POWIATOWE CENTRUM
USŁUG WSPÓLNYCH
w Nowym Tomyślu
ul. Poznańska 33, 64-300 Nowy Tomyśl

Zarządzenie Nr 4/2023
Dyrektora Powiatowego Centrum Usług Wspólnych w Nowym Tomyślu
z dnia 6 września 2023 r.

w sprawie wprowadzenia Polityki ochrony danych osobowych w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu

Na podstawie § 8 ust. 2 Regulaminu Organizacyjnego Powiatowego Centrum Usług Wspólnych w Nowym Tomyślu stanowiącego załącznik do uchwały nr 54/EK/2019 Zarządu Powiatu Nowotomyskiego z dnia 19 lutego 2019 r. oraz na podstawie art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2018 r.) zarządzam, co następuje:

§1. Wprowadza się w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu „Politykę ochrony danych osobowych", stanowiącą załącznik do niniejszego zarządzenia.

§2. Wszyscy pracownicy Powiatowego Centrum Usług Wspólnych w Nowym Tomyślu w Nowym Tomyślu zobowiązani są zapoznać się z treścią „Polityki ochrony danych osobowych".

§3. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Powiatowego Centrum Usług Wspólnych
w Nowym Tomyślu
Marek Nyćkowiak

Zatwierdzam pod względem formalnoprawnym
radca prawny Wojciech Lignowski

Załącznik
do zarządzenia nr 4/2023
Dyrektora Powiatowego Centrum
Usług Wspólnych w Nowym Tomyślu
z dnia 6 września 2023 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

W POWIATOWYM CENTRUM USŁUG WSPÓLNYCH W NOWYM TOMYŚLU

Zatwierdzam:

Data i miejsce sporządzenia dokumentu	2023
Data aktualizacji dokumentu	
Wydanie:	Pierwsze
Opracowała:	Marlena Galas

Spis treści

Spis załączników

Rozdział I
Postanowienia ogólne

§ 1

Polityka Ochrony Danych Osobowych określa zasady w zakresie zarządzania procesami przetwarzania danych osobowych oraz ich bezpieczeństwem w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu.

§ 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 oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

Rozdział II
Słownik pojęć

§ 3

Występujące w Polityce Ochrony Danych Osobowych zwroty oznaczają:

Administrator Danych Osobowych - ADO – Dyrektor Powiatowego Centrum Usług Wspólnych w Nowym Tomyślu;

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

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

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, 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 PCUW, zwana dalej także Polityką;

przetwarzanie danych osobowych – 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 PCUW, 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 2019r. poz. 1781),

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 PCUW w celu realizacji zadań;

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;

PCUW – Powiatowe Centrum Usług Wspólnych w Nowym Tomyślu

Rozdział III
Zakres stosowania Polityki i zakres przetwarzania

§ 4

1. Polityka ma zastosowanie do:
   1) danych osobowych przetwarzanych w PCUW 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. Zasady i procedury określone w niniejszym zarządzeniu stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych jak i przetwarzanych w systemach informatycznych.

3. Zasady i procedury określone w niniejszym dokumencie stosuje się do wszystkich przetwarzających dane osobowe w PCUW w szczególności do pracowników i innych osób, które zostały dopuszczone do przetwarzania, np. stażyści, praktykanci itd.
4. W PCUW 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 Kategorii 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.
5. W PCUW 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 PCUW jest Dyrektor PCUW w Nowym Tomyślu.
2. Administrator jest odpowiedzialny za przetwarzanie i ochronę danych osobowych w PCUW.
3. Strukturę zarządzania przetwarzaniem danych osobowych oraz ich bezpieczeństwem przedstawia graficznie załącznik nr 3 do PODO.

§ 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.
3. 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, zadania te IOD realizuje w sposób uwzględniający „Zasady organizacji edukacji z zakresu ochrony danych osobowych" stanowiące załącznik nr 4 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. Za zabezpieczenie techniczne danych osobowych przetwarzanych w systemie informatycznym odpowiada ASI.
2. Do zdań 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) dokumentowanie zdarzeń, powodujących naruszenia bezpieczeństwa danych osobowych oraz baz danych systemów informatycznych,

6) przekazywanie IOD informacji o nowych programach i systemach informatycznych, serwerach i innych zmianach systemu informatycznego, ważnych ze względu na realizacje jego obowiązków, w szczególności prowadzenia rejestrów czynności,

7) udział w czynnościach związanych z monitorowaniem przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO, prowadzonych na zasadach określonych w Polityce,

8) podjęcie niezbędnych i odpowiednich do zagrożeń działań w zakresie zabezpieczenia systemów informatycznych w sytuacji naruszenia ochrony danych osobowych,

9) fizyczne nadawanie dostępu do systemu informatycznego osobom upoważnionym do przetwarzania danych osobowych,

10) usuwanie i modyfikacja uprawnień do dostępu do danych osobowych w systemie informatycznym,

11) ustalanie i kontrola identyfikatorów dostępu do systemu informatycznego,

12) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

13) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,

14) realizacja zadań, obejmujących procesy przetwarzania i archiwizowania danych oraz wspomaganie użytkowników w sytuacjach problemowych,

15) nadzór nad realizacją napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe,

16) 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,

17) wykonywanie innych czynności zgodnie z zapisami PODO, a także poleceń Administratora w zakresie ochrony, działań monitorujących i przetwarzania, dotyczących danych osobowych przetwarzanych w PCUW w Nowym Tomyślu.

Rozdział V

Polecanie osobom przetwarzania danych osobowych

§ 8

1. Administrator jest upoważniony do przetwarzania wszelkich danych osobowych, występujących w zasobach PCUW.
2. Administrator upoważnia osoby zatrudnione w PCUW 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 4 do PODO.
5. Upoważnienie do przetwarzania danych osobowych dla osób zatrudnionych w PCUW 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. Upoważnienie do przetwarzania danych osobowych, o którym mowa w § 8 pkt. 5 przygotowuje IOD, po wypełnieniu „Informacji o przeprowadzeniu szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk", której wzór określony został w załączniku nr 6 do PODO.
7. Osoby upoważnione do przetwarzania danych osobowych, wraz z nadaniem im upoważnienia do przetwarzania danych osobowych, składają na stanowisku ds. kadr oświadczenie osoby upoważnionej o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia; wzór oświadczenia stanowi załącznik nr 8 do PODO.
8. „Upoważnienia do przetwarzania danych osobowych" oraz oświadczenia, o których mowa w § 8 pkt. 7, przechowuje zgodnie z przepisami właściwymi w sprawach kancelaryjnych pracownik ds. kadr w PCUW.
9. 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.

10. Upoważnienie do przetwarzania danych osobowych 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.
11. Pracownik ds. kadr informuje o zakończeniu stosunku zatrudnienia ASI oraz IOD.
12. Upoważnienia, o których mowa w § 8 pkt. 2, Administrator może cofnąć o każdym czasie, w szczególności na wniosek IOD, ASI.

§ 9

Rozdział VI
Polecenie przetwarzania danych osobowych podmiotowi przetwarzającemu

1. Zlecanie 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 stanowi załącznik nr 9 do PODO.
4. Pracownik PCUW przygotowuje projekt umowy, na podstawie której dochodzi do powierzenia przetwarzania danych osobowych.
5. Pracownik PCUW uzgadnia projekt umowy z właściwym radcą prawnym, a jeżeli powierzenie danych osobowych jest związane z przetwarzaniem danych w systemie informatycznym, takim jak: przesyłanie danych czy zdalne udostępnianie danych, także z ASI w zakresie zapisów dotyczących:
   1) udostępniania danych w systemie informatycznym,
   2) przesyłania danych drogą teletransmisji.
6. Pracownik PCUW przedkłada umowę do podpisu zgodnie z § 9 pkt. 2.
7. Kopia umowy powierzenia danych osobowych podmiotowi przetwarzającemu jest przedkładana IOD.
8. 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 PCUW, pracownik PCUW 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

§ 10

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.

§ 11

1. Dane osobowe mogą być przetwarzane po ich wcześniejszej rejestracji w „Rejestrze Czynności Przetwarzania Danych Osobowych „ lub w „Rejestrze Kategorii Czynności Przetwarzania Danych Osobowych".
2. W celu dokonania rejestracji pracownik PCUW 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) cel przetwarzania,
   2) kategorie osób, których dane dotyczą,
   3) kategorie danych osobowych (zakres danych osobowych),
   4) kategorie ewentualnych odbiorców, którym dane osobowe byłyby ujawniane,
   5) zgodność przetwarzania z prawem (podstawa prawna),

6) planowane terminy usunięcia danych osobowych,
7) opis technicznych i organizacyjnych środków bezpieczeństwa, w szczególności tych, o których mowa art. 32 ust. 1. RODO, ogólny opis środków bezpieczeństwa,
8) nazwę i dane kontaktowe ewentualnych współadministratorów,
9) jeśli ma to zastosowanie - dane, o których mowa w art. 30 ust. 1 lit. e) RODO.(transfer do kraju trzeciego),
10) nazwa i dane kontaktowe administratora,
11) czas trwania przetwarzania,
12) nazwa systemu lub użyte oprogramowanie.

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 § 11 pkt. 2, pracownik PCUW jest zobowiązany przedstawić zgłoszenie IOD celem dokonania stosownych wpisów w rejestrach.

Rozdział VIII

Zgodność przetwarzania z prawem

§ 12

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 10 do PODO.
3. Zgoda na przetwarzanie danych osobowych, która jest częścią składową kwestionariuszy, formularzy, itp., powinna być odebrana (podpisana) odrębnie.
4. Zapisy § 12 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

§ 13

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 11 do PODO.
2. Pracownik PCUW opracowuje klauzule informacyjne, które powinny być stosowane przy zbieraniu danych osobowych.
3. W przypadku wątpliwości związanych ze stosowaniem i opracowaniem klauzuli Administrator może zażądać opinii IOD.
4. Pracownik PCUW odpowiada za stosowanie klauzul informacyjnych.

§ 14

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. 13 RODO.

2. Zapisy § 13 pkt. 2,3,4 stosuje się odpowiednio.

Rozdział X

Prawa osoby, której dane osobowe dotyczą

§ 15

1. Zasady i warunki korzystania z praw osoby, której dane osobowe dotyczą określone zostały w Rozdziale III RODO: „Prawa osoby, której dane dotyczą".
2. Procedury realizacji praw osób:
    1) Obowiązki informacyjne:
    a) obowiązki informacyjne- prawo do bycia poinformowanym o przetwarzaniu danych przy zbieraniu danych od osoby, której dane dotyczą,

b) prawo do bycia poinformowanym o przetwarzaniu danych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą,

2) Prawa realizowane na wniosek:

b) Prawo dostępu do danych osobowych przysługuje osobie, której dane dotyczą,

c) Prawo do sprostowania, uzupełnienia danych,

d) Prawo do usunięcia danych (prawo do bycia zapomnianym),

e) Prawo do ograniczenia przetwarzania,

f) Prawo do powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania,

g) Prawo do przenoszenia danych,

h) Prawo do sprzeciwu,

i) Prawo do niepodlegania decyzji w oparciu o zautomatyzowane przetwarzane danych w tym profilowanie,

j) Prawo do poinformowania o naruszeniach.

3. Wnioski w sprawie skorzystania z praw osoby, której dane osobowe dotyczą rozpatruje i realizuje pracownik PCUW; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, a w szczególności w sytuacji wątpliwości co odpowiedzi odmownej lub udostępniania danych, pracownik PCUW na polecenie administratora może zasięgnąć opinii IOD.
4. 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 PCUW.
5. W przypadku skontaktowania się osoby, której dane dotyczą bezpośrednio z IOD, Administrator lub wskazani przez niego pracownicy PCUW 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.
6. 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.
7. Po załatwieniu sprawy wniosek i odpowiedź zostaje przekazana do IOD.
8. Rejestr wszystkich wniosków prowadzi IOD.

9. Co do zasady realizacja żądań wyżej wymienionych wynikających z art. 15-21 RODO są wolne od opłat.
10. Jeżeli okaże się, że żądania osoby są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator może pobrać od osoby rozsądną opłatę uwzględniając administracyjne koszty udzielania informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań.
11. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter spoczywa na Administratorze.

§ 16

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 pracownik PCUW; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, pracownik PCUW 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

§ 17

1. Obszarem przetwarzania danych osobowych zarówno w formie papierowej, jak i w systemie informatycznym w PCUW są pomieszczenia lub części pomieszczeń, zlokalizowane w siedzibie w Nowym Tomyślu, ul. Poznańska 33.
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.
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 8 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.

§ 18

1. W sytuacji konieczności przetwarzania danych osobowych, poza obszarem wymienionym w § 17 pkt. 1 PODO, zgodę na takie działania wydaje Administrator. O zgodę do Administratora występuje pracownik PCUW.
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 PCUW.

Rozdział XII

Przetwarzanie danych osobowych w systemie informatycznym i na nośnikach papierowych

§ 19

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,

§ 20

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", tzn. że po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do szafy zamykanej na klucz. Po zakończonej pracy pracownik może pozostawić na biurku jedynie telefon oraz materiały biurowe takie jak np. długopis i zszywacz.
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. Dokumenty powinny być niszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji.
5. Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, określają przepisy kancelaryjne PCUW.

Rozdział XIII

Postępowanie w sytuacji naruszenia ochrony danych osobowych

§ 21

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 12 do PODO.

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

§ 22

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. 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.
3. 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".

Rozdział XV
Ocena ryzyka naruszenia praw lub wolności osób fizycznych

§ 23

1. Zasady oceny ryzyka naruszenia praw lub wolności osób fizycznych określa dokument „Arkusz szacowania ryzyka naruszenia praw lub wolności osób fizycznych" stanowiący załącznik nr 13 do PODO.
2. Ocenę skutków dla ochrony danych osobowych prowadzi się w sytuacjach i na zasadach określonych w art. 35 RODO.

§ 24
Bezpieczeństwo danych oraz zarządzanie ryzykiem

1. W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem Administrator dokonuje oszacowania ryzyka właściwego dla przetwarzania oraz wdraża środki minimalizujące to ryzyko. Środki takie powinny

zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, bierze się pod uwagę ryzyko związane z przetwarzaniem danych osobowych - takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych - i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych PCUW przeprowadza co najmniej raz w roku:
   a) analizę ryzyka dla czynności przetwarzania danych;
   b) przeprowadza ocenę skutków dla ochrony danych tam gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
4. Analizę ryzyka przeprowadza IOD. Wyniki analizy ryzyka przedstawiane są każdorazowo Administratorowi.
5. Do oszacowania ryzyka w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych w PCUW stosowany jest rejestr ryzyka wg wzoru stanowiącego załącznik nr 13 do niniejszej polityki.

§ 25
Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych (wystąpieniu zdarzenia stanowiącego incydent naruszenia obowiązujących procedur wew.) sprawca incydentu lub inna osoba posiadająca informacje o wystąpieniu incydentu, przekazuje Administratorowi informacje najpóźniej z przeciągu 24 godzin.
2. Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
3. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi.
4. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

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

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu.
6. IOD lub Administrator zobowiązani są zaistniały incydent wpisać do rejestru naruszeń danych osobowych PCUW (załącznik nr 12 do niniejszej polityki).

§26

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.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) rozporządzenia.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

d) Jeżeli Administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

§ 27

Opis zdarzeń naruszających ochronę danych osobowych

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
2) zagrożenia losowe wewnętrzne – (np. niezamierzone pomyłki administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenia ciągłości pracy), zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);
   - nieuprawniony dostęp do systemu z jego wnętrza;
   - nieuprawniony przekaz danych;
   - pogorszenie jakości sprzętu i oprogramowania rozumiane m.in. jako brak wsparcia technicznego producenta oprogramowania;
   - bezpośrednie zagrożenie materialnych składników systemu.

§ 28

Procedury postępowania w sytuacjach naruszenia ochrony danych osobowych

Niniejsze procedury wew. określają tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzenia i przetwarzanych zarówno w zbiorach tradycyjnych jak i informatycznych. Poniższe procedury wew. stosuje się w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe. Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych przetwarzanie danych oraz usuwanie danych osobowych.

1. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę przetwarzanych danych osobowych w PCUW i ich zabezpieczeń są:
   a) Administrator,
   b) Inspektor Ochrony Danych (IOD),
   c) Administrator Systemu Informatycznego (ASI),
   d) pracownicy PCUW upoważnieni do przetwarzania danych osobowych.
2. Każdy pracownik PCUW biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania IOD oraz Administratora Danych Osobowych lub innej osoby wskazanej przez niego.
3. Każda osoba zatrudniona w PCUW, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) powinna niezwłocznie poinformować o tym fakcie Administratora lub IOD.
4. Do czasu przybycia Administratora lub IOD należy:
   a) niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   b) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,
   c) wstrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony, oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
   d) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
   e) nie zmieniać położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
   f) podjąć stosowne do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
   g) podjąć inne działania przewidziane w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   h) wstępnie udokumentować zaistniałe naruszenie,
   i) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub osoby upoważnionej.
5. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych IOD lub Administrator powinni:
   a) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy PCUW,

b) zaprotokołować wszelkie informacje związane ze zdarzeniem,
c) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
d) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych niepowołanych,
e) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,
f) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.
g) dokonać zmiany haseł na wszystkich kontach użytkowników.
h) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

6. IOD dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych w zdarzenie,
   b) określenie czasu, miejsca naruszenia i powiadomienia,
   c) określenie okoliczności towarzyszących i rodzaj naruszenia,
   d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
7. Raport, o którym mowa w pkt. 5, IOD przekazuje niezwłocznie Administratorowi.
8. IOD przy współpracy Administratorem Systemów Informatycznych przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:
   - przeprowadzenie naprawy sprzętu informatycznego;
   - rekonfigurację sprzętu informatycznego;
   - wprowadzenie poprawek do oprogramowania;
   - rekonfiguracje oprogramowania;
   - odtworzenie danych z kopii awaryjnych;
   - modyfikacje danych w celu odtworzenia ich integralności;
   - wycofanie z użycia materiału kryptograficznego;

9. Inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagającej lub zabezpieczając
10. ych działanie systemu informatycznego.

Rozdział XVI

Procedura retencji danych

§ 29

1. Poprzez retencje danych rozumie się ustalenie celu oraz okresu przechowywania zebranych danych osobowych.
2. Pracownik merytoryczny, który przetwarza dane osobowe zobowiązany jest:
   a) dokonać inwentaryzacji przetwarzania danych osobowych w konkretnych procesach,
   b) sprawdzić miejsce przechowywania danych,
   c) określić cel, dla którego dane zostały zebrane,
   d) określić czas przechowywania danych poprzez analizę przepisów szczegółowych, z których wynika okres przechowywania danych, a jeżeli taki okres nie jest podany, ustalić kryteria ustalenia okresu.
3. Ustalając okres retencji należy wziąć pod uwagę obecną i przyszła wartość informacji, koszty, ryzyko i zobowiązania związane z przetwarzaniem danych, a także realną możliwość zapewnienia, by dane były aktualne.
4. Po ustaniu okresu przechowywania, dane podlegają usunięciu, gdy:
   a) minął okres ich przydatności,
   b) okaże się, że cel dla którego dane zostały zebrane został osiągnięty.

Rozdział XVII

Odpowiedzialność karna

§ 30

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 PCUW, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

DYREKTOR
Powiatowego Centrum Usług Wspólnych
w Nowym Tomyślu
Marek Nyckowiak

Załącznik Nr 1
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Nazwa Administratora	
Dane kontaktowe	
Imię i nazwisko Inspektora Ochrony Danych	

LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontaktowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

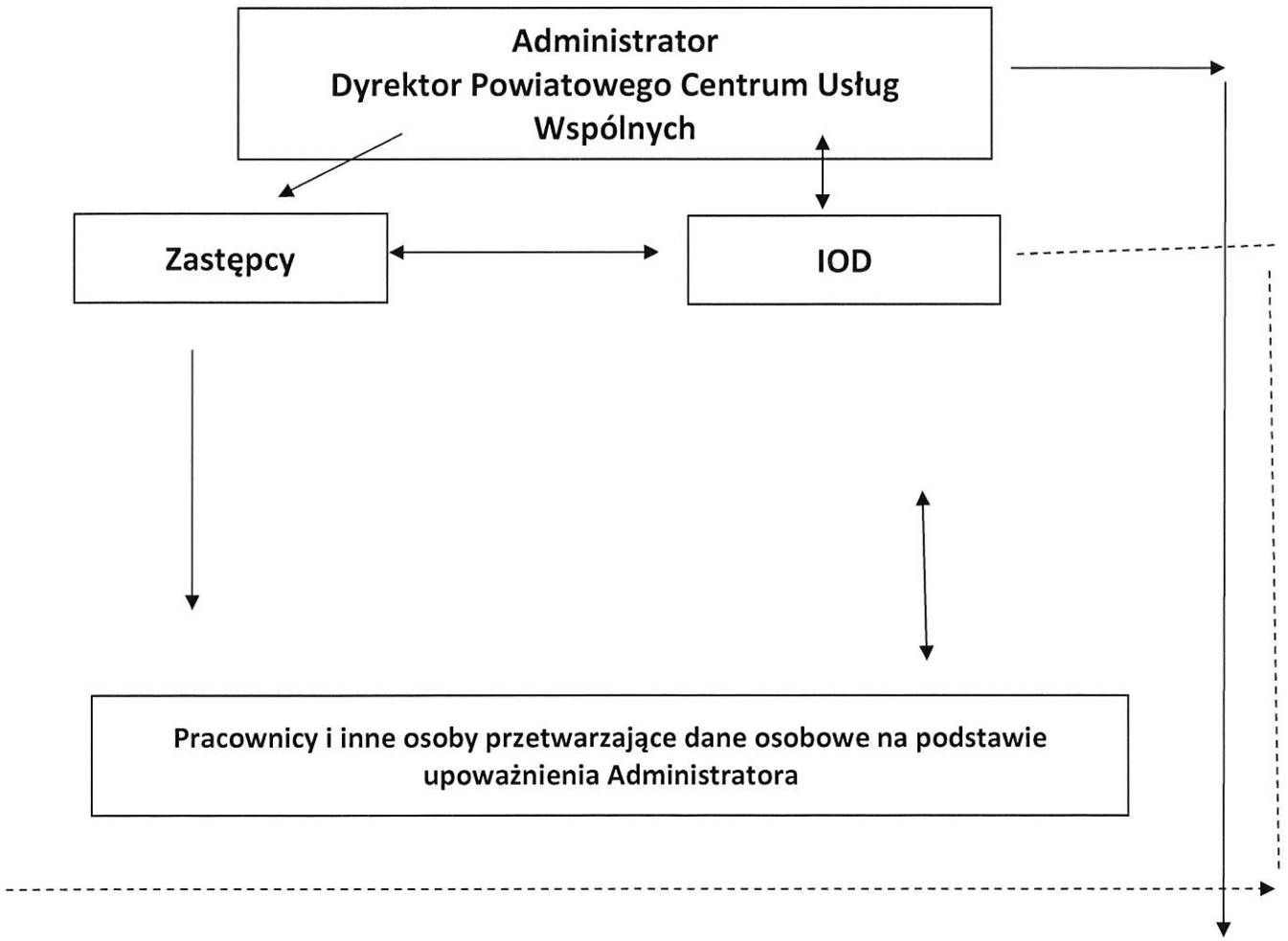
Załącznik Nr 2
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

WZÓR REJESTRU KATEGORII CZYNNOŚCI PRZETWARZANIA

Lp	Kategoria przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Administrator				Czas trwania przetwarzania	Nazwa państw trzecich lub organizacji międzynarodowych do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art.49 ust. 1 akapit drugi	Użyte oprogramowanie	Podprzetwarzajacy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora	Przedstawiciel Administratora	IOD					Nazwa i dane kontaktowe podwykonawcy	Kategorie podpowierzonych przetwarzań
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art.32 ust. 1	Art. 30 ust. 2 lit. a					Art. 30 ust. 2 lit. c	Art.30 ust. 2 lit. c			
1	2	3	4	5	6	7	8	9	10	11	12	13

Załącznik Nr 3
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

Struktura zarządzania przetwarzaniem danych osobowych oraz ich bezpieczeństwem



Załącznik Nr 4
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

Zasady organizacji edukacji z zakresu ochrony danych osobowych

1. Celami działań edukacyjnych jest zapoznanie osób przetwarzających dane osobowe w Powiatowym Centrum Usług Wspólnych z regulacjami prawnymi w zakresie ochrony danych osobowych i zasadami bezpiecznego przetwarzania danych osobowych w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu.
2. Wyróżnia się następujące rodzaje działań edukacyjnych:
   a) szkolenie przed przystąpieniem do pracy/służby/stażu/praktyk,
   b) informowanie o zmianach w zakresie ochrony danych osobowych,
   c) szkolenie fakultatywne.
3. Zasady organizacji szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk:
   a) szkolenie powinno być przeprowadzone dla osób, które będą przetwarzały dane osobowe, przed rozpoczęciem pracy/służby/stażu/praktyk w PCUW polegającej na przetwarzaniu danych osobowych,
   b) celem szkolenia jest zapoznanie tych osób z regulacjami prawnymi w zakresie ochrony danych osobowych, w tym regulacjami wewnątrzzakładowymi z zakresu ochrony danych osobowych obowiązującymi na terenie PCUW,
   c) organizacja i przeprowadzenie szkolenia dla pracowników, stażystów i praktykantów jest obowiązkiem IOD, za wyjątkiem określonym w lit. d), e)
   d) Administrator może także nakazać w innych sytuacjach, do których zalicza się także wprowadzenie nowych regulacji z zakresu ochrony danych osobowych dla całego PCUW, zorganizowane szkolenia w formie samokształcenia kierowanego z wykorzystaniem narzędzi internetowych,
   e) czas szkolenia powinien zapewniać realizację celu przy uwzględnieniu doświadczenia uczestnika szkolenia w zakresie ochrony danych osobowych,
   f) szkolenie dokumentuje się poprzez wystawienie „Informacji o przeprowadzeniu szkolenia" stanowiącej załącznik nr 6 do PODO,
   g) przygotowaniem i przechowywaniem „Informacji o przeprowadzeniu szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk" w aktach osobowych wraz z upoważnieniem do przetwarzania danych osobowych, zajmuje się pracownik d/s kadrowych.
4. Zasady organizacji instruktażu stanowiskowego w zakresie ochrony danych osobowych:
   a) szkolenie powinno być przeprowadzone dla:
      — osób, które będą przetwarzały dane osobowe, przed dopuszczeniem do wykonywania tej pracy/służby/stażu/praktyk w PCUW,
      — osób, które już przetwarzały dane osobowe w PCUW, ale obecnie zmieniają się przy ich pracy warunki jej wykonywania, związane z ochroną danych osobowych,
   b) celem szkolenia jest zapoznanie osób, które będą przetwarzały dane osobowe, z zasadami ochrony danych osobowych na danym stanowisku pracy,

c) czas szkolenia należy dostosować do warunków ochrony danych osobowych na stanowisku pracy oraz doświadczenia osób w zakresie ochrony danych osobowych.

5. Zasady informowania o zmianach w zakresie ochrony danych osobowych:
   a) informowanie o zmianach w zakresie ochrony danych osobowych jest obowiązkiem:
      — IOD w stosunku do Administratora,
      — IOD w stosunku do pracowników,
   b) poinformowanie może być prowadzone w formie instruktażu, wykładu, samokształcenia z wykorzystaniem informacji przesłanej drogą elektroniczną lub informacji w formie papierowej, informacji ustnej,
   c) celem przekazania informacji jest jak najszybsze zapoznanie osób, które przetwarzają dane osobowe, z zmienionymi przepisami i zasadami z zakresu ochrony danych osobowych.
6. Zasady organizacji szkoleń fakultatywnych:
   a) organizacja szkoleń fakultatywnych określana jest doraźnie dla każdego szkolenia oddzielnie,
   b) o potrzebie zorganizowania szkolenia decyduje sam Administrator, lub czyni to na wniosek IOD, ASI lub grupy pracowników.

Załącznik Nr 5
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
Nowym Tomyślu

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Przedmiot Instrukcji.

Przedmiotem Instrukcji jest określenie zagadnień związanych z bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych, w szczególności gromadzonych, transmitowanych i przechowywanych w systemach informatycznych, a także sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Instrukcja określa w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym;
3) stosowane metody i środki uwierzytelnienia oraz procedury, związane z ich zarządzaniem i użytkowaniem;
4) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
5) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania;
6) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w § 1 pkt. 5 powyżej;
7) sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
8) udostępnianie danych osobowych;
9) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych;
10) przetwarzanie danych osobowych na laptopach;
11) przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż laptopy.

§ 2

Charakterystyka systemu.

1. System informatyczny bazuje na strukturze sieci w topologii gwiazdy w standardzie Ethernet o przepustowości 100Mbps, 1Gbps i wyższych. Szkielet sieci strukturalnej oparty jest na technologii okablowania światłowodowego oraz skrętki miedzianej. System ma charakter złożony, rozległy i hybrydowy.
2. W budynku „C" znajduję się główna serwerownia Starostwa Powiatowego w Nowym Tomyślu skąd za pomocą okablowania światłowodowego połączono mniejsze serwerownie oraz punkty dystrybucyjne - budynek „B" i „D".
3. Sieć strukturalna klient-serwer oparta jest na urządzeniach typu: serwery, macierze blokowe, macierze dyskowe, dyski zewnętrzne, UTM, UPS'y oraz pozostałe sieciowe urządzenia aktywne przełączniki, routery, access pointy, hub'y itp.
4. Serwery Starostwa w tym PCUW pracują zarówno w oparciu o struktury wirtualizacji jak i wydzielonych maszyn dziedzinowych. Sieć oparta jest na usłudze katalogowej AD Microsoft Windows Server 2019.
5. Stacje klienckie rozmieszczone w kilku budynkach, oparte są na licencjonowanych systemach operacyjnych Microsoft oraz Linux.
6. Użytkownicy systemu informatycznego posiadają dostęp do zasobów serwerowych wewnętrznych, aplikacji Internetowych oraz aplikacji chmury zewnętrznej (paragraf Vulcana). Możliwa jest również praca w trybie terminalowym za pomocą RDP.
7. Użytkownicy posiadają dostęp do sieci Internet oraz otrzymują osobiste adresy poczty elektronicznej przydzielane na zasadzie: (pierwsza_litera_imienia)(nazwisko)@powiatnowotomyski.pl
8. Sieć lokalna zabezpieczona jest na styku z siecią Internet urządzeniem typu UTM a na stacjach roboczych zainstalowano oprogramowanie antywirusowe.
9. Serwerownia główna zabezpieczona jest centralnym zasilaczem awaryjnym utrzymującym właściwe parametry zasilania a punkty dostępowe zasilaczami typu rack.
10. Kopie zapasowe zarówno całych serwerów jak i baz danych dystrybuowane są pomiędzy poszczególnymi serwerowniami na serwery, macierze blokowe i dyskowe oraz dyski zewnętrzne.

§ 3

Procedury nadawania, modyfikacji i anulowania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Dostęp do systemu informatycznego (rozumiany również jako nadanie, odebranie lub zmiana uprawnień zarówno do oprogramowania stanowiskowego jak i sieciowego) nadawany jest użytkownikowi na wniosek ADO.
2. Uprawnienia w systemie informatycznym przyznawane użytkownikowi, wynikają z zakresu jego obowiązków i powinny być zgodne z upoważnieniem do przetwarzania danych osobowych.

3. Użytkownikom należy przyznawać minimalne uprawnienia, niezbędne do realizacji zadań, wynikających z ich zakresu obowiązków.
4. ADO jest zobowiązany wystąpić drogą do ASI o nadanie identyfikatora do systemu dla osoby upoważnianej, z podaniem programów i zasobów, których będzie używał pracownik upoważniony do przetwarzania danych osobowych.
5. ASI wprowadza nadany identyfikator do systemu dopiero po otrzymaniu potwierdzenia o podpisaniu upoważnienia do przetwarzania danych osobowych od pracownika ds. kadr w PCUW.
6. Nadawanie odbieranie modyfikacja uprawnień odbywa się na podstawie „karty uprawnień do systemów informatycznych" załącznik nr . XX na zasadzie jedna karta - jeden użytkownik.
7. ASI nadaje uprawnienia do określonego zasobu na opisanych uprawnieniach oraz ustala hasło które zostaje zmienione przez użytkownika przy pierwszym logowaniu.
8. Informacja o ustaniu stosunku zatrudnienia lub zakończeniu przez użytkownika wykonywania prac, określonych umową zlecenia / umową o dzieło / o staż / praktykę powinna być przekazana niezwłocznie przez pracownika ds. kadr w PCUW do ASI. W takim przypadku ASI natychmiast po otrzymaniu informacji blokuje dostęp użytkownikowi do systemu.
9. Każda zmiana uprawnień jest możliwa na wniosek ADO w oparciu o „kartę uprawnień do systemów informatycznych" po uzyskaniu wszystkich podpisów i przedstawiony ASI.
10. ASI przy realizacji zadań z zakresu dostępu do systemu informatycznego, a w szczególności przy zakładaniu konta o odpowiednim identyfikatorze, zabezpiecza je hasłem, tokenem lub kartą mikroprocesorową.
11. Konto użytkownika zostaje zablokowane przez ASI na polecenie ADO, lub z inicjatywy ASI w przypadku wystąpienia incydentu bezpieczeństwa.
12. W przypadku naruszania przez użytkownika zasad pracy w systemie informatycznym, ASI może zablokować konto do czasu wyjaśnienia nieprawidłowości. ASI o fakcie zablokowania konta informuje ADO.
13. ASI dokonuje okresowych przeglądów kont użytkowników w celu wykrycia kont nieaktywnych.
14. Powyższe zasady obowiązują również osoby uzyskujące dostęp do danych osobowych na podstawie umowy zlecenia.

§ 4
Rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym.

1. Przyznanie uprawnień w zakresie dostępu do danych przetwarzanych w systemach informatycznych zarówno stanowiskowych jak i sieciowych polega na przypisaniu przez ASI w systemie dla upoważnionego użytkownika:
   a. Unikalnego identyfikatora i hasła lub unikalnego identyfikatora i przypisanej do niego karty mikroprocesorowej;

b. wprowadzeniu do systemu zakresu dostępnych dla danego użytkownika uprawnień.

2. Każdy z użytkowników systemu posiada własny/unikalny identyfikator i hasło.
3. Ustanowione hasło dostępu, w sposób poufny ASI przekazuje użytkownikowi.
4. Hasło ustanowione podczas przyznawania uprawnień użytkownik jest zobowiązany zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.
5. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
6. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła, tokena lub karty mikroprocesorowej. Przekazywanie loginów i haseł innym pracownikom i osobom trzecim jest zabronione.
7. W przypadku anulowania uprawnień użytkownika jego identyfikator, token lub kartę mikroprocesorową należy niezwłocznie zablokować w systemie oraz unieważnić hasło użytkownika. Pracownik zobowiązany jest do zwrotu tokena lub karty do ASI.

§ 5

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła, lub weryfikacji tożsamości użytkownika przy użyciu tokena lub karty mikroprocesorowej.
2. Zmiana hasła użytkownika jeśli pozwala na to aplikacja lokalna lub sieciowa następuje nie rzadziej niż co 30 dni.
3. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie.
4. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł i ochronę swoich tokenów lub kart mikroprocesorowych.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
8. Przy wyborze hasła jeśli pozwala na to aplikacja obowiązują następujące zasady:
   a. minimalna długość hasła – 8 znaków,
   b. właściwa złożoność hasła - litery duże i małe oraz cyfry lub znaki specjalne.
9. Jeśli pozwala na to aplikacja zakazuje się stosowania haseł:

1) które użytkownik stosował uprzednio (do sześciu haseł wstecz),
2) będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
3) analogicznych jak identyfikator,
4) zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.,
5) stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków np. 12345678, abcdefgh, qwerty, qazwsx itp.

10. W systemach umożliwiających zapamiętanie hasła nie należy korzystać z tego ułatwienia.
11. Powyższe reguły w zakresie haseł dotyczą obowiązków użytkownika systemu niezależnie od istnienia lub nie mechanizmów wymuszających (ułatwiających) ich stosowanie.

§ 6

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Przed rozpoczęciem pracy w systemie informatycznym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora i hasła lub identyfikatora i przypisanej do niego karty mikroprocesorowej lub tokena.
1. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu, zablokowania dostępu poprzez zabezpieczony hasłem wygaszacz ekranu lub zablokowanie, wylogowanie sesji użytkownika, np. poprzez użycie kombinacji klawiszy na klawiaturze komputera:

   a. „Ctrl+Alt+Delete" i wybór polecenia „zablokuj ten komputer" lub „wyloguj";
   b. „logo systemu Windows+L" dla zablokowania komputera;
   c. usunięcie tokena/karty.

2. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
3. Ustawienie monitora podczas pracy powinno uniemożliwić podgląd jakimkolwiek osobom nieupoważnionym jeśli pozwalają na to warunki.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów na zasadzie wylogowania się.
5. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do ASI, który po stwierdzeniu przypadku stanowiącego incydent bezpieczeństwa podejmuje działania.
6. Zabronione jest podejmowanie działań mogących stanowić zagrożenie dla systemu, a w tym:
   1) łamanie haseł,
   2) dokonywanie włamań na konta innych użytkowników,
   3) nieprawne uzyskiwanie dostępu do kont administracyjnych,

4) zakłócanie działania usług,
5) omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione),
6) doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty,
7) przeglądanie zasobów sieciowych lub stacji roboczych innych użytkowników,
8) używanie nośników zewnętrznych typu pendrive, cd, dysków zewnętrznych, kart rozszerzeń nie zaszyfrowanych i nie należących do Starostwa Powiatowego w Nowym Tomyślu. Nośniki zewnętrzne otrzymać można od IODO. Pozostałe (np. otrzymane od klientów) nośniki powinny być najpierw przekazane do ASI w celu sprawdzenia ich pod kontem bezpieczeństwa antywirusowego.
9) Udostępniania haseł, loginów, pinów, tokenów, kart osobom postronnym.
10) Otwierania poczty od nieznanych nadawców, firm kurierskich oraz uruchamiania nieznanych linków i załączników zawierających faktury.
11) Przeglądania stron internetowych niezwiązanych z zakresem obowiązków.
12) praca na koncie innego użytkownika.

§ 7

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. W celu zagwarantowania bezpieczeństwa danych przechowywanych w systemie wykonywane są ich kopie zapasowe, tj. kopie bezpieczeństwa oraz archiwalne.
2. Kopie zapasowe dotyczą zarówno aplikacji lokalnych jak i sieciowych.
3. Bazy danych, oprogramowanie oraz konfiguracja systemów powinny być zabezpieczone w postaci kopii bezpieczeństwa.
4. Należy wykonywać następujące kopie bezpieczeństwa:
   a. przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,
   b. przed dokonaniem zmian w programach (np. zmiana wersji),
   c. zgodnie z przyjętym harmonogramem, określonym indywidualnie przez każdego KKO w stosunku do kopii danych lokalnych i przez ASI w stosunku do kopii danych w aplikacjach sieciowych.
5. Oprócz kopii bezpieczeństwa wykonywane są okresowo kopie archiwalne istotnych dla działalności PCUW danych.
6. Za wdrożenie i nadzór nad stosowaniem zasad i trybu wykonywania kopii zapasowych odpowiedzialny jest ASI. Backupy aplikacji i baz danych znajdujące się na serwerach Starostwa Powiatowego wykonywane są min 3 razy w tygodniu. Stacje robocze 1 raz w tygodniu.

§ 8

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

I. Kopie zapasowe.
   1. Kopie zapasowe należy przechowywać w warunkach gwarantujących brak dostępu do nich osób nieupoważnionych, tj. w zabezpieczonych pomieszczeniach, w sejfach lub szafach zamykanych na klucz.
   2. W przypadku wykonywania zabezpieczeń długoterminowych lub na nośnikach zewnętrznych, np. płytach CD, DVD nośniki te należy sprawdzać pod kątem ich dalszej przydatności oraz odtwarzalności.
   3. Kopie zapasowe należy usunąć niezwłocznie po upływie okresów przechowywania lub w przypadku ustania ich użyteczności.

II. Elektroniczne nośniki informacji.
   1. Dopuszcza się używanie służbowych elektronicznych nośników informacji, zwanych dalej nośnikami, w celu przenoszenia i archiwizowania danych osobowych, w tym płyt DVD, dysków zewnętrznych oraz nośników przenośnych typu pendrive.
   2. Należy unikać przechowywania danych osobowych na nośnikach zewnętrznych.
   3. Zabronione jest używanie nośników do przenoszenia danych osobowych na prywatne komputery lub inne prywatne urządzenia mogące służyć do przechowywania danych.
   4. Zabronione jest przetwarzanie danych osobowych poza siecią lokalną.
   5. Nośniki, zawierające dane osobowe, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny.
   6. Nośniki, zawierające dane osobowe, podlegają szczególnemu nadzorowi i są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w zamykanych szafach biurowych lub kasetkach.
   7. W przypadku zaistnienia okoliczności uzasadniających konieczność wyniesienia nośnika zawierającego dane osobowe poza obszar przetwarzania danych osobowych jego użytkownik zobowiązany jest uzyskania zgody ADO oraz do zachowania szczególnej ostrożności i zabezpieczenia nośnika przed dostępem osób nieupoważnionych, utratą lub zniszczeniem (np. poprzez szyfrowanie nośnika).
   8. Nośniki, zawierające dane osobowe, należy transportować w sposób bezpieczny (nie pozostawić ich w miejscach widocznych np. w samochodach, przypiętych do pasków itp.).
   9. Nośniki, zawierające dane osobowe, przeznaczone do:
      a. likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
      b. przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
      c. naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO.

§ 9

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

1. Oprogramowanie stosowane, wdrażane, modyfikowane, zakupione w PCUW może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych oraz powinno spełniać wymagania przepisów z zakresu ochrony danych osobowych.
2. Dozwolone jest jedynie uruchamianie oprogramowania związanego merytorycznie z wykonywaną pracą oraz dopuszczonego przez ASI do użytkowania w systemach PCUW.
3. Korzystanie z zasobów informatycznych PCUW poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności UTM, firewall oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.
4. Sieć wewnętrzna PCUW odseparowana jest od sieci publicznej za pomocą uaktywnionych firewall sprzętowych lub programowych.
5. Dostęp do sieci wewnętrznej, przy zastosowaniu zasad dopuszczenia do zasobów informatycznych obowiązujących w PCUW mogą posiadać:
   a. pracownicy PCUW,
   b. osoby lub podmioty, z którymi PCUW współpracuje na podstawie zawartych umów oraz ich pracownicy – w zakresie przewidzianym umową.
6. W celu ochrony systemów przed szkodliwym oprogramowaniem oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym systemu. Za prawidłowość realizacji powyższego obowiązku odpowiada ASI.
7. Sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.
8. Użytkownicy zobowiązani są do niezwłocznego zgłaszania do ASI każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów). ASI podejmuje działania mające na celu eliminację nieprawidłowości w zakresie realizacji obowiązku, o którym mowa w ust. 7 powyżej.
9. Programy antywirusowe winny być uaktywnione cały czas podczas pracy danego systemu.
10. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania szkodliwego oprogramowania najnowszą dostępną wersją programu antywirusowego. Pliki pochodzące z nośników zewnętrznych podlegają obowiązkowej kontroli pracowników ds. informatyki.

11. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
12. Zabrania się używania elektronicznych nośników informacji niewiadomego pochodzenia.
13. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia otwierania podejrzanych wiadomości pocztowych (np. faktur, informacji o przesyłkach kurierskich oraz od nieznanych nadawców) .
14. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania, każdy użytkownik winien zawiadomić ASI o zaistniałym zdarzeniu.

§ 10
Udostępnianie danych osobowych.

1. Dane osobowe administrowane w PCUW mogą być udostępniane:
   a. osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
   b. innym osobom i podmiotom w przypadku posiadania przez wnioskującego podstaw do legalnego przetwarzania danych.
2. Udostępnienie danych nie może naruszać praw i wolności osób, których dane dotyczą.
3. W przypadku pojawienia się wątpliwości w zakresie możliwości udostępnienia danych osobowych ADO zasięga opinii IOD.
4. IOD może wydać opinię negatywną udostępnienia danych jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzonych w systemie informatycznym.
5. W celu nadzoru nad udostępnianiem danych osobowych przypadki przekazania danych należy odnotowywać w systemach.
6. Dane udostępnione PCUW przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§ 11
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądy, konserwacje lub naprawy systemów i nośników wykorzystywanych w PCUW dokonywane są przez osobę upoważnioną do tego typu czynności, w szczególności ASI.
2. Dopuszcza się realizację czynności określonych w ust. 1 przez specjalistyczne firmy świadczące usługi w tym zakresie; w takim przypadku konieczne jest zawarcie stosownej umowy cywilnoprawnej.
3. Umowy w zakresie świadczenia usług teleinformatycznych wiążące się z przetwarzaniem danych osobowych powinny być traktowane jako powierzenie przetwarzania danych osobowych.

4. Pracownicy firm świadczących usługi, o których mowa w ust. 2 powyżej wykonują zlecone zadania tylko za zgodą ASI, lub innego uprawnionego pracownika PCUW i pod jego nadzorem.
5. W przypadku zdalnego dostępu do komputera lub fizycznej pracy osoby nie posiadającej uprawnień (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez ASI lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania.
6. Przeglądy i konserwacje wykonywane są cyklicznie oraz w przypadku pojawienia się usterki lub awarii systemów informatycznych.

§ 12

Przetwarzanie danych osobowych na komputerach przenośnych.

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
2. W przypadku potrzeby korzystania z komputerów przenośnych poza obszarem przetwarzania należy bezwzględnie zgłosić ten fakt ASI, w celu zaszyfrowania komputera.
3. W sytuacji przetwarzania danych osobowych, przez pracowników PCUW na komputerach przenośnych poza obszarem przetwarzania wskazanym w PODO, odpowiedzialni za ich bezpieczeństwo są ich użytkownicy i są zobowiązani chronić dane przed dostępem do nich osób nieupoważnionych.
4. Komputery przenośne po zakończonej pracy winny być przechowywane przez użytkownika w warunkach zapewniających ich bezpieczeństwo.
5. W przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
6. Podczas transportu komputerów przenośnych wynoszonych poza obszar przetwarzania danych osobowych należy zapewnić ich bezpieczeństwo tj. nie należy ich pozostawiać bez nadzoru w samochodzie (lub innym miejscu). Muszą one być przewożone jako bagaż podręczny.
7. Należy unikać przechowywania na komputerach przenośnych danych osobowych.
8. Komputery przenośne muszą być wyposażone w uaktywniony firewall programowy lub poprzez szyfrowanie.
9. W przypadku przetwarzania danych osobowych na komputerach przenośnych baza danych osobowych powinna być szyfrowana, zabezpieczona odpowiednim hasłem. Przetwarzanie danych na komputerach przenośnych poza obszarem przetwarzania odbywa się za zgodą ADO.

§ 13

Przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż komputery.

1. Pracownicy korzystający z teleinformatycznych urządzeń przenośnych, tj. m.in. telefonów służbowych, tabletów, aparatów fotograficznych, kamer wideo, są zobowiązani chronić dane osobowe zawarte w pamięci tych urządzeń przed dostępem osób nieupoważnionych.
2. Wszelkie –dane– osobowe- wprowadzone do pamięci- urządzeń przenośnych powinny być usunięte przed zdaniem urządzenia do właściwej komórki organizacyjnej. Osobą właściwą do ich usunięcia jest pracownik lub funkcjonariusz korzystający z danego urządzenia. W przypadku trudności technicznych przy usuwaniu danych osobowych należy kontaktować się z ASI.
3. Kontakt z serwisami zewnętrznymi, dotyczący użytkowanego sprzętu oraz oprogramowania, możliwy jest tylko za pośrednictwem ASI.
4. W treści informacji o przyznaniu pracownikowi urządzenia powinny znaleźć się wskazania w zakresie ochrony danych osobowych przetwarzanych przy jego pomocy.

Załącznik Nr 6
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

WZÓR INFORMACJI O PRZEPROWADZENIU
SZKOLENIA PRZED PRZYSTĄPIENIEM DO PRACY/SŁUŻBY/STAŻU/PRAKTYK

W dniu ..... przeprowadzone zostało „Szkolenie przed przystąpieniem do pracy / służby / stażu / praktyk [1)]" dla osoby, która będzie w ramach swoich obowiązków w Powiatowym Centrum Usług Wspólnych przetwarzała dane osobowe.

W trakcie szkolenia zapoznano Panią(a) ..... z regulacjami prawnymi w zakresie ochrony danych osobowych, w szczególności przekazano informację o obowiązkach spoczywających na osobach przetwarzających dane osobowe na mocy:

- ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 o ochronie danych osobowych,
- innych przepisów Unii lub przepisów polskich o ochronie danych osobowych,
- regulacji wewnątrzzakładowych, takich jak polityki, instrukcje, procedury z zakresu ochrony danych osobowych obowiązujące na terenie Powiatowego Centrum Usług Wspólnych w Nowym Tomyślu,

Szkolenie przeprowadzono zgodnie z zapisami Polityki Ochrony Danych Osobowych w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu.

....

(czytelny podpis osoby szkolonej) *(czytelny podpis prowadzącego szkolenie)*

OBJAŚNIENIA.

1) właściwe podkreślić lub podać inne,

Załącznik Nr 7
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

.....
(pieczątka nagłówkowa)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie art. 29 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679, upoważniam Panią/Pana

.....

do przetwarzania danych osobowych w systemie informatycznym/nieinformatycznym[1)] w zakresie zasobów przetwarzanych w ramach pełnionych obowiązków pracowniczych/służbowych/wynikających z zawartej umowy zlecenie/praktyk/stażu[2)] .

Data nadania: ..... Data ustania: dzień zakończenia stosunku pracy

Wyżej wymieniona osoba została dopuszczona do przetwarzania danych osobowych w zakresie określonym w ogólnym rozporządzeniu o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 oraz procedurach i instrukcjach, obowiązujących w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu.

.....
(podpis Administratora lub osoby upoważnionej do nadawania i podpisywania upoważnień w jego imieniu)

.....
(data i podpis osoby upoważnionej)

OBJAŚNIENIA.
1) *właściwe podkreślić,*
2) *właściwe podkreślić lub wstawić inny zakres obowiązków,*

Załącznik Nr 8
do Polityki Ochrony Danych Osobowych w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu

OŚWIADCZENIE [1)]

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem prac na rzecz Powiatowego Centrum Usług Wspólnych w Nowym Tomyślu.

Zobowiązuję się przestrzegać polityk, instrukcji, regulaminów i procedur obowiązujących w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów PCUW.

Oświadczam, że zostałam(em) zapoznana(y) z przepisami ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679, właściwymi przepisami z zakresu ochrony danych osobowych, w tym informacjami o grożącej odpowiedzialności karnej, a także z procedurami i instrukcjami obowiązującymi w zakresie ochrony danych osobowych w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu.

.....

(data i czytelny podpis osoby upoważnionej do przetwarzania danych osobowych)

Załącznik Nr 9
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

WZORY ZAPISÓW UMOWY DOTYCZĄCEJ POWIECZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu

reprezentowanym przez Dyrektora PCUW

_____

zwana w dalszej części umowy „Administratorem"

reprezentowana przez: _____

oraz

(dane podmiotu który umowę zawiera, w szczególności: firma spółki, siedziba, adres, oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; NIP. W przypadku podmiotów prowadzących działalność gospodarczą imię nazwisko adres zamieszkania osoby fizyczne, PESEL, firma pod jaką działalność jest prowadzona oraz adres głównego miejsca wykonywania działalności)

zwana w dalszej części umowy „Podmiotem Przetwarzającym"

reprezentowana przez:

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi Przetwarzającemu dan osobowe do przetwarzania w trybie art. 28 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz.UE.L Nr 119, str.1), zwanego w dalszej części Umowy „Rozporządzeniem" na zasadach, w zakresie i w celu określonych w niniejszej Umowie.

2. Podmiot Przetwarzający zobowiązuje się przetwarzać:
   a) powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy dane ..... (należy podać rodzaj danych, tj. tzw. dane zwykłe lub/i dane osobowe szczególnych kategorii) dotyczące ..... (należy podać kategorię osób, których dane dotyczą np. pracowników administratora, klientów administratora, kontrahentów, osoby biorące udział w konkursie ..... (podać nazwę konkursu itd.) w zakresie ..... (należy podać kategorię danych osobowych, np. imiona i nazwiska, adresy zamieszkania, numer PESEL, data urodzenia, imiona rodziców itd.).
2. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu ..... (należy podać cel przetwarzania danych przez Podmiot przetwarzający, np. realizacja umowy z dnia .....nr ..... w zakresie przeprowadzenia szkolenia w zakresie BHP, prowadzenia spraw .....).

3. Podmiot Przetwarzający oświadcza, że stosuje środki techniczne i organizacyjne spełniające wymogi Rozporządzenia i chroniące prawa osób, których dane dotyczą.

§ 3

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z Rozporządzeniem, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Lista środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający stanowi załącznik nr 1 do Umowy.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby, o których mowa w niniejszym ustępie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
5. Dla prawidłowej realizacji ust. 4 Podmiot Przetwarzający dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie *usuwa/zwraca Administratorowi* wszelkie dane osobowe [należy wybrać, czy Podmiot przetwarzający ma usunąć, czy zwrócić dane] oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 Rozporządzenia. Podmiot przetwarzający w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora w terminie 5 dni roboczych od otrzymania wiadomości [Administrator termin może określić dowolnie, z zastrzeżeniem terminowej realizacji zadań wynikających z Rozporządzenia*]*. Udzielając informacji, Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.
8. W przypadku stwierdzenia jakiegokolwiek naruszenia ochrony danych osobowych Podmiot przetwarzający lub podwykonawca Podmiotu przetwarzającego zgłasza je Administratorowi w ciągu 24 h.

§ 4

Prawo kontroli

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo kontroli, mającej na celu weryfikację, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych będzie realizować prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum ..... uprzedzeniem *[*
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób

upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.

4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni [Administrator termin może określić dowolnie].
5. Powyżej określone zasady kontroli Podmiotu Przetwarzającego mają zastosowanie do przeprowadzanych przez Administratora kontroli podwykonawców Podmiotu przetwarzającego, o których mowa w § 6 ust. 1 Umowy.

§ 5

Raportowanie

1. Na wniosek Administratora Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z Rozporządzenia.
2. Informacji, o których mowa w ust. 1, udziela się w terminie 15 dni roboczych [Administrator termin może określić dowolnie, z zastrzeżeniem terminowej realizacji zadań wynikających z Rozporządzenia] od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

§ 6

Dalsze powierzenie danych do przetwarzania

1. Administrator wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania przez podwykonawców Podmiotu przetwarzającego, w celu wykonania niniejszej Umowy, przy czym podwykonawcy Podmiotu przetwarzającego powinni spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający niniejszą Umową. Lista takich podmiotów (podprocesorów) stanowi załącznik nr 2 do Umowy.
2. W przypadku zmiany lub dodania innych podwykonawców biorących udział w przetwarzaniu danych powierzonych przez Administratora Podmiot przetwarzający informuje o zamierzonych zmianach, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian w terminie 5 dni roboczych od przekazania informacji o zamierzonych zmianach [Administrator termin może określić dowolnie].
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora danych, chyba że taki obowiązek nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa

członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków spoczywających na podwykonawcy, wynikających z niniejszej Umowy.

§ 7

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 8

Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony od .... do ....* [należy wybrać].
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem ..... okresu wypowiedzenia[należy wskazać okres wypowiedzenia].

§ 9

Rozwiązanie Umowy

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

§ 10

Zasady zachowania poufności

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

§ 11

Postanowienia końcowe

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

_____ _____

Administrator danych Podmiot przetwarzający

Załączniki:

1. załącznik nr 1 – Wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający;
2. załącznik nr 2 – Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów).

Załącznik nr 1

Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający

PYTANIE	ODPOWIEDŹ
Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy?	
Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia?	
Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów	

funkcjonujący w jego organizacji system ochrony danych osobowych?	
Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?	
Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji?	
Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany?	
Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?	
Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby?	
Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób?	
Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane	

osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	
Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka?	
Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	
Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach?	
Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane?	
Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych?	
Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu?	
Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych?	
Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe?	
Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych?	
Gdzie są przechowywane kopie zapasowe?	
Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania?	

Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design?	
Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default?	
Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?	
Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	

Załącznik nr 2

Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów)

Przy wykonaniu Umowy Procesor korzysta z usług następujących podprocesorów:

PODPROCESOR	ADRES SIEDZIBY

Załącznik Nr 10
do Polityki Ochrony Danych Osobowych w
Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Zgodnie z art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 wyrażam zgodę, na przetwarzanie moich danych osobowych .....[1)], przez Powiatowe Centrum Usług Wspólnych w Nowym Tomyślu w celu ....

Zgodnie z art. 7 ust. 3 wyżej wskazanego Rozporządzenia zgoda udzielona na przetwarzanie danych osobowych może być wycofana w formie oświadczenia na piśmie w dowolnym czasie, nie wpływa to jednak na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

.....
(miejscowość i data)

.....
(podpis osoby wyrażającej zgodę)

OBJAŚNIENIA.

1) wskazać o jakie dane osobowe chodzi.

Załącznik Nr 11
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

OGÓLNA KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46 WE (zwanym dalej RODO) informujemy, że:

1. Administratorem przetwarzającym Pani/Pana dane osobowe jest Powiatowe Centrum Usług Wspólnych z siedzibą w Nowym Tomyślu, ul. Poznańska 33, 64-300 Nowy Tomyśl, telefon 614426732, e-mail: oswiata@powiatnowotomyski.pl.
2. Administrator wyznaczył Inspektora Ochrony Danych - Marlenę Galas, z którym można się kontaktować: telefonicznie: 614426705, poprzez e-mail: iod@powiatnowotomyski.pl oraz listownie na podany wyżej adres.
3. Pani/Pana dane osobowe będą przetwarzane w celu:
   - wypełnienia obowiązku prawnego ciążącego na Administratorze, na podstawie art. 6 ust. 1 lit. C RODO,
   - wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi, na podstawie art. 6 ust. 1 lit. E RODO,
   - realizacji umów zawartych z kontrahentami) art. 6 ust. 1 lit. b RODO),
   - w pozostałych przypadkach Pani/Pana dane osobowe przetwarzane będą wyłącznie na podstawie wcześniej udzielonej zgody (podstawa prawna: art. 6 ust. 1 lit. a RODO)
4. W związku z przetwarzaniem danych osobowych w celach, o których mowa w pkt. 3 odbiorcami Pani/Pana danych osobowych mogą być:
   - organy władzy publicznej oraz inne podmioty wykonujące zadania publiczne lub działające na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów powszechnie obowiązującego prawa,
   - inne podmioty, które na podstawie stosownych umów przetwarzają dane osobowe w imieniu Administratora na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (tzw. Podmioty przetwarzające).
5. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celu dla którego zostały zebrane, a następnie przez okres niezbędny wynikający z przepisów dotyczących archiwizowania dokumentów obowiązujących u Administratora (Rzeczowy Wykaz Akt) albo do momentu wycofania przez Panią /Pana zgody na ich przetwarzanie.

Załącznik Nr 12
do Polityki Ochrony Danych Osobowych
w Powiatowym Centrum Usług Wspólnych
w Nowym Tomyślu

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1

Osoby zobowiązane do ochrony danych osobowych

1. Osobami odpowiedzialnymi za ochronę danych osobowych, zgodnie z właściwością, są :
   a) Dyrektor Powiatowego Centrum Usług Wspólnych,
   b) IOD,
   c) ASI,
   d) osoby upoważnione do przetwarzania danych osobowych,
   e) osoby, które nie przetwarzają danych osobowych, ale w ramach czynności poznały sposoby ich zabezpieczania.

§ 2

Obowiązki osób zobowiązanych do ochrony danych osobowych w sytuacji naruszenia ochrony danych osobowych

1. Każdy zobowiązany do ochrony danych osobowych, zwany dalej Zobowiązanym, jeśli stwierdzi lub podejrzewa naruszenie zabezpieczenia danych osobowych, powinien niezwłocznie poinformować o tym Dyrektora PCUW lub osobę zastępującą, IOD oraz ASI.
2. Informację o naruszeniu Administrator powinien niezwłocznie przekazać do IOD w celu umożliwienia mu realizacji jego obowiązków.
3. Zobowiązany, który stwierdził lub podejrzewa naruszenie zabezpieczenia danych osobowych, oprócz obowiązku wymienionego w § 2 pkt. 1 powinien:
   a) powstrzymać się od wykonywania pracy lub jakichkolwiek czynności mogących spowodować zatarcie śladów lub dowodów naruszenia,
   b) podjąć, odpowiednie do zaistniałej sytuacji działania niezbędne do zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych.
3. Administrator lub osoba zastępująca, po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:

b) przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, dostępu do danych osobowych itp.,

c) podjąć odpowiednie kroki w celu zminimalizowania szkód i rozmiarów zdarzenia oraz zabezpieczenia przed usunięciem śladów zdarzenia,

d) osobiście lub polecić IOD w terminie 72 godzin przesłać do właściwego Organu Nadzorczego zgłoszenie naruszenia ochrony danych osobowych jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych;

e) osobiście lub polecić IOD bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o naruszeniu jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych; postępowanie to powinno być zgodne z art. 34 RODO,

4. IOD jest zobowiązany zarejestrować zdarzenie; wzór „Rejestru naruszeń ochrony danych osobowych w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu" stanowi załącznik nr 1 do tej Instrukcji,

5. Administrator, czynności o których mowa w § 2 pkt. 3 lit. a), b), w sytuacjach szczególnych, takich jak konieczność zgłoszenia naruszenia ochrony danych osobowych do właściwego Organu Nadzorczego, może dokumentować wykorzystując dokumenty określone w rozdziale XIV Polityki „Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO"; sporządzeniem tej dokumentacji powinien zająć się wskazany pracownik Administratora, a w sytuacjach szczególnych IOD.

6. W przypadku zdarzenia mającego związek z systemem informatycznym ASI zobowiązany jest do:
   a) szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia,
   b) wygenerowania, wydrukowania wszystkich możliwych dokumentów, raportów lub zestawień, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je
   c) datą i podpisem,
   d) fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwiać dostęp do bazy danych osobowych osobie nieupoważnionej,
   e) wylogowania użytkownika podejrzewanego o naruszenie ochrony danych osobowych,
   f) zmiany haseł na konta, poprzez które uzyskano nielegalny dostęp,
   g) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, przywrócenia jej z ostatniej kopii awaryjnej z zachowaniem środków ostrożności przed ponownym dostępem tą samą drogą przez osobę nieupoważnioną,

5. ASI o podjętych działaniach powinien niezwłocznie poinformować Administratora.

6. Wszyscy zobowiązani mają obowiązek udzielić wszelkiej niezbędnej pomocy przy realizacji zadań przez IOD.

Załącznik Nr 1
do Instrukcji Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych

.....
(pieczątka nagłówkowa)

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH
w Powiatowym Centrum Usług Wspólnych w Nowym Tomyślu

Lp.	Data i godzina zgłoszenia IOD faktu naruszenia	Imię i nazwisko osoby zgłaszającej naruszenie	Okoliczności naruszenia	Skutki naruszenia	Opis podjętych działań zaradczych	Decyzja Administratora o zgłoszeniu naruszenia właściwemu organowi nadzorczemu	Decyzja Administratora o powiadomieniu o naruszeniu osoby, której dane dotyczą	Podpis Administratora
1.	2.	3.	4.	5.	6.	7.		8.
1.								

Powiatowe Centrum Usług Wspólnych w Nowym Tomyślu	załącznik nr 13

Analiza Ryzyka Bezpieczeństwa Danych Osobowych

		Imię i nazwisko	Data	Podpis
Opracował	**Inspektor Ochrony Danych**			
Zatwierdził	**Administrator Danych**			

Powiatowe Centrum Usług Wspólnych w Nowym Tomyślu	załącznik nr 13

1. PODSTAWA PRAWNA

- ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781).

2. TERMINOLOGIA I SKRÓTY

Ryzyko naruszenia praw i wolności osób fizycznych na gruncie RODO uwzględnia:

- prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem, oraz
- powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą.

Aktywa – wszystko, co posiada wartość dla organizacji z punktu widzenia bezpieczeństwa danych osobowych.

Dostępność - możliwość uzyskania i wykorzystania na żądanie przez uprawnioną jednostkę.

Poufność - cecha informacji, która nie jest udostępniana ani ujawniana nieupoważnionym osobom, jednostkom lub procesom.

Integralność - dokładność i kompletność zasobów.

Bezpieczeństwo danych osobowych - ochrona poufności, integralności i dostępności informacji; mogą tu także należeć inne właściwości, takie jak autentyczność, odpowiedzialność, brak odrzucenia i niezawodność.

Incydent związany z ochroną danych osobowych - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, stwarzających znaczne prawdopodobieństwo zakłócenia lub zatrzymania działań biznesowych i zagrażających bezpieczeństwu danych osobowych w odniesieniu do poufności, integralności i dostępności,

Zdarzenie związane z ochroną danych osobowych - zwane też zdarzeniem bezpieczeństwa — jest to określony stan systemu, usługi lub sieci, który wskazuje na niezgodność, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem (może wpływać na bezpieczeństwo) i może być przyczyną incydentu lub słabością systemu,

Słabość systemu lub zabezpieczenia, aktywu — stan, sytuacja lub właściwość która, może spowodować wystąpienia incydentu lub zdarzenia związanego z ochroną danych osobowych,

Podatność — słabość aktywu lub grupy aktywów, która może być wykorzystana przez co najmniej jedno zagrożenie.

3. PODEJŚCIE OPARTE NA RYZYKU

Zasada podejścia opartego na ryzyku jest ważną, perspektywiczną koncepcją, stanowiącą trzon ogólnego rozporządzenia o ochronie danych.
Zasada ta uzależnia sposób realizacji obowiązków nałożonych na administratora od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów administratora

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko [motyw 76 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych - RODO)].

Etapy szacowania ryzyka.

Ustalenie kontekstu

- Określenie informacji i uwarunkowań związanych z działaniem organizacji
- Szczegółowy opis przetwarzanych danych i ich klasyfikacja
- Szczegółowy opis stosowanych zabezpieczeń i innych ograniczeń
- Określenie kryteriów akceptacji ryzyka

Mechanizmy kontrolne

- Identyfikacja wymagań dla procesów przetwarzania danych w kontekście konkretnych celów działalności administratora
- Wymagania dotyczące zastosowania środków kontroli i bezpieczeństwa oraz stopień ich wypełnienia

Szacowanie ryzyka

- Identyfikacja zagrożeń
- Identyfikacja występujących podatności
- Analiza i ocena następstw zmaterializowania się zagrożeń
- Szacowanie poziomu ryzyka
- Określenie listy zidentyfikowanych ryzyk

Postępowanie z ryzykiem - decyzja

- Ustalenie, czy przeprowadzenie oceny skutków jest wymagane
- Zasięgnięcie opinii ekspertów i osób, których dane dotyczą lub ich przedstawicieli. Stworzenie ram dla oceny skutków dla ochrony danych w kodeksach postępowania
- Uwzględnienie szczególnych elementów oceny skutków dla ochrony danych.

4. CEL

Celem Analizy Ryzyka jest zapewnienie, że:

1. Proces szacowania ryzyka jest kompletny oraz daje szczegółowe, porównywalne i odtwarzalne rezultaty,

2. Kryteria oceny ryzyka są ustanowione i spójne z rzeczywistym stanem bezpieczeństwa danych osobowych w Organizacji oraz dostarczają rzetelnych wyników na temat faktycznego poziomu ryzyka,
3. Zidentyfikowano potencjalne ryzyko, opisano w kategoriach ilościowych i zarządza się nim świadomie,
4. Dokumentacja szacowania ryzyka jest poddawana cyklicznym przeglądom.

Celem Analizy jest ustalenie metodyki oceny ryzyka bezpieczeństwa danych osobowych oraz skutecznego pomiaru wyselekcjonowanych zabezpieczeń i grup zabezpieczeń poprzez mierniki oceny skuteczności. Na proces oceny ryzyka składa się:

1. Przeprowadzenie szczegółowej oceny ryzyka w kontekście utraty integralności, poufności i/lub dostępności danego aktywa,
2. Opracowanie planu postępowania z ryzykiem w oparciu o przyjęte kryteria akceptacji ryzyka z uwzględnieniem powtórnej analizy, w ramach wdrożonych działań zawartych w Planie postępowania z ryzykiem, zidentyfikowanych nowych podatności i zagrożeń oraz dokonanych incydentów dotyczących naruszenia bezpieczeństwa informacji.

5. SZACOWANIE RYZYKA

TRYB POSTĘPOWANIA

- Ocena ryzyka

Istotą procesu oceny ryzyka jest określenie znaczenia ryzyka na podstawie porównania wyznaczonych wartości ryzyk dla zidentyfikowanych aktywów z kryteriami akceptowania ryzyka w kontekście celów strategicznych i biznesowych organizacji oraz spełnienia przepisów prawa. Ocena ryzyka powinna być prowadzona na właściwym stopniu szczegółowości z uwzględnieniem strat finansowych, wizerunkowych i informacyjnych których organizacja doświadczyła bądź może doświadczyć w przyszłości. Polega to na przypisywaniu wartości liczbowej prawdopodobieństwu wystąpienia podatności oraz skutkom zdarzeń.

Ponowną ocenę ryzyka przeprowadza się raz w roku lub w przypadku wystąpienia zmian w organizacji mogących mieć wpływ na ocenę ryzyka.

- Identyfikowanie potencjalnych zagrożeń i podatności

Ocena ryzyka przeprowadzana jest dla każdego zidentyfikowanego aktywa i rozpatruje dwa obszary:

1. Prawdopodobieństwo wystąpienia zagrożenia,
2. Siła oddziaływania - skutków potencjalnych zagrożeń, biorąc pod uwagę następstwa naruszenia lub utraty:
   - poufności,
   - integralności,
   - dostępności,

   które mogą nastąpić w wyniku działań:
   - umyślnych - (U),
   - przypadkowych - (P),
   - naturalnych - (N).

Przyjmuje się, że zagrożenia (U, P) są wynikiem działań ludzkich, natomiast źródła zagrożeń (N) są niezależne od człowieka.

Przykładową listę potencjalnych i realnych dla Organizacji zagrożeń umieszczono w poniższej tabeli. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa oraz skutków zdarzeń.

Typowe zagrożenia — przykłady

Rodzaj	Zagrożenie
Zniszczenia fizyczne	pożar, zalanie, zanieczyszczenie, poważny wypadek, zniszczenie urządzeń lub nośników, pył, korozja, wychłodzenie
Zjawiska naturalne	zjawiska klimatyczne, zjawiska pogodowe, powódź
Naruszenie bezpieczeństwa informacji	podsłuch, kradzież nośników lub dokumentów, kradzież urządzenia, szpiegostwo, kopiowanie danych, odtworzenie wyrzuconych nośników
	ujawnienie informacji, dane z niewiarygodnych źródeł, sfałszowanie oprogramowania,
Awarie techniczne	awaria urządzenia, niewłaściwe funkcjonowanie urządzenia, niewłaściwe funkcjonowanie oprogramowania
	umyślne uszkodzenie urządzenia lub oprogramowania
Utrata usług	awaria systemu klimatyzacji, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego
Zakłócenia spowodowane promieniowaniem	promieniowanie elektromagnetyczne, promieniowanie cieplne, impuls elektromagnetyczny
Nieautoryzowanie działania	niewłaściwe funkcjonowanie urządzeń, niewłaściwe funkcjonowanie oprogramowania
	przeciążenie systemu informacyjnego, naruszenie zdolności utrzymania systemu informacyjnego
Naruszenie bezpieczeństwa funkcji	błąd użytkowania
	naruszenie praw
	fałszowanie praw, odmowa działania
	naruszenie dostępności personelu

- Metodyka Oceny Ryzyka

Metodyka Oceny Ryzyka w Organizacji, została ustanowiona w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w organizacji oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka. Ocena ryzyka przeprowadzana jest w Arkuszu Oceny Ryzyka w programie EXCEL. Za dane wejściowe do procesu oceny uważa się wszelkie informacje przedstawione w analizie ryzyka, a także wiedzę pracowników na temat stosowanych zabezpieczeń, w szczególności miejsce przetwarzania, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywa.

Szacowanie prawdopodobieństwa

Badane kryterium	Ryzyko	Wartość
(P) Prawdopodobieństwo (możliwość wystąpienia)	niskie, odległe, mało realne szanse na zdarzenie	1
	może się zdarzyć lub zdarza się sporadycznie	2
	bardzo realne szanse wystąpienia	3

Powaga zdarzenia

Badane kryterium	Ryzyko	Wartość
(S) Skutek (wpływ na organizację i/lub proces)	utrata danych nie spowoduje utrudnień w pracy przedsiębiorstwa lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu	1
	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku przedsiębiorstwa, odtworzenie danych jest możliwe ale pracochłonne	2
	utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne; odtworzenie danych i reputacji będzie trudne i kosztowne.	3

3.2.4. Kategoria Ryzyka

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:

$$R = P \times S$$

P - Prawdopodobieństwo

S – Skutek (powaga zdarzenia)

Wynik z działania zgodnie z poniższą tabelą, należy przypisać ustanowionym kategoriom ryzyka, a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego w ramach Planu postępowania z ryzykiem.

Wytyczne do postępowania z ryzykiem

Klasa Kategorii	Kategoria Ryzyka	Wartość Ryzyka	Akceptacja Ryzyka Tak / Nie	Działania zapobiegawcze
1	Małe	1 - 3	TAK	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące.
2	Średnie	4	TAK	Należy rozważyć konieczność zredukowania ryzyka do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne.
3	Duże	6 - 9	NIE	Ocena skutków. Należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc aktywa w bezpieczniejsze miejsce.

3.2.6. Plan postępowania z ryzykiem

Inspektor Ochrony Danych dla aktywów gdzie ryzyko było nieakceptowalne, ocenia skutki i formułuje Plan Postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu bezpiecznego — akceptowalnego.

Ostatecznie zatwierdzone i wdrożone zabezpieczenia należy wpisać w dokument oceny ryzyka, w kolumnie działań zapobiegawczych i/lub korygujących w celu przeprowadzenia ponownej oceny ryzyka.

Podpis AD