

## POLITYKA BEZPIECZEŃSTWA

Administrator Danych - Jacek Malinowski Dyrektor Zespołu Szkół Rolnicze Centrum Kształcenia Ustawicznego w Przemystce dnia 27.03.2017 r. w podmiocie o nazwie:  
ZESPÓŁ SZKÓŁ ROLNICZE CENTRUM KSZTAŁCENIA USTAWICZNEGO  
W PRZEMYSTCE

**Zgodnie z ROZPORZĄDZENIEM MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) wdraża dokument o nazwie „Polityka Bezpieczeństwa”.  
Zapisy tego dokumentu wchodzi w życie z dniem 27.03.2017 r.**

### § 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Zespole Szkół Rolnicze Centrum Kształcenia Ustawicznego w Przemystce, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

### § 2

Ileokroć w „Polityce Bezpieczeństwa” jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,
7. specjaliście ds. ochrony danych osobowych – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad

ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.

8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową.

### § 3.

Administrator Danych w podmiocie Zespole Szkół Rolnicze Centrum Kształcenia Ustawicznego w Przemystce wyznacza specjalistę ds. ochrony danych osobowych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych chyba, że Administrator Danych sam wykonuje te czynności. Upoważnienie dla specjalisty ds. ochrony danych osobowych oraz zakres obowiązków określa **załącznik nr 1**.

### § 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 2**.

### § 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik nr 3**.

### § 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik nr 4**

### § 7.

**Specjalista ds. ochrony danych osobowych** dba o to aby dane osobowe w formie papierowej i elektronicznej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

### § 8.

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych. Specjalista ds. ochrony danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **załącznik nr 5**
3. Administrator danych nadaje upoważnienia do przebywania w obszarze przetwarzania danych dla pracowników wykonujących pracę w pomieszczeniach, w których są przetwarzane dane osobowe – **załącznik nr 6**
4. Specjalista ds. ochrony danych osobowych prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

- 1) Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie – załącznik nr 6
- 2) Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. – **załącznik nr 7**
- 3) Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazane zgodnie z art. 38 Ustawy o ochronie danych osobowych – **załącznik nr 8**
- 4) Treść obowiązku informacyjnego Administratora danych osobowych zgodnie z art. 24 i art. 25 ustawy z dnia 29.08.1997 r. o ochronie danych osobowych - **załącznik nr 9**

§ 9.

Na wniosek osoby, której dane dotyczą, specjalista ds. ochrony danych osobowych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie – **załącznik nr 10**

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa” mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych, oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2014 nr 100, poz. 1024)

§ 13.

### **Deklaracja intencji, cele i zakres polityki bezpieczeństwa**

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.
5. Celem Polityki jest przetwarzanie, zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranieniem przez



osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie się zmieniającym w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:

- a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
- b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

8. Dla skutecznej realizacji Polityki Administrator danych zapewnia:

- a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
- b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
- c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
- d) monitorowanie zastosowanych środków ochrony;
- e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
- f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

9. Monitorowanie przez Administratora Danych Osobowych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych Osobowych lub osoba przez niego upoważniona wdraża wszystkie dokumenty składające się na Polityki Bezpieczeństwa i zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych:

- a) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.);
- b) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
- c) Innymi przepisami mającymi zastosowania przy przetwarzaniu danych osobowych.

DYREKTOR

Podpis Administratora Danych Osobowych

  
mgr Jacek Malinowski

Podpis specjalisty ds. ochrony danych osobowych

Podpis