowaniu danych osobowych w poufności  
w Starostwie Powiatowym w Sierpcu  
(dalej „administrator”)

### TREŚĆ OŚWIADCZENIA

W związku z dopuszczeniem do przetwarzania danych osobowych oświadczam, że:

1. Zapoznałam/-em się i zobowiązuję się do przestrzegania obowiązków wynikających z:
  - 1) przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
  - 2) regulacji wewnętrznych administratora danych obowiązujących w obszarze przetwarzania danych osobowych, w tym w szczególności Polityki ochrony danych osobowych.
2. Zapewnię bezpieczeństwo przetwarzanych danych osobowych poprzez ich ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.
3. Zachowam w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie zatrudnienia, jak i po jego zakończeniu.
4. Będę wykonywać polecenia Inspektora Ochrony Danych oraz innych przedstawicieli administratora odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych i sposobów ich zabezpieczenia w poufności.
5. W razie uzyskania nieuprawnionego dostępu do danych osobowych lub wykrycia incydentu godzącego w bezpieczeństwo danych osobowych, zobowiązuję się powiadomić o tym bezpośredniego przełożonego lub Sekretarza Powiatu.
6. Znane mi są zasady monitorowania sposobu używania sprzętu służbowego, w tym m.in. telefonu komórkowego, komputerów, poczty elektronicznej, obowiązujące u administratora. Zostałem poinformowany o zakresie i sposobach prowadzenia ww. monitoringu.
7. Znane mi są zasady odpowiedzialności prawnej za niezgodne z przepisami o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u administratora danych, kodeksu pracy, kodeksu karnego lub kodeksu cywilnego.
8. Zostałem poinformowany, iż:

- 1) administratorem moich danych osobowych jest Starostwo Powiatowe w Sierpcu ul. Świętokrzyska 2A, 09-200 Sierpc
- 2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogę się kontaktować w sprawach przetwarzania moich danych osobowych za pośrednictwem poczty elektronicznej: [ido@powiat.sierpc.pl](mailto:ido@powiat.sierpc.pl)
- 3) administrator będzie przetwarzał moje dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Moje dane osobowe są przetwarzane na podstawie przepisów prawa w szczególności ustawy z dnia 26 czerwca 1974 r. Kodeks pracy oraz ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych;
- 4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);
- 5) mam prawo uzyskać kopię swoich danych osobowych w siedzibie administratora;
- 6) moje dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w przepisach prawa;
- 7) przysługuje mi prawo dostępu do treści moich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;
- 8) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy;
- 9) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o moje dane osobowe.

Oświadczam, że treść niniejszego oświadczenia jest mi znana i zobowiązuje się do jego przestrzegania.

Potwierdzam odbiór 1 egz. niniejszego oświadczenia.

.....  
data i podpis składającego oświadczenie

**STAROSTA**  
  
**Mariusz Turalski**

## Załącznik nr 5

Wzór nadania upoważnienia do przetwarzania danych osobowych:

Sierpc.....

**UPOWAŻNIENIE nr .....**  
do przetwarzania danych osobowych  
w Starostwie Powiatowym w Sierpcu

### TREŚĆ UPOWAŻNIENIA

Działając na podstawie Polityki ochrony danych osobowych, w celu zapewnienia realizacji postanowień 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, zwanego dalej „RODO”, **administrator upoważnia:**

imię: \_\_\_\_\_  
nazwisko: \_\_\_\_\_  
stanowisko: \_\_\_\_\_  
wydział: \_\_\_\_\_

do przetwarzania danych osobowych, których administratorem w rozumieniu art. 4 pkt 7 RODO jest Starostwo Powiatowe w Sierpcu lub które zostały powierzone Starostwu Powiatowemu w Sierpcu do przetwarzania.

Upoważnienie dotyczy przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępu do systemów informatycznych służących do przetwarzania danych osobowych w zakresie zgodnym z zakresem powierzonych czynności.

Upoważnienie traci ważność z chwilą jego cofnięcia, wydania nowego upoważnienia lub ustania stosunku umownego wiążącego upoważnionego ze Starostwem Powiatowym w Sierpcu .

Wzrost: \_\_\_\_\_

\_\_\_\_\_ podpis i pieczęćka Naczelnika Wydziału

\_\_\_\_\_ podpis i pieczęćka Starosty Sierpeckiego

Potwierdzam otrzymanie niniejszego upoważnienia.

\_\_\_\_\_ data i podpis osoby upoważnionej

**STAROSTA**  
*Mariusz Turalski*

## Załącznik nr 6

Wzór cofnięcia upoważnienia do przetwarzania danych osobowych:

Sierpc.....

### COFNIĘCIE UPOWAŻNIENIA nr ..... do przetwarzania danych osobowych w Starostwie Powiatowym w Sierpcu

#### TREŚĆ COFNIĘCIA UPOWAŻNIENIA

Działając na podstawie Polityki ochrony danych osobowych, w celu zapewnienia realizacji postanowień 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, zwanego dalej „RODO”, **administrator cofa upoważnienie:**

imię: \_\_\_\_\_

nazwisko: \_\_\_\_\_

stanowisko: \_\_\_\_\_

wydział: \_\_\_\_\_

do przetwarzania danych osobowych, których administratorem w rozumieniu art. 4 pkt 7 RODO jest Starostwo Powiatowe w Sierpcu lub które zostały powierzone Starostwu Powiatowemu w Sierpcu do przetwarzania.

Cofnięcie upoważnienia dotyczy przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępu do systemów informatycznych służących do przetwarzania danych osobowych w zakresie zgodnym z zakresem powierzonych czynności.

\_\_\_\_\_  
podpis i pieczęćka Naczelnika Wydziału

\_\_\_\_\_  
podpis i pieczęćka Starosty Sierpeckiego

Potwierdzam otrzymanie niniejszego cofnięcia upoważnienia.

\_\_\_\_\_  
data i podpis osoby, której cofnięto upoważnienie

**STAROSTA**  
  
**Mariusz Turalski**

## Załącznik nr 7

Wzór wniosku o nadanie, zmianę lub odebranie uprawnień w systemie:

Sierpc, .....

### Wniosek o NADANIE/ODEBRANIE/ZMIANĘ\* uprawnień użytkownika

Pani/Pan .....

zatrudniona/y na stanowisku .....

w Wydziale .....

Uprawnienie ważne od dnia .....

uprawnienie ważne do dnia: .....

SYSTEM INFORMATYCZNY SERWISY INTERNETOWE (wewnętrzne)	<input type="checkbox"/> Domena	<input type="checkbox"/> Poczta elektroniczna
	<input type="checkbox"/> EZD Elektroniczne Zarządzanie Dokumentacją	<input type="checkbox"/> Bestia
	<input type="checkbox"/> Serwis www powiat.sierpc.pl	<input type="checkbox"/> SJO Bestia
	<input type="checkbox"/> serwis BIP	<input type="checkbox"/> Księgowość Budżetowa
	<input type="checkbox"/> Środki trwałe	<input type="checkbox"/> Kadry i Płace
	<input type="checkbox"/> Edytor Aktów Prawnych	<input type="checkbox"/> Rejestr VAT
	<input type="checkbox"/> eFaktury	<input type="checkbox"/> PJK
	<input type="checkbox"/> Płatnik	<input type="checkbox"/> .....
	<input type="checkbox"/> Ewidencja Nieruchomości Skarbu Państwa i Powiatu	<input type="checkbox"/> System obsługi nieodpłatnej pomocy prawnej
	<input type="checkbox"/> Ewopis	<input type="checkbox"/> Ewmapa
	<input type="checkbox"/> Ośrodek	<input type="checkbox"/> Rejestr Cen
	<input type="checkbox"/> Bank Osnów	<input type="checkbox"/> Geoportal
	SYSTEM INFORMATYCZNY SERWISY INTERNETOWE (zewnętrzne)	<input type="checkbox"/> ePUAP
<input type="checkbox"/> System GUS raport.stat.gov.pl		<input type="checkbox"/> Bank https:bsstarabiala.pl
<input type="checkbox"/> Centralna Ewidencja Pojazdów i Kierowców CEPiK		<input type="checkbox"/> Portal Starosty
<input type="checkbox"/> Rejestr Wniosków, Decyzji i Zgłoszeń w sprawach budowlanych RWDZ		<input type="checkbox"/> System Publicznie dostępny wykaz danych PDW
<input type="checkbox"/> Centralna Ewidencja Informacji Działalności Gospodarczej CEIDG		<input type="checkbox"/> System Informacji Oświatowej SIO

<input type="checkbox"/> System ORE	<input type="checkbox"/> System Biuletyn Zamówień Publicznych <a href="https://bzp.uzp.gov.pl">https://bzp.uzp.gov.pl</a>
<input type="checkbox"/> <a href="https://sl2014.gov.pl">https://sl2014.gov.pl</a>	<input type="checkbox"/> <a href="https://mewa2.mazowia.pl">https://mewa2.mazowia.pl</a>
<input type="checkbox"/> <a href="https://zus.ezd.gov.pl">https://zus.ezd.gov.pl</a>	<input type="checkbox"/> <a href="http://www.bazakonkurencyjności.gov.pl">www.bazakonkurencyjności.gov.pl</a>
<input type="checkbox"/> <a href="https://pfron.org.pl">https://pfron.org.pl</a>	<input type="checkbox"/> <a href="https://car.ezd.pl">https://car.ezd.pl</a>
<input type="checkbox"/> .....	<input type="checkbox"/> .....

.....  
 (podpis Naczelnika Wydziału)

**STAROSTA**  
  
**Mariusz Turalski**

**WYPEŁNIA ADMINISTRATOR SYSTEMU INFORMATYCZNEGO**

<b>Nr wniosku:</b>		
<b>Identyfikator użytkownika systemowego (domena SPSIERPC):</b>		
<b>Identyfikator użytkownika w Systemie EZD:</b>		
<b>Identyfikator użytkownika w systemach informatycznych, serwisach internetowych:</b>	<i>nazwa systemu informatycznego, serwisu internetowego</i>	<i>identyfikator</i>
<b>Nazwa konta mailowego:</b>		
<b>Data zarejestrowania/zmiany* w systemach:</b>		
<b>Data wyrejestrowania użytkownika (zablokowania dostępu) z systemów:</b>		

*Użytkownik wraz z kopią dokumentu otrzymał kopertę z loginami i hasłami do poszczególnych systemów.*

Potwierdzam otrzymanie uprawnień

\_\_\_\_\_ podpis Administratora Systemów Informatycznych

\_\_\_\_\_ podpis użytkownika

**STAROSTA**  
*Mariusz Turalski*





## Załącznik nr 10

Wzór umowy powierzenia przetwarzania danych osobowych:

### UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Niniejsza umowa została zawarta w Sierpcu w dniu ..... r. roku przez:

.....

.....

zwaną dalej „**Administratorem**”,  
reprezentowaną przez:

.....  
oraz

.....

.....

zwaną dalej „**Podmiotem Przetwarzającym**”,  
reprezentowaną przez:

.....

Administrator i Podmiot Przetwarzający będą dalej zwani łącznie „**Stronami**”, a każdy z osobną „**Stroną**”.

Zważywszy, że:

1. Administrator jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 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, zwanego dalej „**RODO**”, wskazanych w załączniku nr 1 do umowy.
2. Administrator zamierza powierzyć Podmiotowi Przetwarzającemu przetwarzanie danych osobowych, a Podmiot Przetwarzający zamierza przyjąć powierzone mu dane osobowe do przetwarzania w imieniu Administratora, zgodnie z umową oraz z przepisami regulującymi przetwarzanie danych osobowych, wiążącymi Podmiot Przetwarzający i Administratora.

Strony postanowiły, co następuje:

## § 1

### Przedmiot umowy

Administrator powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych w imieniu Administratora, na zasadach określonych w Umowie oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w szczególności w RODO.

Rodzaj danych osobowych, kategorie osób, których dotyczą dane osobowe, jak również przedmiot, czas trwania, charakter i cel przetwarzania danych osobowych są wskazane w załączniku nr 1 do umowy.

Strony zobowiązują się wykonywać zobowiązania wynikające z umowy z najwyższą starannością, w celu prawidłowego zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron oraz osób, których dane osobowe dotyczą, w zakresie przetwarzania danych osobowych.

## § 2

### Oświadczenie Podmiotu Przetwarzającego

Podmiot Przetwarzający oświadcza, że:

- a) wdrożył środki techniczne i organizacyjne gwarantujące przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami, w sposób zapewniający ochronę praw osób, których dotyczą dane osobowe; oraz
- b) dysponuje środkami, doświadczeniem, wiedzą oraz odpowiednio wyszkolonym personelem, umożliwiającymi prawidłowe przetwarzanie danych osobowych w zakresie i w celu określonych w umowie.

## § 3

### Przetwarzanie danych osobowych

1. Z zastrzeżeniem ust. 2, przetwarzanie danych osobowych przez Podmiot Przetwarzający może następować wyłącznie w przypadkach wynikających z Umowy lub na podstawie odrębnych zleceń Administratora, wyrażonych w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej).
2. Podmiot Przetwarzający ma prawo przetwarzać dane osobowe, jeżeli obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. W takim przypadku Podmiot Przetwarzający jest zobowiązany poinformować Administratora o stosującym się do niego obowiązku prawnym co najmniej na 24 godziny przed rozpoczęciem przetwarzania, chyba że wiążące go przepisy zabraniają mu udzielania takiej informacji, z uwagi na ważny interes publiczny.
3. Przetwarzanie danych osobowych przez Podmiot Przetwarzający jest ograniczone do celu i zakresu wskazanych w załączniku nr 1 do umowy.
4. Podmiot Przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych, zawierający informacje wymagane przez obowiązujące przepisy, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
5. Podmiot Przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
6. Wszelkie zlecane przez Administratora operacje przetwarzania danych osobowych Podmiot Przetwarzający wykonuje niezwłocznie, w szczególności jeśli chodzi o usunięcie danych osobowych na żądanie osoby, której dotyczą.

7. Biorąc pod uwagę charakter przetwarzania danych osobowych, Podmiot Przetwarzający ma obowiązek współdziałania z Administratorem w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w obowiązujących przepisach, wdrażając odpowiednie środki techniczne i organizacyjne.
8. Podmiot Przetwarzający zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
  - a) otrzymają pisemne upoważnienia do przetwarzania danych osobowych;
  - b) będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
  - c) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora, z zastrzeżeniem ust. 2; oraz
  - d) zobowiążą się do bezterminowego zachowania w tajemnicy danych osobowych oraz stosowanych przez Podmiot Przetwarzający sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z odpowiednich przepisów.
9. Podmiot Przetwarzający prowadzi ewidencję udzielonych upoważnień do przetwarzania danych osobowych, o których mowa w ust. 8 lit. a).

#### § 4

##### Dalsze powierzenia przetwarzania

1. Podmiot Przetwarzający ma prawo korzystać z podwykonawców przy przetwarzaniu danych osobowych (dalsze powierzenie przetwarzania), pod warunkiem, że przed powierzeniem podwykonawcy przetwarzania danych osobowych:
  - a) uzyska na to zgodę Administratora, wyrażoną w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej);
  - b) zawrze z podwykonawcą umowę powierzenia przetwarzania danych osobowych na warunkach nie gorszych niż warunki umowy;
  - c) upewni się, że podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom obowiązujących przepisów.
2. Jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wypełnienie obowiązków podwykonawcy.
3. Wykaz podwykonawców, z których Podmiot Przetwarzający korzysta w dniu zawarcia umowy, i co do których Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych osobowych, stanowi załącznik nr 2 do umowy.

#### § 5

##### Bezpieczeństwo danych osobowych

1. Podmiot Przetwarzający stosuje środki techniczne i organizacyjne, odpowiednie do zagrożeń oraz charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, zapewniające bezpieczeństwo danych osobowych, w szczególności przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.

2. Podmiot Przetwarzający zobowiązuje się stale monitorować stan stosowanych zabezpieczeń danych osobowych oraz występujących zagrożeń bezpieczeństwa, i w razie potrzeby aktualizuje stosowane środki techniczne i organizacyjne, tak, żeby zapewnić najwyższy osiągalny poziom ochrony danych osobowych.
3. Podmiot Przetwarzający, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Administratorem w wywiązaniu się z obowiązków określonych w art. 32–36 RODO.
4. Podmiot Przetwarzający niezwłocznie zawiadamia Administratora, przed podjęciem jakichkolwiek działań, o każdym przypadku:
  - a) wystąpienia jakiegokolwiek organu z żądaniem udostępnienia danych osobowych, chyba że zakaz ujawnienia tej informacji wynika z obowiązujących przepisów;
  - b) wystąpienia przez osobę, której dane osobowe dotyczą, z żądaniem dotyczącym przetwarzania danych osobowych lub ich treści.
5. Podmiot Przetwarzający niezwłocznie – w każdym wypadku nie później niż w ciągu 24 godzin od wykrycia – informuje Administratora o wszelkich wykrytych naruszeniach bezpieczeństwa danych osobowych, przekazując Administratorowi wszelkie dostępne Podmiotowi Przetwarzającemu informacje na temat naruszenia, w szczególności:
  - a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorii i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorii i przybliżoną liczbę wpisów, których dotyczy naruszenie;
  - b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - c) możliwe konsekwencje naruszenia ochrony danych osobowych; oraz
  - d) środki zastosowane lub proponowane przez Podmiot Przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Podmiot Przetwarzający współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym Administratorowi naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.
7. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu przez Administratora polecenie dotyczące przetwarzania danych osobowych stanowi naruszenie obowiązujących przepisów.

## § 6

### Prawo do kontroli

1. Administrator ma prawo kontrolowania sposobu wypełniania przez Podmiot Przetwarzający jego obowiązków określonych w umowie lub w obowiązujących przepisach. W szczególności Administrator może żądać udostępnienia określonych informacji lub dokumentów oraz może przeprowadzać – samodzielnie lub przez upoważnionego przez Administratora pracownika lub współpracownika – audyty, w tym inspekcje w miejscu przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. Podmiot Przetwarzający ma obowiązek współpracować z Administratorem lub upoważnionym przez Administratora pracownikiem lub współpracownikiem w czasie przeprowadzanej kontroli, w sposób umożliwiający Administratorowi weryfikację prawidłowej realizacji obowiązków Podmiotu Przetwarzającego.

## § 7

### Rozwiązanie umowy

1. Umowa wchodzi w życie z dniem podpisania umowy i zostaje zawarta na czas określony do dnia rozwiązania lub wygaśnięcia ostatniej z umów łączących Strony, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. W przypadku stwierdzenia naruszenia przez Podmiot Przetwarzający obowiązków wynikających z umowy, Administrator ma prawo rozwiązać wszystkie umowy zawarte z Podmiotem Przetwarzającym, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający, ze skutkiem natychmiastowym.
3. Najpóźniej w dniu rozwiązania umowy Podmiot Przetwarzający ma obowiązek:
  - a) usunąć wszelkie dane osobowe; albo
  - b) zwrócić Administratorowi wszelkie nośniki zawierające dane osobowe oraz usunąć wszelkie istniejące kopie danych osobowych, chyba że obowiązujące przepisy wymagają od niego dalszego przechowywania części lub całości danych osobowych,
  - c) zależnie od wyboru Administratora, zakomunikowanego Podmiotowi Przetwarzającemu w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej) co najmniej na 7 dni przed terminem rozwiązania Umowy.
4. W przypadku rozwiązania Umowy w trybie ust. 2 wybór Administratora będzie zakomunikowany Podmiotowi Przetwarzającemu w oświadczeniu o rozwiązaniu umowy ze skutkiem natychmiastowym.
5. Czynności wskazane w ust. 3 zostaną wykazane w pisemnym protokole, podpisanym przez przedstawiciela Podmiotu Przetwarzającego i dostarczonym Administratorowi w terminie 7 dni od dokonania wskazanych w nim czynności.

#### § 8

#### Postanowienia końcowe

1. Podmiotowi Przetwarzającemu nie przysługuje wynagrodzenie za wykonywanie Umowy.
2. Umowa stanowi całość porozumienia pomiędzy Stronami i zastępuje w całości uprzednie lub równoczesne uzgodnienia poczynione przez Strony (w formie pisemnej lub ustnej) w przedmiocie regulowanym postanowieniami niniejszej Umowy.
3. Załączniki do Umowy stanowią jej integralną część.
4. Wszelkie spory między Stronami będą rozwiązywane na zasadzie polubownych negocjacji. W przypadku nieosiągnięcia przez Strony porozumienia, spór zostanie przekazany do rozstrzygnięcia sądowi powszechnemu właściwemu dla siedziby Administratora.
5. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
6. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron.

Administrator:

Podmiot Przetwarzający:

\_\_\_\_\_

\_\_\_\_\_

**STAROSTA**  
*Mariusz Turalski*

## Załącznik I – Dane osobowe

<b>Rodzaje danych osobowych</b> (np. imię, nazwisko, adres, numer PESEL, numer telefonu, e-mail, adres IP, dane o stanie zdrowia)	
<b>Kategorie osób, których dane osobowe dotyczą</b> (np. pracownicy, dostawcy, pacjenci, kontrahenci, klienci)	
<b>Zakres przetwarzania danych osobowych</b> (czynności dokonywane na powierzonych danych osobowych, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, adaptowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, udostępnianie, zmienianie, usuwanie)	
<b>Charakter przetwarzania</b> (np. systematyczny/sporadyczny)	
<b>Cel przetwarzania</b> (np. wykonanie umowy z dnia...)	
<b>Czas przetwarzania</b> (np. <i>okres obowiązywania umowy z dnia...</i> )	

**Załącznik II – Podwykonawcy zatwierdzeni przez Administratora**

<b>Lp.</b>	<b>Nazwa</b>	<b>Adres</b>	<b>NIP</b>



## Załącznik nr 12

Wzór wykazu podmiotów przetwarzających:

Wykaz podmiotów przetwarzających dane osobowe w imieniu administratora					
Lp.	Nazwa podmiotu	Adres	Kod pocztowy	Poczta	Informacje o umowie

**STAROSTA**  
*Mariusz Turalski*





## Załącznik nr 15

Wzór formularza oceny skutków:

Ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych	
1. Informacje ogólne	
Administrator danych osobowych:	
Oceniane operacje przetwarzania <sup>1</sup> :	[opis ocenianych operacji]
Data przeprowadzenia oceny:	[data przeprowadzenia pierwszej oceny]
Daty aktualizacji oceny:	1. [ data pierwszej aktualizacji oceny] 2. [ data drugiej aktualizacji oceny] 3. [ data trzeciej aktualizacji oceny]
Powód aktualizacji oceny:	1. [ powód pierwszej aktualizacji oceny] 2. [ powód drugiej aktualizacji oceny] 3. [ powód trzeciej aktualizacji oceny]
2. Opis planowanych operacji przetwarzania danych osobowych	
1. Uwagi ogólne	
2. Charakter przetwarzania danych osobowych <sup>2</sup>	
3. Zakres przetwarzania danych osobowych <sup>3</sup>	
4. Kontekst przetwarzania danych osobowych <sup>4</sup>	
5. Cele przetwarzania danych osobowych <sup>5</sup>	
6. Podmioty uczestniczące w przetwarzaniu	Podmioty przetwarzające dane Osoby upoważnione
7. Okres przetwarzania	
8. Aktywa wykorzystywane do przetwarzania danych osobowych <sup>6</sup>	
9. Stosowanie zatwierdzonych kodeksów postępowania <sup>7</sup>	
3. Ocena niezbędności i proporcjonalności przetwarzania danych osobowych	
1. Czy dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach? <sup>8</sup>	
2. Czy dane osobowe są przetwarzane zgodnie z prawem? <sup>9</sup>	
3. Czy dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane?	
4. Czy okres przechowywania danych osobowych został stosownie ograniczony?	
4. Ocena wdrożenia środków pozwalających na realizację praw podmiotów danych	
1. Czy zapewnione są odpowiednie środki, aby udzielić podmiotowi danych osobowych wszelkich wymaganych przez prawo informacji?	
	prawo dostępu do danych

2. Czy zapewnione są odpowiednie środki, aby umożliwić podmiotowi danych osobowych realizację:	osobowych	
	prawo do przenoszenia danych osobowych	
	prawo do sprostowania danych osobowych	
	prawo do przenoszenia danych osobowych	
	prawo do sprzeciwu	
	prawo do ograniczenia przetwarzania danych osobowych	
3. Czy ograniczono liczbę odbiorców danych osobowych?		
4. Czy zapewniono odpowiednie relacje z podmiotami przetwarzającymi dane osobowe? <sup>10</sup>		
5. Czy zapewniono odpowiednie zabezpieczenia przy międzynarodowym przekazywaniu danych osobowych (z uwzględnieniem stopnia ochrony występującego w państwie, do którego przekazywane są dane osobowe)?		
6. Czy przeprowadzono uprzednie konsultacje z organem nadzorczym?		
<b>5. Zaangażowanie zainteresowanych stron</b>		
1. Czy administrator danych dostatecznie ograniczył zidentyfikowane ryzyko? Czy środki zaplanowane są wystarczające do ograniczenia ryzyka do dopuszczalnego poziomu?		
2. Czy przetwarzanie danych odbywa się w celu wykonania zadania realizowanego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym?		
3. W przypadku odpowiedzi negatywnej na pytanie V.1 lub odpowiedzi pozytywnej na pytanie V.2, czy skonsultowano się z inspektorem ochrony danych w celu uzyskania zaleceń?		
4. Czy udokumentowano decyzję inspektora ochrony danych i wprowadzono konkretne rozwiązanie do oceny skutków dla ochrony danych?		
5. Czy skonsultowano się z użytkownikiem bądź jego przedstawicielem w celu zasięgnięcia opinii w zakresie planowanego przetwarzania danych?		
<b>6. Monitorowanie i przegląd ryzyka</b>		
1. Za pomocą jakich narzędzi prowadzone jest monitorowanie ryzyka?		
2. Jaka jest częstotliwość przeglądu ryzyka?		
3. W jaki sposób dokonuje się przeglądu ryzyka?		
4. Czy po przeprowadzeniu monitoringu i przeglądu		

ryzyka miała miejsce zmiana klasyfikacji ryzyka?	
5. Czy po zmianie klasyfikacji ryzyka opracowano odpowiednią strategię postępowania w celu jego ograniczenia?	
Podpis osób odpowiedzialnych	
imię i nazwisko - stanowisko	imię i nazwisko - stanowisko

<sup>1</sup> Do operacji wymagających przeprowadzenia oceny skutków przetwarzania dla ochrony danych osobowych zalicza się w szczególności (lecz nie wyłącznie):

1. Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą” (motyw 71 i 79 RODO).
2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku wobec osoby fizycznej (art. 35 ust. 3 lit. a RODO).
3. Systematyczne monitorowanie, tj. przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, w tym gromadzenie danych za pośrednictwem sieci lub systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie (art. 35 ust. 3 lit. c RODO).

Grupa Robocza Art. 29 wskazuje, iż „systematycznie” uzyskuje jedno z następujących znaczeń:

- a) przeprowadzane w ramach określonego systemu;
- b) wcześniej zaplanowane, zorganizowane lub mające metodyczny charakter;
- c) odbywające się w ramach ogólnego planu gromadzenia danych;
- d) realizowane jako część strategii.

Pojęcie „miejsca publicznie dostępne” interpretować należy jako miejsca otwarte dla każdego obywatela, np. plac, centrum handlowe, ulica, rynek, stacja kolejowa, biblioteka publiczna. Katalog miejsc publicznie dostępnych nie jest zamknięty.

4. Przetwarzanie danych wrażliwych lub danych o charakterze wysoce osobistym: w szczególności kategorii danych osobowych ujętych w art. 9 RODO oraz danych osobowych dotyczących wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO.

5. Przetwarzanie danych na dużą skalę. Przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, zaleca się wziąć pod uwagę następujące czynniki:
  - a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
  - b) liczbę danych lub zakres poszczególnych przetwarzanych pozycji danych;
  - c) czas trwania lub trwałość czynności przetwarzania danych;
  - d) zakres geograficzny czynności przetwarzania.
6. Dopasowanie lub łączenie zbiorów danych, np. pochodzących z co najmniej dwóch operacji przetwarzania danych prowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.
7. Przetwarzanie danych dotyczących osób wymagających szczególnej opieki, pozbawionych przysługujących im praw i wolności oraz kontroli nad zarządzaniem ich danymi osobowymi. Do osób tych zaliczyć należy dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl, osoby starsze, pacjenci). Uwzględnić tu należy każdą sytuację, w której można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.
8. Innowacyjne wykorzystanie lub stosowanie przy przetwarzaniu danych nowych rozwiązań technologicznych lub organizacyjnych takich jak połączenie technologii rozpoznającej odcisk palca i twarzy w celu poprawienia fizycznej kontroli dostępu.
9. Przesyłanie danych poza granice Unii Europejskiej.
10. Przetwarzanie, które „uniemożliwia osobom, których dane dotyczą, wykonywanie lub korzystanie z usługi lub umowy” (art. 22 i motyw 91 RODO). Obejmuje operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

W przypadku, gdy operacja przetwarzania danych spełnia co najmniej dwa z ww. kryteriów, należy przeprowadzić w odniesieniu do takiej operacji ocenę skutków dla ochrony danych. W niektórych przypadkach administrator danych może uznać, że operacja przetwarzania spełniająca tylko jedno z wymienionych powyżej kryteriów będzie wymagała przeprowadzenia oceny skutków dla ochrony danych.

Kategorie operacji niewymagających przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych:

1. Operacje, które nie „powodują ryzyka naruszenia praw lub wolności osób, których dane dotyczą”.
2. Operacje, których zakres, kontekst i cele przetwarzania są bardzo podobne do operacji przetwarzania, w przypadku których przeprowadzono ocenę skutków dla ochrony danych.
3. Operacje, które zostały sprawdzone przez organ nadzorczy przed majem 2018 roku, w szczególnych warunkach, które nie uległy zmianie, tj. decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE (do czasu ich zmiany, zastąpienia lub uchylecia).
4. Operacje, które mają podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje dane operacje przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już z przyjęciem tej podstawy prawnej, chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem operacji przetwarzania.
5. Operacje przetwarzania umieszczone w opcjonalnym wykazie (utworzonym przez organ nadzorczy) operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych.

<sup>2</sup> Charakter przetwarzania danych osobowych – należy wskazać, czy dane osobowe są przetwarzane w sposób całkowicie, częściowo zautomatyzowany czy w sposób inny niż zautomatyzowany; jaka jest częstotliwość przetwarzania, czy przetwarzanie ma charakter krótko- czy długoterminowy, systematyczny czy sporadyczny, na jaką skalę przetwarzanie jest prowadzone (charakter masowy, znikomy).

<sup>3</sup> Zakres przetwarzania danych osobowych – należy zawrzeć w tym miejscu opis każdej z planowanych operacji przetwarzania, dokonywanych na danych osobowych.

<sup>4</sup> Kontekst przetwarzania danych osobowych – w punkcie tym należy wskazać wszelkie okoliczności prawne faktyczne planowanego przetwarzania – kategorie przetwarzanych danych, kategorie osób, których dane dotyczą, okoliczności zbierania i dalszego przetwarzania danych osobowych (wykonanie obowiązków informacyjnych, zebranie danych na potrzeby wykonania innych czynności prawnych np. zawarcia umowy), a także otoczenie i zagrożenie dla bezpieczeństwa i integralności danych.

<sup>5</sup> Cel przetwarzania danych – należy wskazać konkretne, wyraźne, jednoznaczne, ograniczone i legalne cele. O celach przetwarzania danych decyduje administrator danych. Przetwarzanie danych sprzeczne z celami, dla których zostały zebrane, jest niezgodne z prawem. Przetwarzanie danych w celach nieokreślonych lub określonych nieprecyzyjnie, tj. nieograniczonych i niejasnych powoduje niezgodność przetwarzania z prawem.

<sup>6</sup> Kategorie aktywów – w tym miejscu należy wyszczególnić:

1. procesy i działania biznesowe – seria powiązanych ze sobą działań lub zadań, które realizują operacje przetwarzania danych osobowych lub prowadzą do osiągnięcia celu przetwarzania danych;
2. personel – wszystkie grupy osób zaangażowane w przetwarzanie danych tj.: decydenci, użytkownicy, personel eksploatacji/utrzymania, twórcy oprogramowania;
3. sprzęt – wszelkie urządzenia fizyczne w organizacji tj.: urządzenia przenośne, stacjonarne, peryferyjne, nośniki danych;
4. siedziba – wszelkie lokalizacje wykorzystywane do przetwarzania danych oraz środki fizyczne potrzebne do ich funkcjonowania tj. siedziba, strefy bezpieczeństwa, usługi komunalne i techniczne;
5. oprogramowanie – wszelkie programy uczestniczące w operacjach przetwarzania danych tj.: systemy operacyjne, aplikacje biznesowe, oprogramowania usługowe, utrzymaniowe lub administracyjne;
6. sieć – wszelkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego, tj.: media i usługi wspierające, przekaźniki aktywne lub pasywne, interfejsy komunikacyjne;
7. kanały transmisji – wszelkie rodzaje mediów służących do przekazu informacji między nadawcą a odbiorcą.

<sup>7</sup> W przypadku braku kodeksów postępowania regulujących zasady przeprowadzania opisywanej operacji przetwarzania danych należy uwzględnić te informacje w odpowiedzi na pytanie.

<sup>8</sup> Odpowiedź powinna być oparta na analizie i porównaniu odpowiedzi z punktu 2.5 dotyczącej celu przetwarzania danych osobowych ze stanem faktycznym.

<sup>9</sup> Zgodność z prawem – zgodnie z art. 5 ust. 1 RODO dane powinny być przetwarzane zgodnie z prawem, tj. z ustawami i rozporządzeniami wydanymi na podstawie ustaw z uwzględnieniem interesów podmiotów danych.

<sup>10</sup> Podstawowe wymagania dotyczące treści porozumienia między administratorem a podmiotem przetwarzającym dane osobowe zostały określone w art. 28 RODO.

