Załącznik
do Zarządzenia nr 3/2023
Dyrektora Zespołu Szkół Społecznego
Towarzystwa Oświatowego w Białymstoku

POLITYKA
BEZPIECZEŃSTWA INFORMACJI
Zespołu Szkół Społecznego Towarzystwa Oświatowego w Białymstoku

Podstawa prawna

Konstytucja RP (art. 47 i 51)
Konwencja nr 108 Rady Europy – dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych
Ustawa z 10 maja 2018 o ochronie danych osobowych
Ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku za zapobieganiem i zwalczaniem przestępczości
USTAWA z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
Kodeks pracy
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Podstawowe pojęcia

Szkoła – w tym dokumencie jest rozumiana, jako Zespół Szkół Społecznego Towarzystwa Oświatowego w Białymstoku, zlokalizowana przy ulicy Mieszka I 5;
Polityka - – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa" obowiązująca w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku;
Instrukcja – w tym dokumencie rozumiana jest jako Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku;
Administrator Danych Osobowych (Administrator)– Dyrektor Zespołu Szkół Społecznego Towarzystwa Oświatowego w Białymstoku;
Inspektor – pracownik szkoły wyznaczony przez Administratora Danych Osobowych (Dyrektora) do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy ustawy o ochronie danych osobowych w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku. Inspektor może być powołany zarządzeniem Dyrektora Zespołu Szkół Społecznego Towarzystwa Oświatowego w Białymstoku.
Specjalista ds. IT – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie;
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;
Identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
Przetwarzanie danych – rozumie się to w tym dokumencie, jako jakiekolwiek operacje wykonywane na danych

osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;

Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną,

Sieć lokalna – połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych;

Sieć publiczna – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych,

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 1

I.1 System przetwarzania danych osobowych

W skład systemu wchodzą:

- dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
- wydruki komputerowe;
- urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
- procedury przetwarzania danych w tym systemie, w tym procedury awaryjne

Sposób przepływu danych pomiędzy poszczególnymi systemami (office udostępnianie plików). Sposób przekazywania danych jest manualny poprzez System Ewidencji Oświatowej, Dziennik elektroniczny LIBRUS. Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziom bezpieczeństwa.

§ 2

I.2 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

Cele i zasady funkcjonowania polityki bezpieczeństwa.

Realizując Politykę bezpieczeństwa informacji zapewnia ich:

- poufność informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- integralność dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
- dostępność istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
- rozliczalność możliwość jednoznacznego przypisania działań poszczególnym osobom,
- autentyczność zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
- niezaprzeczalność uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- niezawodność zamierzone zachowania i skutki są spójne.

§ 3

Polityka bezpieczeństwa informacji w Szkole ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

- naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
- naruszeń przepisów prawa oraz innych regulacji;
- utraty lub obniżenia reputacji Szkoły;
- strat finansowych ponoszonych w wyniku nałożonych kar;
- zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 4

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

- przetwarzane zgodnie z prawem,
- bierne dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 5

I.3 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

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.

§ 6

Administrator Danych Osobowych – Dyrektor Szkoły:

- 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,
- decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- wydaje upoważnienie/ odwołanie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik nr 1,**
- odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.

§ 7

Inspektor Ochrony Danych Osobowych – pracownik Szkoły wyznaczony przez Dyrektora:

- egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Szkole w imieniu Administratora,
- prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa **załącznik nr 5,**
- ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 1 i nr 2**,
- określa potrzeby w zakresie stosowanych w Szkole zabezpieczeń, wnioskuje do Administratora o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,
- udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
- bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

§ 8

Specjalista ds. IT – pracownik Szkoły wyznaczony przez Dyrektora:

- zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami Inspektora,
- doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzanie

- przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
- nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

I.4 Zasady udzielania dostępu do danych osobowych

§ 9

Dostęp do danych osobowych może mieć wyłącznie **osoba zaznajomiona** z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Szkole Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w **pisemnym oświadczeniu**.

§ 10

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne **upoważnienie** wydane przez Administratora.

§ 11

Inspektor może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Szkoły do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Szkole.

I.5 Udostępnianie i powierzanie danych osobowych

§ 12

Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

§ 13

Udostępnienie danych może nastąpić **na pisemny wniosek** zawierający następujące elementy:
- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

§ 14

Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

§ 15

Powierzenie danych może nastąpić wyłącznie w drodze **pisemnej umowy**, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. **Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania**.

§ 16

Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z **wnioskiem** o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

§ 17

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi Inspektor, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w **załączniku nr 3**.

I.6 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 18

Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

§ 19

Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych. Dostęp do pokoi poza godzinami pracy szkoły jest kontrolowany za pomocą systemu alarmowego.

§ 20

Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu **upoważnienia** lub skonsultowane z Inspektorem w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

I.7 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 21

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w ***Instrukcji zarządzania systemem informatycznym***, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego szkoły.

I.8 Analiza ryzyka związanego z przetwarzaniem danych osobowych
Identyfikacja zagrożeń

§ 22

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; ataki terrorystyczne; brak rejestrowania udostępniania danych; niewłaściwe miejsce i sposób przechowywania dokumentacji;
przetwarzane w systemach informatycznych	nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów; niewłaściwa administracja i konfiguracja systemem; zniszczenie (sfałszowanie) kont użytkowników; kradzież danych kont; pokonanie zabezpieczeń programowych; zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; zdarzenia losowe (powódź, 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;

I.9 Sposób zabezpieczenia danych

§ 23

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
dane przetwarzane w sposób tradycyjny	• przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; • przechowywanie danych osobowych w szafach zamykanych na klucz; • zastosowanie czujników ruchu informujących wyznaczonych pracowników Szkoły o nieautoryzowanym wejściu do budynku; • przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez Administratora; • zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania;
dane przetwarzane w systemach informatycznych	• kontrola dostępu do systemów; • zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; • systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; • składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; • przydzielenie pracownikom indywidualnych kont użytkowników i haseł; • stosowanie indywidualnych haseł logowania do poszczególnych programów; • właściwa budowa hasła;

I.10 Określenie wielkości ryzyka

§ 34

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.

I.11 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 25

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Specjalista ds. IT przeprowadza **okresową analizę ryzyka dla poszczególnych systemów** i na tej podstawie przedstawia Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II.1 Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

§ 27

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.
Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada Administrator. Specjalista ds. IT nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez Administratora.

§ 28

Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.

§ 29

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

Zabezpieczenie danych w systemie informatycznym

§ 30

Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.

§ 31

W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z Specjalistą ds. IT celem uzyskania nowego hasła.

§ 32

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem system
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

§ 33

System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,

- sposobu przekazania danych.

§ 34

Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania”) na każdym komputerze, na którym przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

II.2 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 35

W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
- loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
- loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła. Uwierzytelnienie dwuskładnikowe.

§ 36

W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu chroniony hasłem.

§ 37

W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

§ 38

Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

§39

Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez Specjalistę ds. IT na co najmniej 30 minut przed planowanym zawieszeniem.

§40

Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia Specjalistę ds. IT w razie:
- podejrzenia naruszenia bezpieczeństwa systemu;
- braku możliwości zalogowania się użytkownika na jego konto;
- stwierdzenia fizycznej ingerencji w przetwarzana dane;
- stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

§ 41

Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
- inne nadzwyczajne sytuacje.

II.3 Tworzenie kopii zapasowych

§ 42

Pełne kopie zapasowe zbiorów danych tworzone są 4 razy w ciągu roku. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane. Kopie przechowywane są w szafie metalowej w sekretariacie Szkoły. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Inspektor. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

II.4 Udostępnienie danych

§ 43

Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa. Do podmiotów, dla których dopuszczalne jest udostępnianie danych przez szkołę należą:
- Organ Nadzorujący [w związku z awansem zawodowym]
- Organ Prowadzący [wykaz z czasem pracy pracowników, udostępnianie dzienników zajęć, wykazy wygenerowane z SIO]
- Dzienniki lekcyjne [dane rodziców w zakresie opisanym w Rozporządzeniu MEN z dnia 19 lutego 2002r. w sprawie sposobu prowadzenia dokumentacji]
- Strona www [dane osobowe ucznia i np. jego osiągnięcia, publikowanie list z wynikami, ocenami, zdjęciem – tylko za zgodą]
- Szkolna tablica ogłoszeń [publikowanie list z wynikami, ocenami, zdjęciem – tylko za zgodą]
- Formularz zgłoszeniowy do szkoły [dane osobowe: nr telefonu, PESEL dziecka, itp. – tylko za zgodą]
- Podmioty świadczące usługi w zakresie oświaty, np. PZU [w zależności od celu]

II.5 Przeglądy i konserwacje systemów

§ 44

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców. Prace powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych. Przed rozpoczęciem prac przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

II.6 Niszczenie wydruków i nośników danych

§ 45

Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski). Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III.1 Istota naruszenia danych osobowych

§ 46

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

III.2 Postępowanie w przypadku naruszenia danych osobowych

§ 47

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to Inspektorowi lub Administratorowi.

§ 48

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

§ 49

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora.

§ 50

Inspektor podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Szkoły,

- może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora,
- nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

§ 51

Inspektor dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik nr 4** i przekazuje go Administratorowi.

§ 52

Inspektor zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

III.3 Sankcje karne

§ 53

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

§ 54

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załączniki:

Załącznik nr 1 – Upoważnienie/ Odwołanie do przetwarzania danych osobowych
Załącznik nr 2 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych
Załącznik nr 3 – Informacja o zawartości zbioru danych
Załącznik nr 4 – Raportu z naruszenia bezpieczeństwa danych osobowych
Załącznik nr 5– Ewidencja Osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 6 – Ewidencja kontroli upoważnień do przetwarzania danych osobowych
Załącznik nr 7– Ewidencja umów powierzenia – przetwarzania danych osobowych
Załącznik nr 8 – Umowa powierzenia danych osobowych (wzór)
Załącznik nr 9 – Ewidencja nośników danych osobowych
Załącznik nr 10 - Rejestr czynności przetwarzania danych osobowych

Załącznik Nr 1
do Polityki bezpieczeństwa w Zespole
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

Wzór Upoważnienie do przetwarzania danych osobowych

Z dniem …… upoważniam Panią: …….
do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków: - na stanowisku:
……..
- wynikających z umowy o pracę z dnia …….. – na czas określony
do…….dnia……../nieokreślony
w następujących zbiorach danych osobowych:
1. Np. Dzieci: dane podstawowe w zakresie: *WG, WP, MO, PR,AR,PO,UD,*
- *w formie elektronicznej/papierowej**
2. Np. Rodzice: dane podstawowe w zakresie: WG, WP, MO,PO, PR, AR, UD
- *w formie elektronicznej/papierowej**
3. Np. Dane pracowników w zakresie: WG, WP,MO,PR,AR,PO,UD
- *w formie elektronicznej/papierowej**
4. Np. Dane wrażliwe dzieci oraz pracowników- dotyczące stanu zdrowia dzieci i pracowników w zakresie niezbędnym do realizowania obowiązków pracowniczych;

Nazwa systemu:
……
Konieczność zmiany hasła do systemu operacyjnego (komputera) TAK
Upoważnienie wygasa z chwilą:
-ustania Pana/Pani*) zatrudnienia na stanowisku …….
wygaśnięcia lub rozwiązania umowy ……..
- odwołania upoważnienia……

Zobowiązuję Panią/Pana do zachowania w tajemnicy danych osobowych oraz znanych Pani/Panu sposobów zabezpieczenia danych osobowych stosowanych w Zespole Szkół STO w Białymstoku (dalej Administrator Danych), przez cały okres zatrudnienia u Administratora Danych / świadczenia usług na rzecz Administratora Danych *), jak również po ustaniu zatrudnienia / świadczenia usług *).

……..…….., dnia …….

……
(podpis Administratora Danych)

……
(podpis IOD)

Uwaga

*****) *w razie potrzeby niepotrzebne skreślić*

Legenda do zakresu powierzenia:

Wgląd (WG), Wprowadzanie (WP), Modyfikowanie (MO), Usuwanie (US), Archiwizowanie (AR), Przechowywanie (PR), Pobieranie (PO), Udostępnianie (UD

Załącznik Nr 2
do Polityki bezpieczeństwa w Zespole
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

..... Białystok, dnia..... r.
(imię i nazwisko)
.....
(stanowisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

1. Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.
2. Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Szkole zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce bezpieczeństwa informacji Zespołu Szkół Społecznego Towarzystwa Oświatowego w Białymstoku i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole.
3. Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz.U. 2002 r. Nr 101 poz. 926 z późn. zm.) oraz Rozporządzenia MSWiA 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). Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w Zespole Szkół Społecznego Towarzystwa Oświatowego może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

Załącznik Nr 3
do Polityki bezpieczeństwa w Zespole
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

Białystok, dnia……..r.

.....
(pieczęć Szkoły)
.....
(imię i nazwisko)

.....

.....
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia.....r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku, działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe:……..

Powyższe dane przetwarzane są w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku w celu …… z zachowaniem wymaganych zabezpieczeń i zostały uzyskane .....(podać sposób).

Powyższe dane nie były / były udostępniane .....(podać komu) w celu .....(podać cel przekazania danych).

Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

.....
(podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 4
do Polityki bezpieczeństwa Zespołu
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

.....
(pieczęć Szkoły)

Białystok, dnia……..r.

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku

1. Data: ..... r. Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....
.....
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia:
.....
.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:
.....
.....

6. Podjęte działania:
.....
.....
7. Postępowanie wyjaśniające:
.....
.....

.....
(podpis Administratora Bezpieczeństwa Informacji

Załącznik Nr 5
do Polityki bezpieczeństwa w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

LP.	Imię i nazwisko osoby upoważnionej	Zakres upoważnienia	Data nadania upoważnienia	Data wygaśnięcia upoważnienia	Data wprowadzenia / aktualizacji rekordu	Data odbycia szkolenia podstawowego z zakresu ochrony danych osobowych

Załącznik Nr 6
do Polityki bezpieczeństwa w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku

EWIDENCJA KONTROLI UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

LP.	Imię i nazwisko kontrolującego	Data realizacji kontroli	Zakres kontroli	Wynik kontroli	Wykaz ewentualnych nieprawidłowości stwierdzonych w toku kontroli	Osoba / dział wskazana do usunięcia nieprawidłowości	Termin usunięcia nieprawidłowości

Załącznik Nr 7
do Polityki bezpieczeństwa w Zespole Szkół Społecznego Towarzystwa Oświatowego w Białymstoku

EWIDENCJA UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH						
LP.	**Nazwa podmiotu (powierzającego lub podmiotu przetwarzającego)**	**Lokalizacja umowy**	**Data nadania umowy**	**Dane kontaktowe osób opiniujących umowę po stronie kontrahenta**	**Data otrzymania ostatniej odpowiedzi od kontrahenta**	**Status umowy**

Załącznik Nr 8
do Polityki bezpieczeństwa w Zespole
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

Umowa
powierzenia przetwarzania danych osobowych
zawarta dnia ___/___/_____r. pomiędzy:

.....

.....
zwanym dalej „*administratorem*" reprezentowany przez:
a

.....

.....
zwany w dalej „ podmiotem *przetwarzającym*" reprezentowanym przez:

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (z mocą obowiązującą **od 25 maja 2018 r.** zwanej dalej **RODO)** dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż znane mu są zasady ochrony danych osobowych, dokonał analizy ryzyka utraty danych osobowych oraz wdrożył adekwatne i skuteczne mechanizmy natury technicznej, organizacyjnej oraz materialnej w celu zabezpieczenia powierzanych danych osobowych.
4. Podmiot przetwarzający oświadcza, że upoważnieni pracownicy zostali zapoznani i przeszkoleni z zasad ochrony danych osobowych.

§ 2
Przedmiot umowy
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał dane osobowe, powierzone w związku z umową z dnia ……nr …… wyłącznie w zakresie np. prowadzenia kadr
2. Kategoria danych , o których mowa w ust. 1 w następującym zakresie:

1. …….
2. …….

(**należy podać rodzaj danych*) ……. *np. dane zwykłe oraz dane szczególnych kategorii ……. (**należy podać kategorię osób, których dane dotyczą*) *np. pracowników administratora, klientów administratora itd. w postaci …….. np. imion i nazwisk, adresu zamieszkania, nr PESEL itd*.

§ 3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2.Podmiot przetwarzający zobowiązuje się dołożyć najwyższej staranności przy przetwarzaniu powierzonych danych osobowych.
3.Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy albo na wyraźne polecenie administratora. Upoważnieni pracownicy nie mogą wykonywać operacji na danych przekraczających zakres wydanych im upoważnień ani posiadać prawa dostępu do danych w zakresie szerszym, niż wynikałoby to z upoważnienia lub też przetwarzać danych w celu innym, niż ten, do którego zostali upoważnieni. Za działania upoważnionych pracowników, podmiot przetwarzający ponosi odpowiedzialność jak za działania własne.
4.Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5.Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6.Podmiot przetwarzający zobowiązany jest do współpracy z Administratorem w celu wykonania obowiązku udzielania odpowiedzi na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
7.Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi do 12 h od wykrycia zagrożenia.
8. Podmiot przetwarzający umożliwia wykonanie prawa do kontroli na zasadach wyrażonych w **§ 5 niniejszej umowy oraz zobowiązuje się do wdrożenia zaleceń wynikających z protokołu kontroli w terminie w nim wskazanym.**

§ 4

Szczegółowe deklarowane środki techniczne i organizacyjne

1.Podmiot przetwarzający zobowiązany jest do wdrożenia środków technicznych i organizacyjnych uniemożliwiających niezgodne z Umową zmiany danych ich utraty, uszkodzenia lub zniszczenia tych danych.
2.Podmiot przetwarzający oraz każda osoba realizująca umowę zobowiązana jest do niedokonywania kopiowania i utrwalania danych osobowych w jakiejkolwiek formie.
3.W przypadku korzystania z sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego podsłuchem połączenia zdalnego (VPN, SSL lub inne).
4.Podmiot przetwarzający i każda osoba realizująca umowę zobowiązana jest do pracy w systemach gwarantujących zachowanie poufności, integralności, dostępności i odporności danych oraz zapewniających konieczność uwierzytelniania dostępu do nich.

§ 5

Prawo kontroli

1.Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2.Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 48 h uprzedzeniem- w formie telefonicznej lub pisemnej.
3.Podmiot przetwarzający ustanawia osobę do kontaktu: ……..
……tel……
…...,która wprowadzi osobę upoważnioną przez administratora do siedziby podmiotu przetwarzającego oraz będzie zobowiązana udzielić pomocy w trakcie prowadzonej kontroli w obszarach, pomieszczeniach w których przetwarzane są powierzone dane osobowe.
4.Osoba upoważniona przez administratora ma prawo:
1) wstępu do pomieszczeń, w których przetwarzane są powierzone dane osobowe, żądania złożenia pisemnych i ustnych wyjaśnień w celu ustalenia stanu faktycznego;

2) żądania wszelkiej dokumentacji w tym szczególności upoważnień od osób, które przetwarzają powierzone dane;
3) weryfikowania stosowanych zabezpieczeń natury organizacyjnej i technicznej, oględzin urządzeń, nośników danych oraz systemów informatycznych służących do przetwarzania powierzonych danych;
5.Z czynności kontrolnych spisywany jest protokół, który jest udostępniany podmiotowi przetwarzającemu.
6.Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
7.Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
8. W przypadku stwierdzenia przez Administratora uchybień w zakresie wykonywania Umowy o powierzenie lub Ustawy, Administratorowi danych przysługuje prawo do:
1) żądania natychmiastowego wstrzymania przetwarzania danych osobowych i wyznaczenia Wykonawcy terminu na usunięcie uchybień;
2) rozwiązania umowy o świadczenie usługi związanej z powierzeniem przetwarzania danych osobowych, w trybie natychmiastowym bez wypowiedzenia.

§ 6

Korzystanie z usług innego podmiotu przetwarzającego

1. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej Administratora.
2. W przypadku ogólnej pisemnej zgody Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3. Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają na mocy umowy te same obowiązki ochrony danych jak w niniejszej umowie zawartej między administratorem a podmiotem przetwarzającym, w szczególności: obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.

Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

§7

Odpowiedzialność podmiotu przetwarzającego

1.Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym, w innych celach niż wynikają z niniejszej umowy.
2.Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.
3.Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem danych osobowych w sposób naruszający przepisy RODO oraz innych przepisów prawa powszechnie obowiązującego lub za naruszenie obowiązków wyrażonych w § 3 niniejszej umowy.
4.Za naruszenie obowiązków wyrażonych w § 3 niniejszej umowy może zostać nałożona kara umowna w wysokości 10 000zł za każde stwierdzone naruszenie. Administrator zastrzega sobie prawo do dochodzenia dalszego odszkodowania na zasadach ogólnych.
5.Podmiot przetwarzający ma obowiązek współdziałania z Administratorem na jego żądanie w zakresie

ustalenia przyczyn szkody wyrządzonej osobie, której dane dotyczą, jak również zapewnia, że ten obowiązek będzie wypełniać dalszy podmiot przetwarzający.

6. W przypadku zapłaty przez Administratora odszkodowania za całą wyrządzoną szkodę na skutek zachowania podmiot przetwarzający zostanie obciążony uiszczoną kwotą przez Administratora obejmującą również wszelkie koszty.
7. W przypadku, gdy Podmiot przetwarzający naruszy przepisy RODO, inne powszechnie obowiązujące przepisy, postanowienia Umowy, w następstwie czego w stosunku do Administratora zostanie wydane jakiekolwiek orzeczenie, w tym organ nadzorczy nałoży na administratora dodatkowe obowiązki- Podmiot przetwarzający zostanie zobowiązany pokryć poniesione z tego tytułu koszty.

§ 8

Zasady zachowania poufności

Podmiot przetwarzający oraz każda osoba działająca z jego upoważnienia mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora danych.

§ 9

Pouczenie zleceniobiorcy

Naruszenie przez przetwarzającego przepisów RODO przy określaniu celów i sposobów przetwarzania- skutkuje uznaniem go za administratora w odniesieniu do tego przetwarzania.

§ 10

Dane kontaktowe Stron

1. W sprawach związanych z realizacją Umowy strony reprezentują:

a) ze strony Administratora danych:

b) ze strony Podmiotu przetwarzającego:

§ 11

Czas trwania i wypowiedzenie umowy

1. Umowa obowiązuje w okresie wykonywania umowy podstawowej. W wypadku wygaśnięcia, rozwiązania lub wypowiedzenia termin wygaśnięcia, rozwiązania lub wypowiedzenia stosujemy odpowiednio do niniejszej umowy.
2. Administrator jest uprawniony do rozwiązania umowy bez wypowiedzenia, w wypadku zaistnienia którejkolwiek z poniższych przesłanek:

a) Podmiot przetwarzający nie wypełnia obowiązków wskazanych w Rozporządzeniu lub innych powszechnie obowiązujących przepisach dotyczących ochrony danych osobowych;
b) Podmiot przetwarzający nie wypełnia obowiązków wyrażonych §3 umowy.
c) Uniemożliwione zostanie wykonanie przez Administratora prawa do kontroli na warunkach określonych w § 5 umowy.

§ 12

Postanowienia końcowe

1. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
2. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją Umowy jest sąd właściwy dla siedziby Administratora.
3. Umowę sporządzono w 2 egzemplarzach, po jednym dla każdej ze Stron.

_____ _____

(podpis administratora danych) (podpis podmiotu przetwarzającego)

Załącznik Nr 9
do Polityki bezpieczeństwa w Zespole
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

EWIDENCJA NOŚNIKÓW DANYCH OSOBOWYCH

LP.	Typ urządzenia	Nr seryjny nośnika	Użytkownik (imię i nazwisko)	Data wydania	Data zwrotu / utylizacji / zawiadomienia o zagubieniu	Przeznaczenie i inne uwagi

Załącznik Nr 10
do Polityki bezpieczeństwa w Zespole
Szkół Społecznego Towarzystwa
Oświatowego w Białymstoku

REJESTR KATEGORI CZYNNOŚCI PRZETWARZANIA

L.p.	Nazwa zbioru	Oznaczenie administratora i adres jego siedziby	Opis kategorii osób których przetwarzanie dotyczy	Opis kategorii odbiorców	Usunięcie danych	Ogólny sposób zabezpieczenia danych	Cele przetwarzania	Informacje o ewentualnym przekazywaniu danych do państwa trzeciego (*)	Data wpisu do rejestru	Data ostatniej aktualizacji informacji dotyczącej zbioru danych