POLITYKA BEZPIECZEŃSTWA

Administrator Danych Osobowych – **ZESPÓŁ SZKÓŁ W BYSTRZEJOWICACH PIERWSZYCH IM. HELENY BABISZ** w osobie dyrektora **AGNIESZKI WILKOŁEK** dnia **14-06-2017r.**

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 **14-06-2017r.**

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: **ZESPÓŁ SZKÓŁ W BYSTRZEJOWICACH PIERWSZYCH IM. HELENY BABISZ** 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: **ZESPÓŁ SZKÓŁ W BYSTRZEJOWICACH PIERWSZYCH IM. HELENY BABISZ** 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

.....
Podpis

Administrator Bezpieczeństwa Informacji

.....
Podpis