

Załącznik
do zarządzenia nr OR.120.40.2018
Starosty Nowotomyskiego
z dnia 11.10.2018r.

POLITYKA OCHRONY DANYCH OSOBOWYCH
w Starostwie Powiatowym w Nowym Tomyślu

Spis treści

Spis załączników		3
Rozdział I	Postanowienia ogólne	4
Rozdział II	Słownik pojęć	4
Rozdział III	Zakres stosowania Polityki i zakres przetwarzania	7
Rozdział IV	Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem	7
Rozdział V	Polecenie osobom przetwarzania danych osobowych	12
Rozdział VI	Polecenie przetwarzania danych osobowych podmiotowi przetwarzającemu	14
Rozdział VII	Zasady przetwarzania danych osobowych	14
Rozdział VIII	Zgodność przetwarzania z prawem	15
Rozdział IX	Realizacja obowiązków informacyjnych	16
Rozdział X	Prawa osoby, której dane osobowe dotyczą	16
Rozdział XI	Obszar przetwarzania danych osobowych	17
Rozdział XII	Przetwarzanie danych osobowych w systemie informatycznym i na nośnikach papierowych	18
Rozdział XIII	Postępowanie w sytuacji naruszenia ochrony danych osobowych	18
Rozdział XIV	Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO	19
Rozdział XV	Ocena ryzyka naruszenia praw lub wolności osób fizycznych	19
Rozdział XVI	Odpowiedzialność karna	20
Rozdział XVII	Postanowienia końcowe	20

Spis załączników

Załącznik 1	Wzór rejestru czynności przetwarzania danych osobowych administratora
Załącznik 2	Wzór rejestru czynności przetwarzania danych osobowych podmiotu przetwarzającego
Załącznik 3	Zasady organizacji edukacji z zakresu ochrony danych osobowych
Załącznik 4	Wzór informacji o przeprowadzeniu szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk
Załącznik 5	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
Załącznik 6	Struktura zarządzania przetwarzaniem danych osobowych oraz ich bezpieczeństwem
Załącznik 7	Upoważnienie do przetwarzania danych osobowych
Załącznik 8	Upoważnienie do udzielania oraz cofania upoważnień do przetwarzania danych osobowych
Załącznik 9	Oświadczenie o zachowaniu poufności
Załącznik 10	Struktura organizacyjna związana z polecaniem osobom przetwarzania danych osobowych
Załącznik 11	Wzory zapisów umowy dotyczącej powierzenia czynności przetwarzania danych osobowych
Załącznik 12	Klauzula informacyjna
Załącznik 13	Zgoda na przetwarzanie danych osobowych
Załącznik 14	Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych
Załącznik 15	Arkusz szacowania ryzyka naruszenia praw lub wolności osób fizycznych

Rozdział I

Postanowienia ogólne

§ 1

Polityka Ochrony Danych Osobowych określa zasady w zakresie zarządzania procesami przetwarzania danych osobowych oraz ich bezpieczeństwem w Starostwie Powiatowym w Nowym Tomysku.

§ 2

Niniejszy dokument wykonany został na podstawie zapisów art. 24 ust. 2 i art. 32 ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 z uwzględnieniem opinii zawartej w motywie 78 tego rozporządzenia.

Rozdział II

Słownik pojęć

§ 3

Występujące w Polityce Ochrony Danych Osobowych zwroty oznaczają:

Administrator – Starosta Nowotomyski;

IOD – Inspektor Ochrony Danych – osoba wyznaczona zarządzeniem przez Starostę, na podstawie art. 37 ust. 1 RODO, realizujący zadania, o których mowa w art. 39 ust. 1 RODO;

ASI - Administrator Systemów Informatycznych - administrator aplikacji/systemów w Starostwie, w których są przetwarzane dane osobowe; osoba odpowiedzialna za realizację zabezpieczeń i odpowiednie funkcjonowanie systemów informatycznych w Starostwie, w których przetwarzane są dane osobowe;

dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

identyfikator użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym, zwany dalej także identyfikatorem;

incydent bezpieczeństwa – jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności, niezawodności i bezpieczeństwa systemu informatycznego, powstałe

samoistnie w systemie, bądź dokonane przez osoby nieuprawnione lub uprawnione, działające w złej wierze albo omyłkowo;

klauzula informacyjna – zbiór informacji jakie powinny być przekazane osobie, której dane dotyczą w celu realizacji obowiązków informacyjnych Administratora w stosunku do tych osób, określonych w RODO;

komórka organizacyjna – zgodnie z Regulaminem Organizacyjnym Starostwa Wydziały lub jednoosobowe stanowiska pracy;

KKO – kierownik komórki organizacyjnej Starostwa – kierownik Wydziału lub osoba zatrudniona na jednoosobowym stanowisku pracy, zgodnie ze strukturą organizacyjną określoną w Regulaminie Organizacyjnym, lub osoba aktualnie zastępująca kierownika Wydziału lub osobę zatrudnioną na jednoosobowym stanowisku pracy;

naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

obszar przetwarzania danych osobowych – pomieszczenia, części pomieszczeń lub teren wokół obiektów Starostwie, w których przetwarza się dane osobowe w formie papierowej, jak i w systemie informatycznym,

odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców;

Organ Nadzorczy – Prezes Urzędu Ochrony Danych Osobowych, niezależny organ publiczny ustanowiony przez Rzeczpospolitą Polską zgodnie z art. 51 RODO;

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

PODO - Polityka Ochrony Danych Osobowych w Starostwie, zwana dalej także Polityką;

przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;

system informatyczny przetwarzający dane osobowe – zespół współpracujących ze sobą urządzeń, programów, narzędzi programowych, wraz z procedurami do ich obsługi, zastosowany w celu przetwarzania danych, w celu przetwarzania danych osobowych w Starostwie, zwany dalej także systemem;

szczególne kategorie danych osobowych - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;

RODO – ogólne rozporządzenie o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679

uodo - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2018r. poz. 1000 ze zm.),

usuwanie danych osobowych – niszczenie danych osobowych lub taką ich modyfikację, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;

użytkownik – osoba upoważniona do bezpośredniego dostępu do danych osobowych, przetwarzanych w systemie informatycznym lub aplikacji, która posiada ustalony indywidualny identyfikator oraz hasło;

zasób danych osobowych – wszystkie dane osobowe, niezależnie od sposobu ich utrwalenia, występujące w zbiorach, jak i w formie nieuporządkowanej, przetwarzane przez Starostwo w celu realizacji jej zadań; w zasobach Starostwa wyróżnia się zasoby poszczególnych komórek organizacyjnych;

zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

SP – Starostwo Powiatowe w Nowym Tomyślu

Rozdział III **Zakres stosowania Polityki i zakres przetwarzania**

§ 4

1. Polityka ma zastosowanie do:

- 1) danych osobowych przetwarzanych w Starostwie niezależnie od sposobu ich utrwalenia,
- 2) danych osobowych przetwarzanych, zarówno w zbiorach jak i w formie nieuporządkowanej w zestawach, jak i pojedynczych informacji osobowych,
- 3) informacji, dotyczących bezpieczeństwa danych osobowych, w szczególności identyfikatorów i haseł we wszystkich systemach/aplikacjach,
- 4) informacji zawartych w rejestrach, instrukcjach i procedurach związanych z przetwarzaniem lub ochroną danych osobowych.

2. W Starostwie prowadzone są następujące rejestry czynności przetwarzania danych osobowych, na które to przetwarzanie zgodę wyraził Administrator:

- 1) Rejestr Czynności Przetwarzania Danych Osobowych Administratora - dla zbiorów danych osobowych, dla których administratorem jest Administrator; wzór rejestru określony został w załączniku nr 1 do PODO,

- 2) Rejestr Czynności Przetwarzania Danych Osobowych Podmiotu Przetwarzającego - dla zbiorów danych osobowych, dla których podmiotem przetwarzającym jest Administrator; wzór rejestru określony został w załączniku nr 2 do PODO.
3. W Starostwie nie powinny być przetwarzane żadne zasoby danych osobowych, w szczególności zbiory danych osobowych, na które to przetwarzanie nie wyraził zgody Administrator.

Rozdział IV

Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

§ 5

1. Administratorem danych osobowych, w rozumieniu art. 4 pkt. 1) RODO, w Starostwie jest Starosta Nowotomyski.
2. Administrator jest odpowiedzialny za przetwarzanie i ochronę danych osobowych w Starostwie.
3. Strukturę zarządzania przetwarzaniem danych osobowych oraz ich bezpieczeństwem przedstawia graficznie załącznik nr 6 do PODO.
4. W sytuacjach szczególnych Administrator może w formie odrębnego aktu wewnętrznego takiego jak zarządzenie doprecyzować postanowienia PODO; doprecyzowanie to powinno być poprzedzone konsultacjami z IOD, a w sytuacji dotyczącej bezpośrednio systemu informatycznego także z ASI.

§ 6

1. Administrator wyznacza IOD o czym powiadamia Prezesa Urzędu Ochrony Danych Osobowych.
2. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych związane z realizacją jego zadań wynikających z RODO.
5. IOD wykonuje zadania w zakresie:
 - 1) informowania administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO, innych właściwych przepisów o ochronie danych osobowych, PODO i doradza im w tej sprawie; zadania te IOD realizuje w sposób uwzględniający „Zasady organizacji edukacji z zakresu ochrony danych osobowych” stanowiące załącznik nr 3 do PODO,
 - 2) monitorowania przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów; zadania te IOD realizuje w sposób uwzględniający zasady zawarte w Rozdziale XIV PODO „Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO”,

- 3) udzielania na żądanie zaleceń co do analizy ryzyka naruszenia praw i wolności osób fizycznych, a także oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 RODO,
- 4) współpracy z właściwym Organem Nadzorczym,
- 5) pełnienia funkcji punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
- 6) pełnienie funkcji punktu kontaktowego dla osób, których dane są przetwarzane na zasadach określonych w art. 38 ust. 4 RODO

§ 7

1. KKO są odpowiedzialni za zarządzanie procesami przetwarzania i ochrony danych osobowych w podległych komórkach organizacyjnych.
2. Do obowiązków KKO, w zakresie zarządzania procesami przetwarzania i ochrony danych osobowych, należy w szczególności:
 - 1) zarządzanie zasobem danych osobowych w ramach zadań, realizowanych przez podległą komórkę organizacyjną,
 - 2) nadzór nad ochroną danych osobowych w podległej komórce organizacyjnej,
 - 3) dopilnowanie, aby terminowo i zgodnie z właściwością, włączać IOD we wszystkie kwestie dotyczące ochrony danych osobowych związane z realizacją jego obowiązków,
 - 4) dopuszczanie do przetwarzania danych osobowych w podległej komórce organizacyjnej tylko osób posiadających stosowne upoważnienie do przetwarzania danych osobowych wydane przez Administratora i przedłożyły oświadczenie o poufności; informacje w tym zakresie uzyskuje z Wydziału Organizacyjnego Starostwa,
 - 5) występowanie z wnioskiem do ASI o nadanie, zmianę lub cofnięcie uprawnień do określonego zasobu danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych, w sposób określony w „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych”, stanowiącej załącznik nr 5 do PODO,
 - 6) realizacja zadań szkoleniowych i informacyjnych na zasadach określonych w „Zasadach organizacji edukacji z zakresu ochrony danych osobowych” stanowiących załącznik nr 3 do PODO,
 - 7) ustalanie w porozumieniu z ASI zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w podległej komórce organizacyjnej,

- 8) realizacja procesu udostępniania danych osobowych,
- 9) realizacja procesu związanego z zapewnieniem praw osobom, których dane dotyczą,
- 10) realizacja procesu powierzania czynności, związanych z przetwarzaniem danych osobowych innym podmiotom, w tym przygotowanie umów związanych z powierzeniem przetwarzania danych osobowych podmiotowi przetwarzającemu.
- 11) przedkładanie Administratorowi projektów umów związanych z powierzeniem danych osobowych w celu ich zatwierdzenia i podpisania, po wcześniejszym zatwierdzeniu przez IOD,
- 12) opracowywanie klauzul informacyjnych, oświadczeń zgody na przetwarzanie danych osobowych, które powinny być stosowane przy zbieraniu danych osobowych w podległej mu komórce organizacyjnej oraz odpowiadanie za ich stosowanie,
- 13) umożliwienie IOD przeprowadzenia czynności monitorujących określonych w RODO,
- 14) wykonywanie kopii zapasowych aplikacji i danych systemów informatycznych gromadzonych na dyskach lokalnych,
- 15) wykonywanie innych zadań zgodnie z zapisami PODO.

§ 8

1. Za zabezpieczenie techniczne danych osobowych przetwarzanych w systemie informatycznym odpowiada ASI.
2. Do zadań ASI należy w szczególności:
 - 1) zapewnienie wdrożenia wymaganych zabezpieczeń technicznych danych osobowych przetwarzanych w systemach informatycznych
 - 2) nadzór nad realizacją postanowień „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych”, stanowiącej załącznik nr 5 do PODO,
 - 3) nadzór nad właściwym funkcjonowaniem systemu informatycznego, w którym przetwarzane są dane osobowe,
 - 4) nadzór nad rozwiązywaniem sytuacji kryzysowych, pojawiających się w systemie informatycznym,
 - 5) przedkładanie do Administratora wniosków dotyczących propozycji zakupu oprogramowania lub sprzętu, w celu realizacji lub podniesienia poziomu bezpieczeństwa systemów informatycznych, bezpieczeństwa kopii zapasowych / bezpieczeństwa nośników pamięci/itp.
 - 6) dokumentowanie zdarzeń, powodujących naruszenia bezpieczeństwa danych osobowych oraz baz danych systemów informatycznych,

- 7) przekazywanie IOD informacji o nowych programach i systemach informatycznych, serwerach i innych zmianach systemu informatycznego, ważnych ze względu na realizację jego obowiązków, w szczególności prowadzenia rejestrów czynności,
- 8) zapewnienie, wspólnie z kierownikiem wydziału właściwego w sprawach technicznych, niezawodności awaryjnego zasilania serwerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,
- 9) udział w czynnościach związanych z monitorowaniem przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO, prowadzonych na zasadach określonych w Polityce,
- 10) podjęcie niezbędnych i odpowiednich do zagrożeń działań w zakresie zabezpieczenia systemów informatycznych w sytuacji naruszenia ochrony danych osobowych,
- 11) fizyczne nadawanie dostępu do systemu informatycznego osobom upoważnionym do przetwarzania danych osobowych,
- 12) usuwanie i modyfikacja uprawnień do dostępu do danych osobowych w systemie informatycznym,
- 13) ustalanie i kontrola identyfikatorów dostępu do systemu informatycznego,
- 14) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
- 15) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,
- 16) realizacja zadań, obejmujących procesy przetwarzania i archiwizowania danych oraz wspomaganie użytkowników w sytuacjach problemowych,
- 17) nadzór nad realizacją napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe,
- 18) wykonywanie kopii zapasowych aplikacji i danych systemów informatycznych gromadzonych na serwerze, zabezpieczenie ich przechowywania oraz okresowe ich sprawdzanie pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
- 19) wykonywanie innych czynności zgodnie z zapisami PODO, a także poleceń Administratora w zakresie ochrony, działań monitorujących i przetwarzania, dotyczących danych osobowych przetwarzanych w Starostwie Powiatowym w Nowym Tomyślu,

Rozdział V

Polecanie osobom przetwarzania danych osobowych

§ 9

1. Administrator jest upoważniony do przetwarzania wszelkich danych osobowych, występujących w zasobach Starostwa.
2. Administrator upoważnia osoby zatrudnione w Starostwie bez względu na charakter zatrudnienia, odbywające staż lub praktykę, realizujące zadania na podstawie umowy cywilnoprawnej, realizujące zadania w ramach prac w komisjach, zespołach, do przetwarzania danych osobowych w zakresie niezbędnym do realizacji zadań podczas wykonywanej pracy lub innych czynności.
3. Osoby, które nie zostały upoważnione do przetwarzania danych osobowych na zasadach określonych w PODO nie powinny przetwarzać danych osobowych.
4. Upoważnianie wskazanych osób do przetwarzania danych osobowych powinno być poprzedzone szkoleniem przeprowadzonym według zasad określonych w „Zasadach organizacji edukacji z zakresu ochrony danych osobowych” stanowiących załącznik nr 3 do PODO.
5. Upoważnienie do przetwarzania danych osobowych dla osób zatrudnionych w Starostwie bez względu na charakter zatrudnienia, odbywających staż lub praktykę, realizujących zadania na podstawie umowy cywilnoprawnej, poza sytuacjami szczególnymi określonymi przez Administratora, powinno mieć charakter pisemny; wzór takiego upoważnienia stanowi załącznik nr 7 do PODO.
6. Upoważnianie do przetwarzania danych osobowych osób realizujących zadania w ramach prac w komisjach, zespołach odbywa się w formie zarządzenia; akt ten opracowany przez właściwego KKO powinien wskazywać zakres oraz czasookres nadania i ustania upoważnienia do przetwarzania danych osobowych.
7. Administrator może pisemnie upoważnić inną osobę do nadawania i podpisywania upoważnień do przetwarzania danych osobowych, o których mowa w § 9 pkt. 5.
8. Upoważnienie do nadawania i podpisywania upoważnień do przetwarzania danych osobowych przygotowuje Wydział Organizacyjny; jego wzór stanowi załącznik nr 8 do PODO.
9. Upoważnienie do przetwarzania danych osobowych, o którym mowa w § 9 pkt. 5 przygotowuje IOD, po otrzymaniu wypełnionej „Informacji o przeprowadzeniu szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk”, której wzór określony został w załączniku nr 4 do PODO.
10. Osoby upoważnione do przetwarzania danych osobowych, wraz z nadaniem im upoważnienia do przetwarzania danych osobowych, składają na stanowisku właściwym w sprawach kadrowych oświadczenie osoby upoważnionej o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia; wzór oświadczenia stanowi załącznik nr 9 do PODO.

11. „Upoważnienia do przetwarzania danych osobowych”, „Upoważnienia do nadawania i podpisywania upoważnień” oraz oświadczenia, o których mowa w § 9 pkt. 10, przechowuje zgodnie z przepisami właściwymi w sprawach kancelaryjnych Wydział Organizacyjny.
12. Zasady postępowania przy nadaniu, modyfikacji lub anulowaniu uprawnień do przetwarzania danych osobowych w systemie informatycznym określone zostały w „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych”, stanowiącej załącznik nr 5 do PODO.
13. Upoważnienie do przetwarzania danych osobowych, jak również upoważnienie do nadawania i podpisywania upoważnień wygasa automatycznie wraz z ustaniem stosunku zatrudnienia, zakończeniem wykonywania prac, określonych umową cywilnoprawną / o staż / praktykę, a także obowiązków związanych z pracą w komisjach, zespołach, grupach roboczych.
14. Komórka ds. kadr informuje o zakończeniu stosunku zatrudnienia ASI oraz IOD.
15. Upoważnienia, o których mowa w § 9 pkt. 2, Administrator może cofnąć o każdym czasie, w szczególności na wniosek IOD, ASI lub KKO.

§ 10

1. Osoby, które nie przetwarzają danych osobowych ale w związku z realizacją swoich obowiązków znają zasady ich zabezpieczania, realizują swoje obowiązki w celu realizacji czynności związanych z zatrudnieniem lub zawartą umową cywilnoprawną; osoby te powinny złożyć na stanowisku właściwym w sprawach kadrowych oświadczenie zgodnie ze wzorem określonym w załączniku nr 9 do PODO; decyzję w tej sprawie podejmuje właściwy KKO.

§ 11

1. Strukturę organizacyjną związaną z polecaniem osobom przetwarzania danych osobowych przedstawiono w formie graficznej w załączniku nr 10 do PODO.

Rozdział VI

Polecenie przetwarzania danych osobowych podmiotowi przetwarzającemu

§ 12

1. Zlecenie jakichkolwiek czynności, związanych z przetwarzaniem danych osobowych podmiotom przetwarzającemu, jest formą powierzenia przetwarzania danych osobowych.
2. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje Administrator lub osoba przez niego upoważniona do zawierania umów.

3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy; wzór zapisów Staroście w zakresie ochrony danych osobowych stanowi załącznik nr 11 do PODO.
4. KKO przygotowuje projekt umowy, na podstawie której dochodzi do powierzenia przetwarzania danych osobowych.
5. KKO uzgadnia projekt umowy z właściwym radcą prawnym, a jeżeli powierzenie danych osobowych jest związane z przetwarzaniem danych w systemie informatycznym, takim jak: przesyła danych czy zdalne udostępnianie danych, także z ASI w zakresie zapisów dotyczących:
 - 1) udostępniania danych w systemie informatycznym,
 - 2) przesyłania danych drogą teletransmisji.
6. KKO przedkłada umowę do podpisu zgodnie z § 12 pkt. 2.
7. Kopia umowy powierzenia danych osobowych podmiotowi przetwarzającemu jest przedkładana IOD.

§ 13

1. W sytuacji gdy przedmiotem innej umowy, zawartej z podmiotem nie będącym podmiotem przetwarzającym, nie jest powierzenie przetwarzania danych osobowych, ale w celu realizacji przedmiotu umowy pracownicy tego podmiotu poznają sposoby ochrony danych osobowych w Starostwie, KKO przygotowujący umowę powinien zawrzeć w niej zapisy dotyczące ochrony danych osobowych, a następnie przed rozpoczęciem realizacji czynności przez tych pracowników aby odebrał od nich oświadczenia o poufności.

Rozdział VII

Zasady przetwarzania danych osobowych

§ 14

1. Dane osobowe w utworzonych zbiorach muszą być zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
2. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
3. Zabronione jest zbieranie wszelkich danych nieistotnych, nie mających znaczenia, o większym stopniu szczegółowości niż wynika to z określonego celu.
4. Zabronione jest przetwarzanie danych osobowych, dla których zakres, cel przetwarzania i sposoby przetwarzania nie został ustalony przez Administratora Danych, z wyjątkiem danych osobowych wynikających wprost z przepisów prawa.

5. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
6. Okres przechowywania może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.

§ 15

1. Dane osobowe w zbiorach danych osobowych mogą być przetwarzane po ich wcześniejszej rejestracji w „Rejestrze Czynności Przetwarzania Danych Osobowych Administratora” lub w „Rejestrze Czynności Przetwarzania Danych Osobowych Podmiotu Przetwarzającego”.
2. W celu dokonania rejestracji KKO zgłasza Administratorowi Danych zamiar przetwarzania nowych kategorii danych osobowych, utworzenia nowego zbioru, zasobów danych osobowych lub dokonania zmian w obrębie już przetwarzanych.
3. Zgłoszenie powinno zawierać w szczególności:
 - 1) kategorie osób, których dane dotyczą,
 - 2) kategorie danych osobowych (zakres danych osobowych),
 - 3) cel przetwarzania,
 - 4) kategorie ewentualnych odbiorców, którym dane osobowe byłyby ujawniane,
 - 5) planowane terminy usunięcia danych osobowych,
 - 6) opis technicznych i organizacyjnych środków bezpieczeństwa, w szczególności tych, o których mowa art. 32 ust. 1. RODO,
 - 7) nazwę i dane kontaktowe ewentualnych współadministratorów
 - 8) jeśli ma to zastosowanie - dane, o których mowa w art. 30 ust. 1 lit. e) RODO.
4. Administrator, w przypadku wątpliwości może żądać opinii IOD w tej sprawie.
5. W sytuacji akceptacji Administratora na rozpoczęcie przetwarzania zgodnie z zamiarem, o którym mowa w § 15 pkt. 2, KKO jest zobowiązany przedstawić zgłoszenie IOD celem dokonania stosownych wpisów w rejestrach czynności Administratora lub Podmiotu Przetwarzającego.

Rozdział VIII

Zgodność przetwarzania z prawem

§ 16

1. W sytuacji gdy podstawą prawną przetwarzania danych osobowych nie będzie żaden z zapisów art. 6 ust. 1 lit. b),c),d),e) RODO przetwarzanie jest możliwe na podstawie zgody na przetwarzanie danych osobowych wyrażonej przez osobę, której dane dotyczą.

2. Zgoda na przetwarzanie danych osobowych powinna być odbierana w formie pisemnego oświadczenia osoby, której dane dotyczą; wzór oświadczenia stanowi załącznik nr 13 do PODO.
3. Zgoda na przetwarzanie danych osobowych, która jest częścią składową kwestionariuszy, formularzy, itp., powinna być odebrana (podpisana) odrębnie.
4. Zapisy § 17 pkt. 2,3,4 stosuje się odpowiednio do oświadczeń zgody na przetwarzanie danych osobowych.
5. W sytuacjach szczególnych, określonych przez Administratora, zgoda może być odebrana w formie jednoznacznego, wyraźnego działania.

Rozdział IX

Realizacja obowiązków informacyjnych

§ 17

1. W przypadku zbierania danych osobowych bezpośrednio od osób - na formularzach, kwestionariuszach, drukach i innych służących do zbierania danych osobowych – prowadzonych zarówno w formie papierowej, jak i elektronicznej, należy umieszczać na nich klauzulę informacyjną; wzór klauzuli stanowi załącznik nr 12 do PODO.
2. KKO opracowuje klauzule informacyjne, które powinny być stosowane przy zbieraniu danych osobowych w podległej mu komórce organizacyjnej.
3. W przypadku wątpliwości związanych ze stosowaniem i opracowaniem klauzuli Administrator może zażądać opinii IOD.
4. KKO odpowiada za stosowanie klauzul informacyjnych.

§ 18

1. W przypadku pozyskiwania danych osobowych w inny sposób niż od osoby, której dane osobowe dotyczą, Administrator jest zobowiązany realizować obowiązek informacyjny w stosunku do tych osób w sposób określony w art. 14 RODO.
2. Zapisy § 17 pkt. 2,3,4 stosuje się odpowiednio.

Rozdział X

Prawa osoby, której dane osobowe dotyczą

§ 19

1. Zasady i warunki korzystania z praw osoby, której dane osobowe dotyczą określone zostały w Rozdziale III RODO: „Prawa osoby, której dane dotyczą”.
2. Wnioski w sprawie skorzystania z praw osoby, której dane osobowe dotyczą rozpatruje i realizuje właściwy KKO; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, a w szczególności w sytuacji wątpliwości co do odpowiedzi odmownej lub udostępniania danych, KKO na polecenie administratora może zasięgnąć opinii IOD.
3. W celu ułatwienia korzystania z praw przez osobę, której dane dotyczą Administrator umożliwia jej kontakt z IOD poprzez umieszczeniu adresu mailowego do niego na stronie internetowej Starostwa.
4. W przypadku skontaktowania się osoby, której dane dotyczą bezpośrednio z IOD, Administrator lub wskazani przez niego KKO są zobowiązani niezwłocznie udzielić mu wszelkiej możliwej pomocy i informacji w celu rozwiązania problemu oraz do spowodowania aby osoba, która się do niego zwróciła mogła skorzystać ze swoich praw.
5. Informacja o osobie, której dane dotyczą powinna być przekazana w ciągu 1 miesiąca z możliwością przedłużenia jej przekazania o kolejne 2 miesiące jeżeli wniosek / żądanie ma skomplikowany charakter.

§ 20

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
 - 1) na podstawie przepisów prawa organom publicznym w ramach konkretnego postępowania,
 - 2) na podstawie wniosku od podmiotu uprawnionego do otrzymania danych na podstawie przepisów prawa,
 - 3) na podstawie umowy z odbiorcą danych lub współadministratorem danych, w ramach której istnieje konieczność udostępnienia danych.
2. Proces udostępniania danych osobowych rozpatruje i realizuje właściwy KKO; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, KKO na polecenie Administratora może zasięgnąć opinii IOD.
3. Informacje zawierające dane osobowe, przekazywane są uprawnionym podmiotom lub osobom, za potwierdzeniem odbioru, w następujący sposób:
 - 1) pocztą kurierską,
 - 2) listem poleconym za pokwitowaniem odbioru,
 - 3) za pomocą teletransmisji danych,
 - 4) osobiście za potwierdzeniem odbioru.
 - 5) w inny, określony konkretnym wymogiem prawnym lub umową, sposób.
4. Osoby przetwarzające dane osobowe zachowują szczególną ostrożność przy przekazywaniu danych osobowych drogą telefoniczną; przekazanie tą drogą może

nastąpić tylko w sytuacji pełnej pewności co do tożsamości osoby, której dane są przekazywane.

Rozdział XI

Obszar przetwarzania danych osobowych

§ 21

1. Obszarem przetwarzania danych osobowych w Starostwie są budynki, pomieszczenia lub części pomieszczeń, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym, zlokalizowane:
 - 1) w siedzibie w Nowym Tomyślu, ul. Poznańska 33
 - 2) w komórkach organizacyjnych zorganizowanych poza tą siedzibą.
2. Przebywanie wewnątrz obszaru przetwarzania danych osobowych, osób nieuprawnionych do dostępu do danych osobowych - jest dopuszczalne za zgodą Administratora lub w obecności osoby dopuszczonej do przetwarzania tych danych lub za zgodą KKO.
3. Pracownicy firm zewnętrznych, przebywający wewnątrz obszaru przetwarzania danych osobowych poza godzinami pracy lub bez obecności osoby dopuszczonej do przetwarzania danych powinny podpisać oświadczenia, zgodnie z załącznikiem nr 9 do PODO i powinny one być dołączone do umów z tymi firmami.
4. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

§ 22

1. W sytuacji konieczności przetwarzania danych osobowych, poza obszarem wymienionym w § 20 pkt. 1 PODO, zgodę na takie działania wydaje Administrator. O zgodę do Administratora występuje KKO.
2. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
3. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada osoba dokonująca ich wyniesienia.
4. W przypadku druku materiałów zawierających dane osobowe poza miejscem pracy pracownik odpowiada za dołożenie należytej staranności, aby druk nie został udostępniony innym pracownikom lub klientom Starostwa.

Rozdział XII

Przetwarzanie danych osobowych w systemie informatycznym i na nośnikach papierowych

§ 23

1. Zasady zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, określa dokument „Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych”, stanowiąca załącznik nr 5 do PODO,

§ 24

1. Dane osobowe, zawarte w dokumentacji papierowej, mogą być przetwarzane jedynie przez osoby upoważnione do przetwarzania danych osobowych zgodnie z zasadami określonymi w PODO.
2. Kopie papierowe z danymi osobowymi muszą być przechowywane w zamykanych na klucz szafach, szufladach lub sejfach; obowiązuje tzw. „zasada czystego biurka”.
3. Dopuszcza się przechowywanie danych osobowych w niezamykanych szafach lub regałach tylko w pomieszczeniu archiwum zabezpieczonym zgodnie z odrębnymi przepisami.
4. Niszczenie dokumentów papierowych powinno przebiegać z wykorzystaniem specjalnych urządzeń do wykonywania tych czynności takich jak niszczarki.
5. Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, określają przepisy kancelaryjne Starostwa. W zakresie nieuregulowanym przepisami kancelaryjnymi Starostwa, odpowiednie zasady określa KKO po konsultacji z Administratorem; w sytuacjach szczególnych mogą w tej sprawie zasięgnąć porady IOD.

Rozdział XIII

Postępowanie w sytuacji naruszenia ochrony danych osobowych

§ 25

1. W sytuacji naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych należy postępować zgodnie z regułami opisanymi w „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych”, której wzór stanowi załącznik nr 14 do PODO.

Rozdział XIV
Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie
danych osobowych oraz PODO

§ 26

1. Działania związane z monitorowaniem przestrzegania przepisów w zakresie ochrony danych osobowych obejmują działania planowe i pozaplanowe; do działań planowych zalicza się w szczególności działania audytowe i kontrolne, ocenę ochrony przetwarzania danych osobowych prowadzoną na podstawie informacji uzyskanych od Administratora w zakresie ustalonym przez IOD; działania pozaplanowe wynikają z zakresu obowiązków IOD.
2. IOD przygotowuje Plan Działań Związanych z Monitorowaniem Przestrzegania Przepisów w Zakresie Ochrony Danych Osobowych.
3. W trakcie realizacji działań monitorujących, w tym audytów IOD może dokumentować swoje czynności:
 - a) notatką z podjętych czynności,
 - b) protokołem odebrania ustnych wyjaśnień,
 - c) innymi sposobami, w tym informacjami zebranymi na piśmie lub drogą elektroniczną.
4. Z przeprowadzonych czynności monitorujących IOD przekazuje informację wraz z wnioskami Administratorowi; w przypadku działań audytowych IOD sporządza „Sprawozdanie z działań planowych/pozaplanowych związanych z monitorowaniem/naruszeniem przestrzegania przepisów w zakresie ochrony danych osobowych”.

Ocena ryzyka naruszenia praw lub wolności osób fizycznych

§ 27

1. Zasady oceny ryzyka naruszenia praw lub wolności osób fizycznych określa dokument „Arkusz szacowania ryzyka naruszenia praw lub wolności osób fizycznych” stanowiący załącznik nr 15 do PODO.
2. Ocenę skutków dla ochrony danych osobowych prowadzi się w sytuacjach i na zasadach określonych w art. 35 RODO.

Rozdział XVI

Odpowiedzialność karna

§ 28

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w uodo oraz w art. 130, 266 - 269, 287 Kodeksu Karnego.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w § 28 pkt 1, naruszenie zasad ochrony danych osobowych, obowiązujących w Starostwie, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Rozdział XVII

Postanowienia końcowe

§ 29

1. Polityka wchodzi w życie z dniem 11.10.2018 r.