****

***ZESPÓŁ PLACÓWEK OŚWIATOWYCH***

***IM. PAPIEŻA JANA PAWŁA II***

***W DYLEWIE***

**POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE OCHRONY DANYCH OSOBOWYCH**

**W ZESPOLE PLACÓWEK OŚWIATOWYCH**

**IM. PAPIEŻA JANA PAWŁA II**

**W DYLEWIE**

SPIS TREŚCI 2

1. Wstęp 3

1.1. Informacje ogólne 3

1.2. Cel przygotowania polityki bezpieczeństwa 3

2. Polityka Bezpieczeństwa Informacji w zakresie ochrony danych osobowych 4

2.1. Zakres informacji objętych polityką bezpieczeństwa oraz zakres zastosowania 4

2.2 Wyjaśnienie terminów używanych w dokumencie polityki bezpieczeństwa 6

2.3. Wykaz budynków, w których przetwarzane są dane osobowe 7

2.4. Wykaz miejsc w których przetwarzane są dane osobowe 8

2.5. Wykaz zbiorów danych przetwarzanych w systemach informatycznych

wraz ze wskazaniem programów stosowanych do przetwarzania tych danych 9

2.6. Opis struktury zbiorów danych wskazujący zawartość pól informacyjnych

i powiązania między poszczególnymi polami informacyjnymi 9

2.7 Zbiory danych przetwarzanych tradycyjnie 10

2.8. Sposób przepływu danych osobowych pomiędzy systemami informatycznymi 11

2.9. Środki techniczne i organizacyjne zapewniające bezpieczeństwo w przetwarzaniu

danych 11

2.10. Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych

osobowych 12

2.11. Zasady udzielania dostępu do danych osobowych 13

2.12. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej. 14

2.13. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach

informatycznych 14

2.14. Analiza ryzyka związanego z przetwarzaniem danych osobowych 14

**1. WSTĘP**

1.1. INFORMACJE OGÓLNE

Niniejszy dokument Polityki Bezpieczeństwa Informacji w zakresie ochrony danych osobowych został opracowany w celu zapewnienia zgodności przetwarzania danych osobowych z polskim ustawodawstwem. Polityka Bezpieczeństwa Informacji wraz z instrukcją zarządzania systemem informatycznym stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1 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.). Polityka Bezpieczeństwa została wdrożona zarządzeniem dyrektora i obowiązuje od dnia 1 stycznia 2015r. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą. Każda osoba mającą dostęp do danych osobowych z upoważnienia Administratora Danych Osobowych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych Osobowych. Osoby o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa Informacji oraz zobowiązały się do stosowania zawartych w niej postanowień.

1.2. CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Polityki Bezpieczeństwa informacji było zapewnienie zgodności działania Zespołu Placówek Oświatowych im. Papieża Jana Pawła II w Dylewie z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Opracowany dokument Polityki Bezpieczeństwa Informacji został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

1. Konstytucja Rzeczypospolitej Polskiej (art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Dz.U. 1997 nr 78 poz. 483).

2. Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych.

3. Dyrektywa PE i RE z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.

4. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. **(tekst jednolity: Dz. U. 2014 r. poz. 1182)**

5. 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. z 2004 r. nr 100 poz. 1024 z późn. zm.).

6. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. 1974 nr 24 poz. 141 z późn. zm.).

7. Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. 2004 r. Nr 256 poz. 2572 z późn. zm.),

8. Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. 2002 r. Nr 23 poz. 225 z późn. zm.),

9. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (tj. Dz.U. z 2001 r. nr 128, poz. 1402 z późn. zm.).

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

**2. POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE OCHRONY DANYCH OSOBOWYCH .**

2.1. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Zespołu Placówek Oświatowych im. Papieża Jana Pawła II w Dylewie. Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Na Politykę Bezpieczeństwa składają się następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

4) sposób przepływu danych pomiędzy poszczególnymi systemami,

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Politykę Bezpieczeństwa stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Polityki Bezpieczeństwa. Rygorowi Polityki Bezpieczeństwa podlegają także dane powierzone Zespołowi Placówek Oświatowych im. Papieża Jana Pawła II w Dylewie do przetwarzania na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych oraz dane osobowe, których ZPO w Dylewie jest odbiorcą w rozumieniu ustawy o ochronie danych osobowych.

§1

W związku z dynamiką zmian w zakresie bezpieczeństwa informacji oraz mając na uwadze częste zmiany w konstrukcji systemów informatycznych, Administrator Danych świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar:

1. Podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych.
2. Stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w placówce w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych placówce danych osobowych jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodności placówki.
3. Traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby.
4. Doskonalenia i rozwijania nowoczesnych metod zabezpieczania danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych .

§2

Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych placówka dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności zapewnia aby te dane były:

1. przetwarzane zgodnie z prawem.
2. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
3. merytorycznie poprawne i adekwatne do celów dla jakich są przetwarzane.
4. przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągniecia celu przetwarzania.

§3

W placówce nie przetwarza się danych osobowych wrażliwych dotyczących:

1. pochodzenia rasowego lub etnicznego
2. poglądów politycznych
3. przekonań religijnych lub filozoficznych
4. przynależności wyznaniowej, partyjnej lub związkowej
5. stanu zdrowia, kodu genetycznego, nałogów lub życia seksualnego
6. skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

2.2 WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

§4

Ilekroć w dokumencie jest mowa o:

1) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 r. Nr 133 poz. 883 z późn. zm.), zwaną dalej „ustawą",

2) **rozporządzenie** – 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. z 2004 r. Nr 100, poz. 1024 z późn. zm.), zwane dalej „rozporządzeniem”,

3) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

4) **polityka bezpieczeństwa** – dokument polityki bezpieczeństwa w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „polityką”,

5) **instrukcja zarządzania systemem informatycznym** – dokument instrukcji zarządzania systemem informatycznym w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „instrukcją”,

6) **zbiór 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,

7) **przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

8) **system informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

9) **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole.

10) **zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

11) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

12) **Administrator Danych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych,

13) **Administrator Bezpieczeństwa Informacji** – rozumie się osobę wyznaczoną przez ADO, odpowiedzialną za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych , zwaną dalej ABI

14) **Administrator Systemów Informatycznych** – rozumie się osobę wyznaczoną przez ADO odpowiedzialną za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych przetwarzających zbiory danych osobowych, zwany dalej ASI.

15) **odbiorca danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a. osoby, której dane dotyczą,

b. osoby upoważnionej do przetwarzania danych,

c. przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,

d. podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,

e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

16) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

17) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

18) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.),

19) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne,

20) **sieć lokalna** – połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.

21) **telentransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

22**) integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

23) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

24) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

25) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

2.3 WYKAZ BUDYNKÓW, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

§5

Do przetwarzania danych osobowych dochodzi lub może dochodzić we wszystkich pomieszczeniach administracyjnych wyposażonych w służbowy komputer osobisty, które znajdują się w budynkach określonych zgodnie z poniższym zestawieniem.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Adres/ Lokalizacja** | **Uwagi** | **Zabezpieczenie** |
| Dane osobowe przetwarzane jako Administrator Danych | Zespół Placówek Oświatowych im. Papieża Jana Pawła II w Dylewie  ul. Szkolna 1  07-420 Kadzidło | sekretariat, gabinet dyrektora | kluczami dysponuje dyrektor  i sekretarka szkoły; |
| Dane osobowe przetwarzane jako Przetwarzający (na podstawie umowy powierzenia przetwarzania danych osobowych) | Zespół Placówek Oświatowych im. Papieża Jana Pawła II w Dylewie  ul. Szkolna 1  07-420 Kadzidło | sekretariat, gabinet dyrektora, pracownia komputerowa, gabinet wicedyrektora, pokój nauczycielski, sale lekcyjne (1-13), pokój nauczycieli wf, świetlica, gabinet pedagoga | Kluczami dysponuje dyrektor szkoły, sekretarka, nauczyciele (klucze dostępne są w zamykanej szafce w pokoju nauczycielskim) |
| Dane osobowe powierzone do przetwarzania Przetwarzającemu (na podstawie umowy powierzenia przetwarzania danych osobowych) | OKE,  ZUS  PZU  Kuratorium Oświaty, | sekretariat,  księgowość |  |

2.4 WYKAZ MIEJSC, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

§6

|  |  |  |
| --- | --- | --- |
| **ADRES – BUDYNEK** | **POMIESZCZENIA** | **ZABEZPIECZENIE** |
| BUDYNEK ZESPOŁU PLACÓWEK OSWIATOWYCH IM. PAPIEŻA JANA PAWŁA II  UL. SZKOLNA 1, 07-420 DYLEWO | gabinet dyrektora | kluczem dysponuje dyrektor, klucz dostępny jest w sekretariacie |
| gabinet wicedyrektora | kluczem dysponuje wicedyrektor, klucz dostępny jest w sekretariacie |
| sekretariat | kluczami dysponuje dyrektor, wicedyrektor i sekretarka szkoły |
| gabinet pedagoga szkolnego | Kluczem dysponuje pedagog, klucz dostępny jest w sekretariacie |
| pokój nauczycielski | kluczem dysponują nauczyciele, klucze dostępne w pokoju woźnych |
| sale lekcyjne | kluczami dysponują nauczyciele, klucze dostępne w pokoju nauczycielskim |
| świetlica | kluczami dysponują wychowawcy świetlicy, klucz dostępny jest w pokoju woźnych |
| pokój nauczycieli wych. fiz. | kluczem dysponują nauczyciele wychowania fizycznego, klucze dostępne są w pokoju woźnych |

2.5 WYKAZ ZBIORÓW DANYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH WRAZ ZE WSKAZANIEM PROGRAMÓW STOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LP | Nazwa zbioru danych | Systemy informatyczne stosowane do przetwarzania danych osobowych w zbiorze | Zastosowany poziom bezpieczeństwa | Uwagi |
| 1 | uczniowie oraz kandydaci do szkoły | Word, Excel, OKE, Librus | wysoki |  |
| 2 | pracownicy oraz kandydaci do pracy | Word, Excel, Płace, SIO, eRU-PZU | wysoki |  |
| 3 | rodzice/prawni opiekunowie | Word, Excel, | wysoki |  |
| 4 | Płace | Płace, Płatnik - ZUS | wysoki |  |

2.6. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY POSZCZEGÓLNYMI POLAMI INFORMACYJNYMI

§8

|  |  |  |
| --- | --- | --- |
| LP | Nazwa zbioru danych | Zakres przetwarzanych danych |
| 1 | uczniowie oraz kandydaci do szkoły | imię, nazwisko, data urodzenia, nr PESEL, adres zamieszkania, klasa, data przyjęcia do szkoły, oceny, obecność na zajęciach, dokumentacja medyczna, oceny zachowania. |
| 2 | pracownicy oraz kandydaci do pracy | imię (imiona) i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), numer telefonu, wykształcenie, przebieg dotychczasowego zatrudnienia, numer PESEL i NIP, imiona i nazwiska oraz daty urodzenia dzieci pracownika, |
| 3 | rodzice/prawni opiekunowie | imiona i nazwiska, adres zamieszkania, numer telefonu |
| 4 | płace | wysokość wynagrodzenia pracowników, imię (imiona) i nazwisko, data i miejsce urodzenia, miejsce zamieszkania i zameldowania, numer telefonu, numery kont bankowych, numer NIP i PESEL |

2.7 ZBIORY DANYCH PRZETWARZANYCH TRADYCYJNIE.

§9

|  |  |  |
| --- | --- | --- |
| LP | Zbiór Danych Osobowych | Lokalizacja Zbioru |
| 1. | Ewidencja oprogramowania | Sekretariat |
| 2. | Zestawienie wysyłanych przesyłek pocztowych | Sekretariat |
| 3. | Wykaz byłych pracowników | Sekretariat |
| 4. | Listy z nagrodami dyrektora | Sekretariat |
| 5. | Listy obecności pracowników | Sekretariat |
| 6. | Badania okresowe (profilaktyczne) | Sekretariat |
| 7. | Akta osobowe pracowników | Sekretariat |
| 8. | Umowy cywilnoprawne | Sekretariat |
| 9. | Ewidencja badań profilaktycznych pracowników | Sekretariat |
| 10. | Ewidencja szkoleń pracowników | Sekretariat |
| 11. | Polecenie wyjazdu służbowego | Sekretariat |
| 12. | Wykaz niezdolności do pracy pracowników | Sekretariat |
| 13. | Ewidencja pracowników przyjętych i zwolnionych oraz czasu pracy | Sekretariat |
| 14. | Wnioski o ustalenie kapitału początkowego pracowników | Sekretariat |
| 15. | Formularz aplikacyjny kandydatów do pracy | Sekretariat |
| 16. | Rejestr szkoleń okresowych BHP i p.poż. | Sekretariat |
| 17. | Wnioski i umowy o staż | Sekretariat |
| 18. | Podania o zapomogi | Sekretariat |
| 19. | Wnioski pracowników o dofinansowanie do świadczeń z ZFŚS | Sekretariat |
| 20. | Protokoły z posiedzeń Komisji Socjalnej | Sekretariat |
| 21. | Pisma do ZUS, Komorników, Sądów, Urzędów Skarbowych, Towarzystw Ubezpieczeniowych | Sekretariat |
| 22. | Lista pracowników posiadających telefony komórkowe służbowe i prywatne | Sekretariat |

2.8. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

§10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LP | Źródłowy system informatyczny | Docelowy system informatyczny | Zakres przesyłanych danych osobowych | Sposób transmisji |
| 1 | Word/Excel | Word/Excel | Excel imię i nazwisko ucznia, data i miejsce urodzenia, PESEL, adres zamieszkania /zameldowania, | manualny (eksport oraz import) |
| 2 |  | SIO | PESEL pracowników, dane o wynagrodzeniu, zatrudnieniu, wykształceniu | przesyłanie danych poprzez sieć telekomunikacyjną |
| 3 |  | OKE | imię i nazwisko ucznia, data i miejsce urodzenia, PESEL | PESEL przesyłanie danych poprzez sieć telekomunikacyjną |
| 4 |  | Librus | imię i nazwisko ucznia, adres, dane rodziców, nr telefonów, data urodzenia, PESEL, oceny, frekwencja, plan lek  cji | manualny (eksport oraz import |
| 5 |  | Płatnik - ZUS | imię i nazwisko pracownika, data urodzenia, PESEL, adres zamieszkania i zameldowania, numer telefonu | przesyłanie danych poprzez sieć telekomunikacyjną |
|  |  | eRU - PZU | imię i nazwisko pracownika, data urodzenia, PESEL, adres zamieszkania | przesyłanie danych poprzez sieć telekomunikacyjną |
|  |  | Nabór | imię i nazwisko ucznia, PESEL, numer szkoły rejonowej, numer wybranej szkoły | imię i nazwisko ucznia, data i miejsce urodzenia, PESEL, adres zamieszkania /zameldowania |

2.9. ŚRODKI TECHNICZNE I ORGANIZACYJNE ZAPEWNIAJĄCE BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH .

§11

Realizując politykę bezpieczeństwa informacji placówka zapewnia ich:

1. poufność – informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
2. integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany.
3. dostępność – dyspozycję do wykorzystania na żądanie, w złożonym czasie, przez autoryzowany podmiot.
4. rozliczalność – przypisanie działań danego podmiotu w sposób jednoznaczny tylko temu podmiotowi.
5. autentyczność – zapewnienie, ze to tożsamość podmiotu lub zasobu jest taka, jak deklarowana
6. niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne.
7. niezawodność – zamierzone zachowania i skutki są spójne.

2.10. KOMPETENCJE I ODPOWIEDZIALNOŚĆ W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH.

§12

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

§13

Administrator Danych Osobowych (ADO)

1. Formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Decyduje o zakresie, celach i metodach przetwarzania danych osobowych i ich ochrony.
3. Odpowiada za zgodne z prawem przetwarzanie danych osobowych w placówce.
4. Udziela upoważnień do przetwarzania danych osobowych określając ich zakres oraz termin ważności.

§14

Administrator Bezpieczeństwa Informacji (ABI)

1. Zapewnia przestrzeganie przepisów o ochronie danych osobowych poprzez:
2. sprawdzanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdania dla administratora danych
3. nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych i środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych.
4. przestrzeganie zasad określonych w dokumentacji wymienionej w punkcie b.
5. zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
6. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych z wyjątkiem zbiorów o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje o których mowa w art. 41 ust. 1 pkt 2-4a i 7.

§15

Administrator Systemu Informatycznego (ASI)

1. Zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI.
2. Doskonali, rozwija metody zabezpieczania danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
3. Przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania zmiany haseł dostępu.
4. Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu informatycznego.
5. Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
6. Prowadzi nadzór nad archiwizacją danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§16

Pracownik przetwarzający dane.

1. Chroni prawo do prywatności osób fizycznych powierzających placówce swoje dane osobowe poprzez skuteczną ochronę tych danych w zgodzie z przepisami prawa oraz zasadami Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym obowiązującymi w placówce.
   1. ZASADY UDZIELANIA DOSTĘPU DO DANYCH OSOBOWYCH

§17

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z zasadami ochrony zawartymi w Polityce bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym. Za zaznajomienie osoby z tymi zasadami odpowiedzialny jest ABI. Osoba zaznajomiona z zasadami ochrony danych osobowych w placówce potwierdza to pisemnym oświadczeniem zgodnie ze wzorem w załączniku nr 5 , stanowiącym integralną część niniejszego dokumentu.

§18

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ADO, zgodne ze wzorem w załączniku nr 3 i nr 4, stanowiącym integralną część niniejszego dokumentu.

§19

ADO może wyznaczać uprawnionych do przetwarzania danych osobowych pracowników placówki do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi osobami przetwarzającymi dane osobowe w placówce w ramach prowadzonej działalności.

§20

Upoważnienia do dostępu do systemu informatycznego dla pracowników zewnętrznych wykonujących prace zlecone (np. konserwacje) wydawane są na wniosek ASI.

2.12 BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W FORMIE TRADYCYJNEJ.

§21

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Klucze do pomieszczeń wydawane są pracownikom upoważnionym do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

§22

Korzystanie ze zbiorów danych osobowych przez osoby nie zatrudnione w placówce powinno odbywać się po zweryfikowaniu upoważnienia udzielonego tej osobie lub skonsultowane z ADO w przypadku przedstawicieli instytucji upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

2.13 BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

§23

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w **Instrukcji zarządzania systemem informatycznym,**  która jest integralną częścią dokumentacji placówki w zakresie ochrony danych osobowych , obligatoryjną do zapoznania się i stosowania przez wszystkich użytkowników i stanowi załącznik nr 1 do niniejszego dokumentu.

* 1. ANALIZA RYZYKA ZWIĄZANEGO Z PRZETWARZANIEM DANYCH OSOBOWYCH
     1. Identyfikacja zagrożeń

§24

|  |  |
| --- | --- |
| **FORMA PRZETWARZANIA DANYCH** | **ZAGROŻENIA** |
| Dane przetwarzane w sposób tradycyjny | * oszustwo, kradzież, sabotaż; * zdarzenia losowe (powódź, pożar); * zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); * niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; * pokonanie zabezpieczeń fizycznych; * podsłuchy, * podglądy, * brak rejestrowania udostępniania danych; * niewłaściwe miejsce i sposób przechowywania dokumentacji. |
| Dane przetwarzane w systemach informatycznych | * nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów; * kradzież danych kont; * pokonanie zabezpieczeń programowych; * • zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); * niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; * zdarzenia losowe (pożar); * niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; * naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione; * przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; * przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; * przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych; * brak rejestrowania zdarzeń tworzenia lub modyfikowania danych |

* + 1. Określenie wielkości ryzyka

§25

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

* + 1. Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§26

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

Zatwierdzam

………………………………………………

(data, pieczątka i podpis dyrektora)

**ZAKRES ZADAŃ I UPRAWNIENIA**

**ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI**

**W ZESPOLE PLACÓWEK OŚWIATOWYCH**

**IM. PAPIEŻA JANA PAWŁA II**

**W DYLEWIE.**

Celem działania ABI jest nadzorowanie i kontrolowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w Zespole Placówek Oświatowych im. Papieża Jana Pawła II w Dylewie.

Zadaniem ABI jest nadzorowanie i kontrolowanie, a w szczególności :

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a)  sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych

b)  nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, (tj. dokumentacji przetwarzania danych) oraz przestrzegania zasad w niej określonych

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych

2. Nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób.

3. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń lub podejrzenia naruszenia,

4. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe.

5. Zarządzanie hasłami użytkowników, systemami antywirusowymi i ich procedurami.

6. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności,

7. Nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,

8. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych oraz stosowania środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach

Informatycznych

9. Prowadzenie (jawnego) rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1ustawy o ochronie danych osobowych (tj. zbiorów zwolnionych z obowiązku rejestracji), zawierającego:

1)  nazwę zbioru oraz

2)  informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 ustawy, tj.:

a)  oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi, o którym mowa w art. 31, lub wyznaczenia podmiotu, o którym mowa w art. 31a; oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania,

b)  cel przetwarzania danych;

c)  opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych;

d)  sposób zbierania oraz udostępniania danych;

e)  informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane;

f)    informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

10. Prowadzenia wewnętrznych kontroli w zakresie przestrzegania przepisów o ochronie danych i przekazywanie **wyników kontroli do GIODO w formie sprawozdań**, którepowinny obejmować m.in.:

a. Wykaz czynności podjętych przez ABI w toku sprawdzenia zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

b. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych osobowych;

c. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem.

Częstotliwość prowadzenia kontroli wewnętrznych oraz przekazywania sprawozdań do GIODO, zostaną określone w drodze rozporządzenia ministra właściwego do spraw administracji publicznej.

Załącznik nr 1

……………………………… Dylewo ……………………….

Pieczątka szkoły data wydania

**Upoważnienie nr … do przetwarzania danych osobowych**

1.Upoważniam Pana/Panią …………………………………………...........................................

Zatrudnioną/ego na stanowisku ………………………………………………………………...

w ………………………………………………………………………………………………...

do dostępu do następujących danych osobowych:

1. …………………………………………………………………………………………...
2. …………………………………………………………………………………………...
3. …………………………………………………………………………………………...

*(należy sprecyzować zakres upoważnienia: można go określić poprzez wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba lub rodzaj czynności lub operacji, jakich może ona dokonywać na danych osobowych)*

2. Identyfikator ………………………………………………………………………………….

*(wypełnia się jedynie w przypadku, gdy dane są przetwarzane w systemie informatycznym)*

3. Okres trwania upoważnienia………………………………………………………………….

………………………………………

*(pieczęć i podpis administratora/pracodawcy*

*lub osoby reprezentującej pracodawcę /administratora albo osoby upoważnionej do składania oświadczeń w imieniu pracodawcy)*

Załącznik nr 2

**EWIDENCJA OSÓB UPOWAŻNIONYCH**

**DO PRZETWARZANIA DANYCH OSOBOWYCH**

**W ZESPOLE PLACÓWEK OŚWIATOWYCH IM. PAPIEŻA JANA PAWLA II**

**W DYLEWIE**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *LP* | *Upoważniony (imię i nazwisko)* | *Stanowisko służbowe* | *Nr upowa-żnienia* | *Zakres upoważnienia do przetwarzania danych osobowych* | *Data nadania upowa-żnienia* | *Data ustania upowa-żnienia* | *Identyfikator jeśli dane są przetwarzane w systemie informatycznym* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

(miejscowość i data)

(pieczęć szkoły)

Znak:

**Pan/Pani**

**nauczyciel**

(nazwa szkoły)

Działając na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DZ. U. z 2014 r. poz. 1182

Powołuję Pana/Panią

z dniem ……………………………………..na administratora bezpieczeństwa informacji w …………………………………………………………………………………………... Zakres Pani/Pana zadań wynikający z pełnionej funkcji określa art. 36a ust. 2 ww. ustawy.

(pieczątka i podpis dyrektora)

**Zarządzenie nr ……………./…………..**

Dyrektora ………………………………………………………………

z dnia ………………………………………………

*w sprawie powołania Administratora Bezpieczeństwa Informacji oraz jego zastępcy*.

Na podstawie art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182) oraz Polityki Bezpieczeństwa Danych osobowych ……………….................................................................................................... zarządzam co następuje :

Powołuję Pana/Panią ……………………..….na stanowisko Administratora Bezpieczeństwa Informacji ……………………………………………………. .

Powołuję Pana/Panią ……………………..………….na stanowisko zastępcy Administratora Bezpieczeństwa Informacji ……………………………………………………………………. .

Zarządzenie wchodzi w życie z dniem ………………………………………

*(pieczęć i podpis dyrektora)*

Załącznik nr

dnia ………………

…………………………………

…………………………………

…………………………………

(pieczęć lub pełna nazwa i adres szkoły )

WNIOSEK

O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do: .................................................................................................................

.................................................................................................................

2. Wnioskodawca:………........................…………………………………..

.................................................................................................................

3. Podstawa prawna upoważniająca do pozyskania danych albo wskazanie wiarygodnie uzasadnionej potrzeby posiadania danych w przypadku osób innych niż wymienione w art. 29 ust. 1 ustawy o ochronie danych osobowych:

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

4. Wskazanie przeznaczenia dla udostępnionych danych:

…………………………………………………………………………………………

…………………………………………………………………………………………

……………………………………………………………………………………….…

5. Oznaczenie lub nazwa zbioru z którego mają być udostępnione dane: Posiadane zbiory danych właściwe do zakresu żądanych informacji.

6. Zakres żądanych informacji ze zbioru (*należy wskazać jakie dane mają zostać*

*udostępnione)*:

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych:

………………………………………………………………………………………….

……………………………………..

(data i podpis wnioskodawcy)

Załącznik Nr

……………………………… Dylewo……………………….

Pieczątka szkoły data wydania

Upoważnienie nr ……….

Upoważniam Pana/Panią …………………………………………....... do dostępu do danych osobowych pracowników i byłych pracowników w zakresie dotyczącym przetwarzania danych zgodnie z zakresem Pana/Pani obowiązków i uprawnień.

Jednocześnie zobowiązuję Pana/Panią do zachowania w tajemnicy informacji, z którymi zapoznał/a się Pan/i podczas korzystania z akt osobowych pracowników.

*Naruszenie obowiązków w zakresie ochrony danych osobowych może skutkować nałożeniem na pracownika kary porządkowej, a nawet rozwiązaniem umowy o pracę bez wypowiedzenia z powodu ciężkiego naruszenia obowiązków pracowniczych.*

Podstawa prawna: art.52 §1 pkt 1, art. 104 §1 ustawy z dnia 26 czerwca 1974r. Kodeks Pracy (t.j. Dz. U. z 1998r. Nr 21, poz. 94 z późn. zm.), art.37 ustawy z dnia z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) §6 rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. z 1996r. Nr 62, poz. 286 z późn. zm.)

Upoważnienie jest ważne od dnia ……………………. do odwołania.

………………………………. …….……………………….

data i podpis upoważnionego data i podpis administratora danych

załącznik nr

(imię i nazwisko rodziców/prawnych opiekunów i adres zamieszkania)

(miejscowość, data)

**Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych**

Wyrażam zgodę na przetwarzanie (w tym utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie) danych osobowych w tym danych wrażliwych, mojego dziecka ………………………………………………………zbieranych przez ………………………

……………………………. z siedzibą w…………………………………., zgodnie z ustawą z dnia 29 sierpnia 1997r o ochronie danych osobowych (DZ.U. z 2014 r. poz. 1182).

Dane te są zbierane do celów:

1. promowania osiągnięć edukacyjnych dziecka, w szczególności na stronie internetowej szkoły, w gablotach informacyjnych w budynku szkoły, w folderach i materiałach promujących szkołę.
2. Zamieszczania wizerunku dziecka w szczególności na stronie www szkoły i w gablotach informacyjnych w budynku szkoły.
3. Zapewnienia dziecku podczas pobytu w szkole odpowiedniej opieki, odżywiania.
4. Stosowania w pracy opiekuńczo-wychowawczej odpowiednich metod mających na celu właściwy rozwój psychofizyczny dziecka.
5. Stosowania właściwej diety.
6. Zapewnienia odpowiedniej (w zależności od możliwości szkoły) opieki zdrowotnej.

Wyrażam również zgodę na przetwarzanie danych wymienionych w lit. a i lit. b oświadczenia, także po ukończeniu szkoły.

W związku z powyższym mam świadomość o celu zbierania tych danych, prawie wglądu do danych dziecka oraz możliwości ich poprawiania.

(podpis rodzica/rodziców/prawnych opiekunów)