POLITYKA BEZPIECZEŃSTWA

Administrator Danych Osobowych – **Centrum Kształcenia Prymus Edyta Sawicka**
w osobie: **Edyta Sawicka** dnia **23-05-2018r**

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 wchodzą w życie

z dniem **23-05-2018r** .

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: **Centrum Kształcenia Prymus Edyta Sawicka**, 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

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1) **ADMINISTRATORZE BEZPIECZEŃSTWA INFORMACJI** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
2) **ADMINISTRATORZE DANYCH OSOBOWYCH** – rozumie się przez to Administratora Danych Osobowych podmiotu reprezentowanego przez osobę kierującą,
3) **ADMINISTRATORZE SYSTEMU INFORMATYCZNEGO** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków administratora systemu,
4) **HAŚLE** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
5) **IDENTYFIKATORZE** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
6) **INTEGRALNOŚCI DANYCH** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **ODBIORCY DANYCH** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
8) **OSOBIE UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH** – rozumie się przez to osobę,

która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie zgodnie z art. 37 ustawy,

9) **POUFNOŚCI DANYCH** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

10) **PRZETWARZAJĄCYM** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

11) **RAPORCIE** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

12) **ROZLICZALNOŚCI** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

13) **ROZPORZĄDZENIU** – rozumie się przez to rozporządzenie 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),

14) **SIECI PUBLICZNEJ** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 100, poz. 1024),

15) **SIECI TELEKOMUNIKACYJNEJ** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2016 poz. 1489 z późn. zm.),

16) **SERWISANCIE** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego i oprogramowania,

17) **SYSTEMIE INFORMATYCZNYM ADMINISTRATORA DANYCH** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

18) **TELETRANSMISJI** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

19) **USTAWIE** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922),

20) **UWIERZYTELNIANIU** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

21) **UŻYTKOWNIKU** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

§ 3

Administrator Danych Osobowych o nazwie: **Centrum Kształcenia Prymus Edyta Sawicka**, nie wyznacza **Administratora Bezpieczeństwa Informacji** celem nadzorowania i przestrzegania zasad ochrony, o których mowa w USTAWIE z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. **Upoważnienie dla Administratora Bezpieczeństwa Informacji**, oraz zakres obowiązków określa **ZAŁĄCZNIK NR 1** do „Polityki Bezpieczeństwa".

§ 4

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **ZAŁĄCZNIK NR 2** do „Polityki Bezpieczeństwa".

§ 5

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi wraz z przepływem danych pomiędzy poszczególnymi systemami określa **ZAŁĄCZNIK NR 3** do „Polityki Bezpieczeństwa".

§ 6

W podmiocie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 7

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych Osobowych. Administrator Danych Osobowych** stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Osobom, które nie przetwarzają danych osobowych, ale mają dostęp do obszaru przetwarzania danych osobowych, **Administrator Danych Osobowych** wydaje **zgody na przebywanie w obszarze przetwarzania – ZAŁĄCZNIK NR 4** do „Polityki Bezpieczeństwa". **Administrator Danych Osobowych** nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **ZAŁĄCZNIK NR 5** do „Polityki Bezpieczeństwa". Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych, oraz przebywania w obszarze przetwarzania w podmiocie – **ZAŁĄCZNIK NR 6** do „Polityki Bezpieczeństwa".
2. Zestawienie danych osobowych - kiedy i przez kogo zostały do zbioru wprowadzone, oraz komu są przekazywane – **ZAŁĄCZNIK NR 7** do „Polityki Bezpieczeństwa".
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – **ZAŁĄCZNIK NR 8** do „Polityki Bezpieczeństwa".

§ 8

Administrator Danych Osobowych 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. Wzór umowy powierzenia danych osobowych określa **ZAŁĄCZNIK NR 9** do „Polityki Bezpieczeństwa".
Jeżeli **Administrator Danych Osobowych** nie powierza danych osobowych innemu podmiotowi, ale istnieją przesłanki na okoliczność zobowiązania drugiej strony do konieczności zachowania powziętych informacji

w tajemnicy, stosuje się klauzulę poufności. Wzór klauzuli poufności określa **ZAŁĄCZNIK NR 10**.

§ 9

Na wniosek osoby, której dane dotyczą, **Administrator Danych Osobowych** jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji. Poza tym, Administrator Danych Osobowych w związku z art. 24 ust. 1, art. 25 ust. 1 i art. 32 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016 roku poz. 922) jest zobowiązany spełniać **obowiązek informacyjny**, którego treść określa **ZAŁĄCZNIK NR 11** do „Polityki Bezpieczeństwa".

§ 10

Administrator Danych Osobowych 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.

§ 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.**

§ 13

DEKLARACJA INTENCJI, CELE I ZAKRES POLITYKI BEZPIECZEŃSTWA

1. Administrator Danych Osobowych 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 w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

5. Celem Polityki bezpieczeństwa jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem 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 zmieniającym się 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 Osobowych** 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 niezbędne dokumenty wynikające z zapisów ustawy, oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

Administrator Danych Osobowych

Edyta Sawicka

.....

Podpis

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych Osobowych – **Centrum Kształcenia Prymus Edyta Sawicka**
w osobie: **Edyta Sawicka** dnia **23-05-2018r**

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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym" zwany dalej „instrukcją". Zapisy tego dokumentu wchodzą w życie z dniem 23-05-2018r .

Ilekroć w „Instrukcji" jest mowa o:

1. **PODMIOCIE** — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową,
2. **USTAWIE** — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922 z późn. zm.), zwaną dalej „ustawą",
3. **IDENTYFIKATORZE UŻYTKOWNIKA** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
4. **HAŚLE** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
5. **SIECI TELEKOMUNIKACYJNEJ** — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (Dz. U. z 2016r., poz. 1489 z późn. zm.),
6. **SIECI PUBLICZNEJ** — rozumie się przez to termin, który przywołuje § 2 ust. 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. z 2004r. Nr 100, poz. 1024),
7. **TELETRANSMISJI** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
8. **ROZLICZALNOŚCI** — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
9. **INTEGRALNOŚCI DANYCH** — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
10. **RAPORCIE** — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
11. **POUFNOŚCI DANYCH** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
12. **UWIERZYTELNIANIU** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

W podmiocie o nazwie: **Centrum Kształcenia Prymus Edyta Sawicka**, za przestrzeganie zapisów „instrukcji" odpowiedzialny jest **Administrator Danych** lub zgodnie z zapisem §3 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji.**

§ 2

W związku z tym, że w podmiocie o nazwie: **Centrum Kształcenia Prymus Edyta Sawicka** przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych Osobowych. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

   w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
   - poprzez zainstalowanie programu antywirusowego o nazwie: .....,
   - poprzez zainstalowanie firewall (zapora sieciowa),
   - poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem,
2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień.

4. Kopie zapasowe:

   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym: **Sekretariat**, zaopatrzonym w system alarmowy.

   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, 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 administratora danych.

§ 3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

   a) daty pierwszego wprowadzenia danych do systemu,

   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,

   d) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

   e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w §7 ust. 1 pkt 1,2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w §7 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024).

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w §7 ust. 1 pkt. 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024), mogą być realizowane w jednym z nich,

lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 minut, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§ 5

Administrator Bezpieczeństwa Informacji, o ile jest wyznaczony, ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§ 6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **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.**

Administrator Danych Osobowych

Centrum Kształcenia Prymus
Edyta Sawicka
ul. Dąbrowska 15, 99-235 Pęczniew
tel. 601 143 456 e-mail: ckprymus@op.pl
NIP 828-100-74-51 regon 730940198

.....

Podpis

TREŚĆ OBOWIĄZKU INFORMACYJNEGO ADMINISTRATORA DANYCH OSOBOWYCH

Centrum Kształcenia Prymus Edyta Sawicka ul. Dąbrowska 15, 99-235 Pęczniew

reprezentowanym przez:

Edytę Sawicką

Zgodnie z art. 24 ust. 1 i art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) informuję, iż administratorem Pani/Pana danych osobowych jest **Centrum Kształcenia Prymus Edyta Sawicka** Pani/Pana dane osobowe przetwarzane będą w celu np. przeprowadzenia postępowania rekrutacyjnego na wolne stanowisko pracy np. nauczyciela. Pana/Pani dane osobowe nie będą udostępniane innym odbiorcom danych za wyjątkiem wypadków obowiązkowego udzielenia informacji określonych w przepisach szczególnych. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania. Podaje Pani/Pan swoje dane osobowe dobrowolnie.

WYJAŚNIENIE CZYM JEST OBOWIĄZEK INFORMACYJNY

Co to jest obowiązek informacyjny?

Obowiązek informacyjny powinien spełniać administrator danych osobowych - w różnych sytuacjach oczywiście. Wynika to wprost z przepisów ustawy o ochronie danych osobowych (podstawowy przepis poniżej):

Art. 24. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1. *adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;*
2. *celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;*
3. *prawie dostępu do treści swoich danych oraz ich poprawiania;*
4. *dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.*

Poza tym, zgodnie z art. 32 ustawy o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) każdy ma prawo do kontroli przetwarzania danych osobowych tej osoby, której dane dotyczą i może złożyć do administratora danych osobowych zapytanie w formie wniosku o udzielenie informacji, od kiedy dane osobowe są przetwarzane oraz w jakim zakresie.
Ustawa nie określa w jakiej formie obowiązek informacyjny powinien być spełniany: czy w formie ustnej czy pisemnej. Administrator Danych Osobowych powinien, wtedy kiedy to jest wymagane, spełnić ten obowiązek jeszcze przed rozpoczęciem procesu przetwarzania danych.

Obowiązek informacyjny powinien być wypełniany dwutorowo:

- kiedy placówka pobiera dane w innym celu, niż cel wynikający z innych przepisów szczególnych np.: wykonywania zadań publicznych rozumianych wąsko. Przykładem, kiedy obowiązek

informacyjny trzeba będzie spełnić to: rekrutacja na konkretne stanowisko pracy, przeprowadzanie konkursów itd. Konieczność stosowania obowiązku informacyjnego zaistnieje głównie wtedy, kiedy placówka/przedsiębiorstwo będzie musiało pobierać zgodę na przetwarzanie danych osobowych tej konkretnej osoby.

- z drugiej strony obowiązek informacyjny powinien być spełniany w stosunku do osób, które korzystają z uprawnienia wynikającego z art. 32 ustawy o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) – informacje powyżej.

Przykład wymagalności obowiązku informacyjnego:

Prowadzenie postępowania rekrutacyjnego:

Treść obowiązku informacyjnego powinna znajdować się w zamieszczonej przez jednostkę samorządu terytorialnego, jednostkę organizacyjną samorządu terytorialnego, przedsiębiorstwo - ofercie pracy. Ustawa o ochronie danych osobowych nie narzuca formy spełnienia obowiązku informacyjnego, ale z kolei zobowiązuje do poinformowania w tym trybie przed rozpoczęciem procesu przetwarzania danych osobowych. Ze względów praktycznych należy zamieszczać klauzulę obowiązku informacyjnego w samej treści oferty, podobnie jak informację, że bez klauzuli wyrażenia zgody na przetwarzanie danych osobowych, aplikacje nie będą rozpatrywane. Placówka musi dochować należytej staranności w zakresie czytelności i klarowności treści obowiązku informacyjnego, tak, by treść rzeczywiście nie budziła żadnych wątpliwości. Treść obowiązku informacyjnego powinna być w dostateczny sposób wyodrębniona spośród innych informacji przekazywanych w ofercie potencjalnemu kandydatowi do pracy na stanowisko, co do którego rozpoczyna się procedurę naboru.

Centrum Kształcenia Prymus
Edyta Sawicka
ul. Dąbrowska 15, 99-235 Pęczniew
tel. 601 143 456 e-mail: ckprymus@op.pl
NIP 828-100-74-51 regon 73094019

Poddębice, dn. 23.05.2018r

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI ORAZ ZAKRES OBOWIĄZKÓW

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3 Polityki Bezpieczeństwa z dnia **23.05.2018** zgodnie z założeniami
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

Na podstawie art. 36a ust. 1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2016 r. poz. 922 z późn. zm.)

Administrator Danych Osobowych (ADO): ***Centrum Kształcenia Prymus Edyta Sawicka***

o numerze NIP: ***8281007451***

powołuje / potwierdza powołanie **([1])**:

w osobie ***Edyta Sawicka***

Administratora Bezpieczeństwa Informacji (ABI): ***Małgorzata Nowak***

o numerze Pesel: ***89121206023***

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia przez **Administratora Danych Osobowych.**

Zgodnie z art. 36a ust. 2 **do zadań ABI należy**:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych,
2. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 u.o.d.o., zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 u.o.d.o. zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji nadzoruje opracowanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2 u.o.d.o., oraz przestrzegania zasad w niej określonych. Jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. **Administrator Bezpieczeństwa Informacji** prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie, a w szczególności:

zgodnie z § 4. „Polityki Bezpieczeństwa"

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

([1]) niepotrzebne usunąć

osobowe, który określa załącznik do „Polityki Bezpieczeństwa" nr 2,

zgodnie z § 5. „Polityki Bezpieczeństwa"

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa" nr 3,

zgodnie z § 6. „Polityki Bezpieczeństwa"

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa" nr 4,

zgodnie z § 8. „Polityki Bezpieczeństwa"

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie oraz posiadających upoważnienie do przebywania w obszarze przetwarzania - załącznik nr 6 do „Polityki Bezpieczeństwa" oraz zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – załącznik nr 7 do „Polityki Bezpieczeństwa".

Administrator Bezpieczeństwa Informacji sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla Administratora Danych Osobowych, lub na wniosek GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator Danych Osobowych zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji - niezbędne do należytego wykonywania przez niego zadań wynikających z niniejszego upoważnienia i przepisów ustawy.

OŚWIADCZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako **Administrator Bezpieczeństwa Informacji**, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie o nazwie: **Centrum Kształcenia Prymus Edyta Sawicka**, zgodnie z obowiązkami wynikającymi z tego upoważnienia, oraz ustawy o ochronie danych osobowych.

Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko **Administratora Bezpieczeństwa informacji** tj.:

- nie byłem(am) karany(a) za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych, oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Danych Osobowych

Podpis

Administrator Bezpieczeństwa Informacji

Centrum Kształcenia Prymus
Edyta Sawicka
ul. Dąbrowska 15, 99-235 Pęczniew
tel. 601-143-456 e-mail: prymus@op.pl
NIP 828-100-74-51 regon 730940198

Podpis

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Załącznik do „Polityki Bezpieczeństwa" nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

LP.	DOKŁADNY ADRES (NP. ADRES SIEDZIBY FIRMY GDZIE PRZETWARZANE SĄ DANE)	DZIAŁ UŻYTKUJĄCY POMIESZCZENIE	NR POKOJU LUB POMIESZCZENIA	RODZAJ ZASTOSOWANEGO ZABEZPIECZENIA POMIESZCZENIA	UWAGI
1.	**Centrum Kształcenia Prymus Edyta Sawicka, ul. Polna 34, 99-200 Poddębice**	Gabinet Dyrektora	Nie dotyczy	Drzwi zamykane na klucz, szafy zamykane na klucz, fizyczne zabezpieczenia budynku	Brak
		Sekretariat			
		sale dydaktyczne			

Data i podpis Administratora Danych Osobowych

23.05.2018 r. ..... E Sawicka .....

ZAŁĄCZNIK NR 3 DO POLITYKI BEZPIECZEŃSTWA:

- **WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH** zgodnie z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004
- **OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI** zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
1.	**AKTA OSOBOWE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, PESEL, DANE TELEADRESOWE, OBYWATELSTWO, STAN RODZINY, NIP, OŚWIADCZENIA, UPOWAŻNIENIA, ORZECZENIA	WERSJA PAPIEROWA	
2.	**DANE PRACOWNICZE KADROWO-PŁACOWE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, PESEL, DANE TELEADRESOWE, STAN RODZINY, NIP, OŚWIADCZENIA, WYNAGRODZENIA, BYŁE MIEJSCA PRACY, NR KONTA, NR EWIDENCYJNY PRACOWNIKA	WERSJA PAPIEROWA	
3.	**DOKUMNETACJA NABORU UCZESTNIKÓW SZKOLEŃ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, DANE TELEADRESOWE, DATA URODZENIA, PESEL, IMIONA I NAZWISKA RODZICÓW, ADRES, TELEFON, INFORMACJA O ZDROWIU, INFORMACJA O NIEPEŁNOSPRAWNOŚCI,	WERSJA PAPIEROWA	
4.	**POCZTOWA KSIĄZKA NADAWCZA**	WERSJA TRADYCYJNA (PAPIEROWA)	DATA, NADANY NUMER, OD KOGO DO KOGO, TREŚĆ	WERSJA PAPIEROWA	
5.	**DZIENNIKI ZAJĘĆ POZALEKCYJNYCH**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, DANE TELEADRESOWE, DATA URODZENIA,	WERSJA PAPIEROWA	
6.	**REJESTR FAKTUR ZAKUPU LUB KSEROKOPIE FAKTUR ZAKUPU**	WERSJA TRADYCYJNA (PAPIEROWA)	DATA, DANE KONTRAHENTA, KWOTA,	WERSJA PAPIEROWA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
7.	**REJESTR WYDANYCH ZAŚWIADCZEŃ LUB KSEROKOPIE WYDANYCH ZAŚWIADCZEŃ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, DATA, CEL ZAŚWIADCZENIA	WERSJA PAPIEROWA	
8.	**UMOWY CYWILNOPRAWNE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	DATA, MIEJSCE, DANE KONTRAHENTA, TREŚĆ UMOWY	WERSJA PAPIEROWA	

Data i podpis Administratora Danych Osobowych

23.05.18 .....

ZGODA NA PRZEBYWANIE
W OBSZARZE PRZETWARZANIA DANYCH

Załącznik nr 4 do Polityki Bezpieczeństwa

Na podstawie zapisów 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. z 2004 r. Nr 100, poz. 1024 z późn. zm.), a także na podstawie zapisów ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2016r. poz. 922 z późn. zm.):

DATA NADANIA ZGODY: ***23-05-2018r***

ADMINISTRATOR DANYCH OSOBOWYCH: **Centrum Kształcenia Prymus Edyta Sawicka**

O NUMERZE NIP: ***8281007451***

W OSOBIE: ***Edyta Sawicka***

wyraża zgodę Pani/Panu:

IMIĘ I NAZWISKO: ***Małgorzata Nowak***

PESEL: ***89121206023***

STANOWISKO SŁUŻBOWE: ***Kierownik biura***

CZAS TRWANIA ZGODY: ***DO USTANIA STOSUNKU PRACY***

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych. Jednocześnie zobowiązuję ww. osobę do zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w pomieszczeniach, co do których uzyskał (a) zgodę na przebywanie.

Zobowiązuję się do zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w pomieszczeniach, co do których uzyskałem (am) zgodę na przebywanie.	
23.05.18 r. ..... (data i podpis osoby upoważnionej do przebywania w obszarze przetwarzania danych)	Centrum Kształcenia Prymus *Edyta Sawicka* ul. Dąbrowska 15, 99-235 Pęczniew tel. 601 143 456 e-mail: ckprymus@op.pl NIP 828-100-74-51 regon 730940198 23.05.18r. ..... (data, podpis i pieczęć Administratora Danych Osobowych)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Załącznik nr 5 do „Polityki Bezpieczeństwa"
zgodnie z Art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Administrator Danych Osobowych – **Centrum Kształcenia Prymus Edyta Sawicka**
w osobie: **Edyta Sawicka**
dnia **23.05.2018r.** nadaje upoważnienie do przetwarzania danych osobowych, dla:

IMIĘ I NAZWISKO:	**Małgorzata Nowak**
NR PESEL:	**89121206023**
STANOWISKO SŁUŻBOWE:	**Kierownik biura**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z:

- **POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH**
- **ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY**

Upoważnienie nadaje się do ustania stosunku pracy. Wszelakie poprzednie upoważnienia do przetwarzania danych osobowych z dniem wprowadzenia niniejszego wygasają. Jednocześnie bieżące upoważnienie zostaje zawieszone w przypadku nieobecności / urlopu przekraczającego 30 dni kalendarzowych. Po upływie w/w okresu nieobecności / urlopu upoważniony(a) wykonując obowiązki wynikające z upoważnienia otrzymuje ponowne upoważnienie niniejszym dokumentem w trybie automatycznym.

Ja niżej podpisany/a zobowiązuję się do przestrzegania zasad panujących w w/w podmiocie w zakresie ochrony danych osobowych, a w szczególności **„Polityki Bezpieczeństwa"** i **„Instrukcji Zarządzania Systemem Informatycznym"** oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Zobowiązuję się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w w/w podmiocie oraz sposobów zabezpieczeń, a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Przyjąłem do wiadomości, iż jestem zobligowany do zmiany hasła dostępu do stanowiska pracy (komputera) w terminie co 30 dni kalendarzowych. Hasło musi być niepowtarzalne względem wcześniejszego, oraz składać się z 8 znaków (w tym małe, duże litery oraz znak specjalny np.: **„REF#gospodarka"** ; **„Kardex2015"** itd...).

Oświadczam, iż zapoznałem(am) się i akceptuję zasady dotyczące korzystania z sieci informatycznej na terenie w/w podmiotu, a mianowicie:

1. Mając na uwadze wysoką sprawność oraz elastyczność kształtowania procesów w pracy, pracodawca zastrzega sobie prawo do archiwizacji, monitorowania oraz przekierowywania służbowej poczty elektronicznej.
2. Pracodawca informuje, że wszystkie połączenia internetowe wykonane w sieci w/w podmiotu są rejestrowane, zgodnie z wymogami ustawy Prawa Telekomunikacyjnego.
3. Pracodawca zastrzega sobie również prawo monitorowania w/w połączeń oraz żądania wyjaśnień w zakresie realizowanej przez pracownika aktywności w sieci oraz do dowolnego kształtowania zakresu dostępu do sieci internetowej.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016r. poz. 922 z późn. zm.) 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. Nr 100, poz. 1024 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

E. Sawicka

[czytelny podpis Administratora Danych Osobowych]

Nowak

[czytelny podpis upoważnionego]

EWIDENCJA OSÓB POSIADAJĄCYCH UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ PRZEBYWANIA W OBSZARZE PRZETWARZANIA

Załącznik nr 6 do „Polityki Bezpieczeństwa" zgodnie z Art. 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

* (z uwzględnieniem osób nieprzetwarzających dane osobowe, ale przebywających w pomieszczeniach, w których zachodzi proces przetwarzania danych osobowych)

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
1.	Małgorzata Nowak	Kierownik biura	**PRZETWARZANIE / PRZEBYWANIE**	23.05.2018r.	DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	

ADMINISTRATOR DANYCH OSOBOWYCH

23.05.18. .....

(data i czytelny podpis Administratora Danych Osobowych)

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Załącznik do „Polityki Bezpieczeństwa" nr 8 zgodnie z § 4 pkt 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. ABI wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

5. Środki ochrony, zastosowane przez ABI dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   - środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
   - środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);
   - środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym);

6. Zastosowane środki:

ŚRODKI OCHRONY FIZYCZNEJ DANYCH:

a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi).

b) Pomieszczenia, w których przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.

c) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.

d) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.

e) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.

f) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie, lub kasie pancernej.

g) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.

h) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.

i) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie, lub kasie pancernej.

j) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

k) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

7. ŚRODKI OCHRONY TECHNICZNEJ DANYCH:

a) Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.

b) Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

c) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

d) Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.

e) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

f) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

g) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

h) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

i) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

j) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

k) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

l) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

8. ŚRODKI ORGANIZACYJNE:

a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.
W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

ADMINISTRATOR DANYCH OSOBOWYCH

23.05.18. .....

(data i czytelny podpis Administratora Danych Osobowych)

KLAUZULA POUFNOŚCI INFORMACJI

Załącznik nr 10 do Polityki Bezpieczeństwa

§ 1

Małgorzata Nowak, Pesel: 89121206023 powinna zachować poufność informacji, które zdobędzie na każdym etapie współpracy z **Edytą Sawicką**

§ 2

Klauzula poufności względem przetwarzanych danych osobowych obowiązuje **Małgorzatę Nowak** przez okres trwania umowy macierzystej**, a także bezwzględnie po jej zakończeniu przez okres **10** lat.

§ 3

Małgorzata Nowak zobowiązuje się do wykorzystywania przetwarzanych danych osobowych, w ramach realizacji umowy macierzystej** z dnia **01.04.2011**, wyłącznie w celach określonych w tejże umowie.

§ 4

Małgorzata Nowak zobowiązuje się do przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922)

§ 5

W przypadku nie dochowania warunków umowy, **Edyta Sawicka** zastrzega sobie prawo rozwiązania umowy macierzystej** z dnia **01.04.2011** w trybie natychmiastowym.

Nowak

.....

[czytelny podpis strony umowy]

* osoba zatrudniona na umowę zlecenia/o dzieło
**umowa zlecenie/o dzieło/ współpracy

ZARZĄDZENIE WEWNĘTRZNE NR 1/05/2018 Z DNIA 23-05-2018r.

Administratora Danych Osobowych: Centrum Kształcenia Prymus Edyta Sawicka w osobie: Edyta Sawicka w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,

w związku z zapisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) 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. z 2004 r. Nr 100, poz. 1024)

zarządza się, co następuje:

§1

Wprowadza się w podmiocie: **Centrum Kształcenia Prymus Edyta Sawicka** Politykę Bezpieczeństwa" oraz „Instrukcję Zarządzania Systemem Informatycznym".

§2

Zarządzenie jest adresowane do pracowników podmiotu: **Centrum Kształcenia Prymus Edyta Sawicka,** wykonujących czynności określone w „Polityce Bezpieczeństwa" oraz „Instrukcji Zarzadzania Systemem Informatycznym". Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią „Polityki Bezpieczeństwa" i „Instrukcji Zarządzania Systemem Informatycznym".

§3

Administrator Danych Osobowych: Centrum Kształcenia Prymus Edyta Sawicka: Edyta Sawicka zobowiązuje wszystkich pracowników do przestrzegania zapisów „Polityki Bezpieczeństwa" oraz stosowania się do „Instrukcji Zarządzania Systemem Informatycznym" pod groźbą konsekwencji służbowych, przewidzianych prawem.

§4

Niniejsze zarządzenie wchodzi w życie z dniem podpisania i ogłoszenia tj. z dniem **23-05-2018r**.

.....
(podpis Administratora Danych Osobowych)

Szczegółowe informacje o wybranej instytucji szkoleniowej

Instytucja szkoleniowa:	**Centrum Kształcenia Prymus Edyta Sawicka**
Numer ewidencyjny:	2.10/00100/2008
Status:	Aktywny
Data wpisu:	2008-10-17
Rok kontynuacji działalności:	2022
Numer REGON:	730940198
Numer NIP:	8281007451
Instytucja zagraniczna:	NIE
Adres:	ul. Dąbrowska 15, 99-235 Pęczniew, łódzkie
Numer telefonu:	601143456
Numer faxu:	
E-mail:	sekretariat@ckprymus.pl
Strona www:	www.ckprymus.pl

Dane dotyczące wpisu do rejestru

Numer ewidencyjny:	2.10/00100/2008
Data wpisu:	2008-10-17
Data wydania zaświadczenia:	2010-03-29
Odebrano zaświadczenie:	TAK

Siedziba główna i oddziały instytucji szkoleniowej

Nazwa	Rok powstania	Siedziba główna
Centrum Kształcenia Prymus Edyta Sawicka	2003	TAK

Zarządzenie nr 01/2019

Centrum Kształcenia Prymus Edyta Sawicka

z dnia 25.11.2019 r.

w sprawie wprowadzenie Regulaminu Reklamacji Usług Szkoleniowych

§ 1

Wprowadzam jako obowiązujący w Centrum Kształcenia Prymus Edyta Sawicka „Regulamin Reklamacji Usług Szkoleniowych" stanowiący załącznik nr 1 do niniejszego zarządzenia.

§ 2

Regulamin podany jest do wiadomości publicznej przez opublikowanie na stronie internetowej www.ckprymus.pl

§ 3

Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązywania od 25.11.2019 r.

Centrum Kształcenia Prymus
Edyta Sawicka
ul. Dąbrowska 15, 99-235 Pęczniew
tel. 601 143 456 e-mail: ckprymus@op.pl
NIP 828-180-74-51 regon 730940198

ZARZĄD POWIATU
w Poddębicach
ul. Łęczycka 16
99-200 Poddębice
tel. 678 33 72, fax 6782701
O.K. 4321/1/2003

Poddębice, 20.02.2003 r.

ZAŚWIADCZENIE

o wpisie do ewidencji szkół i placówek niepublicznych

Na podstawie art. 82 ust. 3 i 3a Ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 1996 r. Nr 67 poz. 329, Nr 106 poz. 496, z 1997 r. Nr 28 poz. 153, Nr 141 poz. 943, z 1998 r. Nr 117 poz. 759, Nr 162 poz. 1126, z 2000 r. Nr 12 poz. 136, Nr 19 poz. 239, Nr 48 poz. 550 i Nr 104 poz. 1104, Nr 122 poz. 1320, Nr 120 poz. 1268, z 2001 r. Nr 11 poz. 1194, Nr 144 poz. 1615, z 2002 r. Nr 41 poz. 362, Nr 141 poz. 1185, Nr 113 poz. 984) zaświadcza się, że do ewidencji szkół i placówek niepublicznych Powiatu Poddębickiego dokonano w dniu 20 lutego 2003 r. pod numerem 7/2003

następującego wpisu:

1. Zarząd Powiatu w Poddębicach
   (nazwa organu, który dokonał wpisu do ewidencji szkoły lub placówki)
2. 20 lutego 2003 r.; Nr 7/2003
   (data i numer wpisu do ewidencji)
3. Centrum Kształcenia Kursowego *„PRYMUS”*
   placówka pracy pozaszkolnej
   (nazwa i typ szkoły lub placówki)
4. Edyta Sawicka – ul. Dąbrowska 28, 99 -235 Pęczniew
   (osoba prawna lub fizyczna prowadząca szkołę lub placówkę-jej adres)
5. ul. Polna 13/15, 99 – 200 Poddębice
   (adres szkoły lub placówki)
6. ---
   (nazwa zawodu lub profilu kształcenia zawodowego w przypadku szkoły prowadzącej kształcenie zawodowe)

Wpis do ewidencji podlega wykreśleniu w przypadku stwierdzenia naruszenia przepisów określonych w art. 83 ust. 1 cytowanej wyżej ustawy.

Za zgodność z oryginałem
STAROSTWO POWIATOWE
w Poddębicach
ul. Łęczycka 16, 99-200 Poddębice
tel. 6782805, fax 678270

Z-ca Kierownika
Wydziału Zdrowia, Pomocy
Społecznej, Oświaty i Kultury
Dorota Kubiak

STAROSTA
mgr inż. Ryszard Rytter

Otrzymują:
1. Edyta Sawicka
2. Kuratorium Oświaty – Delegatura w Sieradzu
3. Urząd Skarbowy w Poddębicach
4. a/a

STAROSTA PODDĘBICKI
ul. Łęczycka 16
99-200 Poddębice
tel. 43 678-28-05, 678-78-16
fax 678-27-01

Poddębice, dn.08.02.2013 r.

ZAŚWIADCZENIE

o zmianie wpisu do ewidencji szkół i placówek niepublicznych

Na podstawie art. 82 ust.3, 3a i 5 Ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256 poz. 2572 z póź. zm.) zaświadcza się, że pod numerem 7/2003 w ewidencji szkół i placówek niepublicznych na wniosek Edyty Sawickiej - jako osoby prowadzącej Centrum Kształcenia Kursowego „Prymus" w Poddębicach, dokonano w dniu 08 lutego 2013r. następującej zmiany:

W punkcie 3: **nazwa oraz odpowiednio typ i rodzaj szkoły lub placówki**:
„ Centrum Kształcenia Kursowego „PRYMUS"
placówka pracy pozaszkolnej"

Wpisano nowe brzmienie:
„Centrum Kształcenia Prymus
placówka kształcenia ustawicznego"

W punkcie 5: **adres szkoły lub placówki:**
„ul. Polna 13/15, 99-200 Poddębice"

Wpisano nowe brzmienie:
„ul. Polna 34, 99-200 Poddębice

Za zgodność z oryginałem

STAROSTWO POWIATOWE
w Poddębicach
ul. Łęczycka 16, 99-200 Poddębice
tel. 6782806, 6782805, fax 678270

STAROSTA
Ryszard Ryter
.....
(pieczęć i podpis osoby upoważnionej)

Zastępca Naczelnika
Wydziału Zdrowia, Pomocy
Społecznej, Oświaty i Kultury
Dorota Kubiak

Otrzymują:
1. Zgłaszający - Edyta Sawicka, ul. Dąbrowska 15, 99-235 Pęczniew
2. Łódzki Kurator Oświaty w Łodzi, Delegatura w Sieradzu
3. Naczelnik Urzędu Skarbowego w Poddębicach

OZ.4330.6.2019 Poddębice, dn. 26.11.2019 r.

ZAŚWIADCZENIE

o zmianie wpisu do ewidencji szkół i placówek niepublicznych

Na podstawie art. 168 ust. 9, 11 i 13 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2019 r. poz. 1148, 1078, 1287, 1680, 1681, 1818) zaświadcza się, że w ewidencji szkół i placówek niepublicznych prowadzonej przez Starostę Poddębickiego na wniosek Pani Edyty Sawickiej – jako osoby prowadzącej Centrum Kształcenia „Prymus" w Poddębicach wpisane do ewidencji pod numerem 7/2003 dokonano w dniu 26.11.2019r. następującej zmiany:

W punkcie 3 (nazwa i typ szkoły lub placówki):

nazwa - „Centrum Kształcenia Prymus
typ - „Placówka kształcenia ustawicznego"

wpisano nowe brzmienie:

nazwa - „Centrum Kształcenia Ustawicznego Prymus w Poddębicach"
typ - „Centrum Kształcenia Ustawicznego"

STAROSTA
Małgorzata Komajda
.....
(pieczęć i podpis osoby upoważnionej)

Otrzymują:
1. Zgłaszający: Edyta Sawicka, ul. Dąbrowska 15, 99-235 Pęczniew
2. Łódzki Kurator Oświaty w Łodzi, Delegatura w Sieradzu, Plac Wojewódzki 3, 98-200 Sieradz
3. Naczelnik Urzędu Skarbowego w Poddębicach, ul. Narutowicza 12, 99-200 Poddębice
4. a/a

STAROSTA PODDĘBICKI
ul. Łęczycka 16
99-200 Poddębice
tel. 43 678-28-05, 678-78-16
fax 678-27-01

OZ.4330.1.2020

Poddębice, 17.04.2020 r.

ZAŚWIADCZENIE

o zmianie wpisu do ewidencji szkół i placówek niepublicznych

Na podstawie art. 168 ust. 9, 11 i 14 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2019 r. poz. 1148, 1078, 1680, 1681, 1818, 2197, 2248; z 2020 poz. 374) zaświadcza się, że w ewidencji szkół i placówek niepublicznych prowadzonej przez Starostę Poddębickiego na wniosek Pani Edyty Sawickiej – jako osoby prowadzącej placówkę pn. Centrum Kształcenia Ustawicznego „Prymus" " w Poddębicach wpisaną do ewidencji pod numerem 7/2003 w dniu 17.04.2020r. dokonano zmiany wpisu w zakresie nazwy placówki:

W punkcie 2 o brzmieniu:

„ Nazwa szkoły lub placówki: Centrum Kształcenia Ustawicznego „Prymus" w Poddębicach"

wpisano nowe brzmienie:

„ Nazwa szkoły lub placówki: Centrum Kształcenia „Prymus" w Poddębicach"

STAROSTA
Małgorzata Komajda

.....

(pieczęć i podpis osoby upoważnionej)

Otrzymują:
1. Zgłaszający: Edyta Sawicka, ul. Dąbrowska 15, 99-235 Pęczniew
2. Łódzki Kurator Oświaty w Łodzi, Delegatura w Sieradzu, Plac Wojewódzki 3, 98-200 Sieradz
3. Naczelnik Urzędu Skarbowego w Poddębicach, ul. Narutowicza 12, 99-200 Poddębice
5. a/a

Poddębice, 18.10.2022 r.

Zespół Szkół Ponadpodstawowych
w Poddębicach
ul. Polna 13/15
99-200 Poddębice

Centrum Kształcenia
Prymus Edyta Sawicka
ul. Polna 34
99-200 Poddębice

Referencje

W związku z realizacją projektu „Branżowy sukces" współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020 z zakresu organizacji szkoleń mających na celu podniesienie umiejętności i kompetencji zawodowych nauczycieli Centrum Kształcenia Prymus Edyta Sawicka przeprowadziło następujące szkolenia pn:

1. Kurs barmański w wymiarze 50 godzin (termin: 24.08.2022 r. – 01.09.2022 r.)
2. Kurs projektowania wnętrz hotelowych w wymiarze 50 godzin (termin: 23.08.2022 r.-29.08.2022 r.)

Współpraca z Centrum Kształcenia Prymus Edyta Sawicka układała się bardzo sprawnie i przebiegała w miłej atmosferze.

Szkolenia zostały przeprowadzone profesjonalnie, bez żadnych zastrzeżeń ze strony uczestników.

Centrum Kształcenia Prymus Edyta Sawicka w pełni wywiązało się z zawartej umowy. Jest to firma reprezentująca wysoki poziom usług, godna zaufania oraz polecenia przyszłym klientom.

KOORDYNATOR PROJEKTU
mgr Bożena Kołodziejek