POLITYKA OCHRONY DANYCH
w Zespole Szkół nr 3 w Katowicach

Podstawa prawna:

1. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*
2. *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), innych przepisów Unii lub państw członkowskich o ochronie danych*
3. *§3 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 2004/100/1024). zgodnie z art. 1 ust. 1 ustawy z 29 sierpnia 1997 r. (Dz. U. 2002/101/926 -Tekst jednolity z późniejszymi zm.).*
4. *art. 68 ust.2 ustawy z 27 sierpnia 2009r. o finansach publicznych (Dz.U.157 poz. 1240 z późn. zm.)*

§ 1

Postanowienia wstępne.

1. „Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w Zespole Szkół nr 3 w Katowicach", jest dokumentem zwanym dalej polityką bezpieczeństwa, który określa zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym ujawnieniem.
2. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
3. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zawiera:
   a. identyfikację zasobów systemu tradycyjnego i informatycznego,
   b. wykaz pomieszczeń, tworzący obszar, w którym przetwarzane są dane osobowe,
   c. wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych,
   d. opis struktury zbiorów danych i sposoby ich przepływu,
   e. środki techniczne i organizacyjne, służące zapewnieniu poufności przetwarzanych danych.
4. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w Zespole Szkół nr 3 w Katowicach, jak i innych, np. studentów, odbywających w niej praktyki pedagogiczne.
5. „Dane osobowe" są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny (np. PESEL, NIP) albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
6. Odpowiedzialność za powierzone dane osobowe, ponoszą wszyscy pracownicy szkoły, mający dostęp do danych osobowych w ramach swych obowiązków służbowych. „Polityka bezpieczeństwa" jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji zasobów w danych osobowych „Polityka bezpieczeństwa" opisuje działania, które w najbardziej efektywny sposób pozwolą osiągnąć postawiony cel.
7. W celu zapewnienia bezpieczeństwa przetwarzanych danych wymaga się, aby wszyscy jego użytkownicy byli świadomi konieczności ochrony wykorzystywanych zasobów. Konsekwencją nie stosowania przez pracownika środków bezpieczeństwa określonych w instrukcjach wewnętrznych może być zniszczenie części lub całości systemów informatycznych, utrata poufności, autentyczności, straty finansowe, jak również utrata wizerunku.
8. Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których mają dostęp. W szczególności w systemach informatycznych odpowiadają oni za poprawne wprowadzanie informacji do tych

systemów oraz za użycie, zniszczenie lub uszkodzenie sprzętu oraz znajdujących się na nim danych i oprogramowania.

§ 2

Definicje.

Ilekroć w instrukcji jest mowa o:

1. administratorze danych osobowych (ADO) – rozumie się przez to osobę decydującą o celach i środkach przetwarzania danych – dyrektor szkoły,
2. inspektorze ochrony danych (IDO) – rozumie się przez to osobę, której administrator danych (dyrektor) powierzył pełnienie obowiązków inspektora ochrony danych,
3. haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
4. identyfikatorze użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
5. odbiorcy danych rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
6. osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to pracownika szkoły, która upoważniona została do przetwarzania danych osobowych przez dyrektora szkoły na piśmie,
7. poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
8. raporcie rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
9. rozporządzeniu MSWiA – 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.)
10. serwisancie – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego,
11. sieci publicznej – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
12. systemie informatycznym rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
13. szkoła – rozumie się przez to Zespół Szkół nr 3 w Katowicach
14. teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
15. ustawie – rozumie się przez to ustawę z dnia 10 maja 2018r. poz. 1000 o ochronie danych osobowych
16. uwierzytelnianiu rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
17. użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

§ 3

Organizacja przetwarzania danych osobowych.

1. Administrator danych osobowych, reprezentowany przez dyrektora szkoły, realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

a. podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,

b. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,
c. wyznacza inspektora ochrony danych i określa zakres ich zadań i czynności,
d. prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych o ile jako właściwą do jej prowadzenia nie wskaże inną osobę,
e. zapewnia, we współpracy z inspektorem ochrony danych i systemu, użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,
f. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

2. Inspektor ochrony danych realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych, w tym zwłaszcza:

a. informuje administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie; monitoruje i przestrzega 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), innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
b. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35; d) współpraca z organem nadzorczym;
c. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
d. wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

§ 4 .

Identyfikacja zasobów systemu informatycznego.

1. Struktura informatyczna Zespołu Szkół nr 3 w Katowicach składa się z sieci wewnętrznej, mieszczącej się w pomieszczeniach: gabinet dyrektora i sekretariat.

§ 5

Wykaz pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.
2. Dane osobowe przetwarzane są na terenie Zespołu Szkół nr 3 w Katowicach
3. Ze względu na szczególne nagromadzenie danych osobowych szczególnie chronione powinny być następujące pomieszczenia :

a. gabinet dyrektora szkoły,
b. sekretariat,
c. gabinet wicedyrektorów
d. gabinet pedagoga szkoły podstawowej
e. gabinet pedagoga liceum ogólnokształcącego
f. gabinet psychologa
g. pokój nauczycielski,
h. gabinet pielęgniarki szkolnej
i. pomieszczenie woźny/rzemieślnik

Pomieszczenie	Zabezpieczenie
Adres: Zespół Szkół nr 3 w Katowicach	SSWiN – System Sygnalizacji Włamania i Napadu; CCTV – monitoring wizyjny
Gabinet dyrektora	Portiernia – wyznaczone miejsce
Sekretariat	Portiernia – wyznaczone miejsce
Gabinet wicedyrektorów	Portiernia – wyznaczone miejsce
Gabinet pedagoga szkoły podstawowej	Portiernia – wyznaczone miejsce
Gabinet pedagoga liceum ogólnokształcącego	Portiernia – wyznaczone miejsce
Gabinet psychologa	Portiernia – wyznaczone miejsce
Pokój nauczycielski	Kluczami dysponują nauczyciele, klucze dostępne u woźny/rzemieślnik
Gabinet pielęgniarki szkolnej	Kluczami dysponuje pielęgniarka, klucze dostępne u woźny/rzemieślnik
Pomieszczenie woźny/rzemieślnik	Kluczami woźny/rzemieślnik, dyrektor szkoły

§ 6

1. **Wykaz zbiorów danych osobowych oraz programów stosowanych do przetwarzania tych danych w Zespole Szkół nr 3 w Katowicach**

Nazwa zbioru danych	Programy zastosowane do przetwarzani danych/nazwa zasobu danych
Uczniowie szkoły	Księga uczniów Dzienniki lekcyjne Dokumentacja medyczna Dokumentacja pedagoga szkolnego Dokumentacja psychologa szkolnego Hermes SIO VULCAN
Pracownicy szkoły	Akta osobowe SIO PABS VULCAN Edytor tekstu
Finanse szkoły	Płatnik ZUS Konto bankowe – depozytowe

2. **Wykaz programów stosowanych w szkole:** Windows 10, Windows 7, SIO – System Informacji Oświatowej, MS Office, Kaspersky, Avila free antivirus, PABS, HERMES, VULCAN

§ 7

Struktura zbiorów danych, sposób przepływu danych i zakres ich przetwarzania.

1. Zbiór danych „Uczniowie szkoły" – Zbiór ten obejmuje dane osobowe uczniów i ich rodziców: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, PESEL oraz imiona i nazwisko rodziców (prawnych opiekunów), adres zamieszkania, numer telefonu domowego lub do pracy, orzeczenie poradni psychologiczno – pedagogicznej, orzeczenie o niepełnosprawności, skierowanie do szkoły.

1) Zakres pierwszy danych tego zbioru: numer ewidencyjny ucznia, imię (imiona) i nazwisko, data i miejsce urodzenia, adres zamieszkania oraz imiona i nazwiska rodziców (prawnych opiekunów) ucznia – obejmuje „Księgę uczniów szkoły" i jest dostępny wychowawcom klasowym, dyrektorowi i jego zastępcy oraz sekretarce. Dane tego zakresu są udostępniane organowi prowadzącemu szkołę i organowi nadzorującemu szkołę w celu przeprowadzenia kontroli. Dane tego zakresu mogą być

udostępnione pracownikom NIK, GIODO, MEN na podstawie pisemnych upoważnień do przeprowadzenia kontroli, a także policji w sytuacji popełnienia przez ucznia wykroczenia przeciw prawu.

2) Zakres drugi danych tego zbioru: imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres ich zamieszkania odnosi się do arkuszy ocen ucznia. Dane w nich zawarte przetwarzają wychowawcy klas, dostęp do nich mają również dyrektor szkoły i jego zastępca oraz sekretarka, która po zakończonym cyklu kształcenia gromadzi je w specjalnych teczkach i przechowuje w archiwum szkolnym.

Dane z zakresu trzeciego mogą być udostępniane tylko przedstawicielom organu nadzorującego szkołę w celach kontrolnych.

3) Zakres trzeci danych osobowych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres zamieszkania i numery telefonów do domu lub do pracy obejmuje dzienniki lekcyjne i jest dostępny wszystkim nauczycielom zatrudnionym w szkole oraz praktykantom, odbywającym w niej praktyki pedagogiczne. Przechowywany jest w pokoju nauczycielskim w specjalnie przeznaczonej do tego celu szafce zamykanej na klucz. Nie mają do niej dostępu ani uczniowie, ani ich rodzice, jak również pozostali pracownicy szkoły, poza sekretarką, która po zakończonym roku szkolnym zdaje je do archiwum szkolnego.
   Dane osobowe z tego zakresu mogą być udostępnione jedynie przedstawicielom organu prowadzącego szkołę oraz organu nadzorującego w czasie wizytacji lub w sytuacjach interwencyjnych, a także NIK i MEN w celu przeprowadzenia odpowiednich kontroli.
4) Zakres czwarty danych zbioru „Uczniowie szkoły": imię (imiona) i nazwisko ucznia, data i miejsce urodzenia, PESEL, informacje o przebytych chorobach, wzroście , wadze, ostrości wzroku itp., a także imiona i nazwisko rodziców (prawnych opiekunów) i ich adres zamieszkania – odnosi się do dokumentacji medycznej ucznia, na którą składają się karta zdrowia ucznia oraz wykazy ewidencyjne uczniów. Dane z tego zakresu są przetwarzane w sposób tradycyjny przez pielęgniarkę szkolną, a dostęp do nich ma oprócz niej mają lekarz, prowadzący badania uczniów, oraz dyrektor szkoły. Wykazy ewidencyjne uczniów, w których są podane ich imiona, nazwiska oraz PESEL są przekazywane do NFZ, natomiast pozostałą dokumentację wydaje się uczniowi po zakończeniu nauki. Dane z tego zakresu mogą być udostępnione NFZ, NIK na podstawie pisemnego upoważnienia w celu przeprowadzenia kontroli.
5) Zakres piąty danych tego zbioru obejmuje dane uczniów (w tym dane wrażliwe), tj. imiona i nazwisko ucznia, data i miejsce urodzenia, adres zamieszkania, a także ostatnie dane o stanie zdrowia (w tym również zdrowia psychicznego), przedstawione w zaświadczeniach i opiniach, poradni psychologiczno – pedagogicznej, która wnioskuje do dyrektora szkoły o nauczanie indywidualne, indywidualny tok nauki, obniżenie progu wymagań albo dostosowanie warunków sprawdzianu do formy niepełnosprawności ucznia. Dostęp do tych danych, które są przetwarzane wyłącznie ręcznie, mają wyłącznie dyrektor szkoły, jego zastępca, pedagog szkolny i nauczyciele pracujący bezpośrednio z dzieckiem oraz specjaliści obejmujący dziecko opieką psychologiczno – pedagogiczną. Mogą być udostępnione organom, prowadzącym kontrolę, w tym zwłaszcza Kuratorium Oświaty i Okręgowej Komisji Egzaminacyjnej.
6) Zakres szósty danych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, PESEL, adres zamieszkania, numer telefonu oraz imiona i nazwisko rodziców, dostępny jest dyrektorowi szkoły, jego zastępcy i sekretarce. Dane te przedstawione są w wersji papierowej w postaci deklaracji składanej przez ucznia o wyborze języka obcego nowożytnego, które następnie wprowadzane są za pomocą programu HERMES do systemu informatycznego i przesyłane do Okręgowej Komisji Egzaminacyjnej w celu przetwarzania ich dla potrzeb sprawdzianu. Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła użytkownika, nadanych przez OKE.
7) Zakres siódmy danych tego zbioru dotyczy danych przekazywanych są w sposób tradycyjny do programów SIO – system informacji oświatowej i uaktualniane dwa razy do roku : 31 marca i 31

września. Wprowadzanie danych do SIO jest możliwe po wprowadzeniu identyfikatora i hasła. Dostęp do tych danych mają organ prowadzący i nadzorujący szkołę, w przypadku SIO do danych osobowych ma dostęp również MEN.

2. Zbiór danych „Pracownicy szkoły" – Zbiór ten obejmuje dane osobowe byłych i obecnych pracowników szkoły, tj. nauczycieli, pracowników administracji i obsługi. Dane te przetwarzane są zarówno ręcznie, jak i w systemie informatycznym.

1) zakres pierwszy danych tego zbioru, tzn. imię i nazwisko nauczyciela oraz ich numery telefonów, dostępne są prawie wszystkim pracownikom szkoły.
2) zakres drugi tego zbioru, tzn. imię i nazwisko pracownika szkoły, data i miejsce urodzenia imiona i nazwisko rodziców, adres zamieszkania, wysokość wynagrodzenia, dane dotyczące wynagrodzenia, kwalifikacji zawodowych, wynagrodzenia, przeszeregowań, urlopów i zwolnień lekarskich, numer dowodu osobistego, numer NIP i PESEL, a także dane wrażliwe – informacje o
odbytych szkoleniach, o posiadanych dzieciach, zawartym związku małżeńskim, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych na podstawie przeprowadzonych badań profilaktycznych (wstępnych, okresowych i kontrolnych) oraz w związku z ubieganiem się nauczyciela przyznanie urlopu dla podratowania zdrowia. Dane te zamieszczone są w dokumentach teczek akt osobowych pracownika, a dostęp do nich mają:

— dyrektor szkoły,
— wicedyrektorzy szkoły,
— sekretarki,

Dane z zakresu drugiego mogą być udostępniane organowi prowadzącemu szkołę i organowi nadzorującemu szkołę, a także innym organom prowadzącym kontrolę, w tym zwłaszcza PIP, RIO i sądom powszechnym w związku z prowadzonym postępowaniem.

3) W systemie informatycznym, funkcjonującym w szkole, dane zbioru „Pracownicy szkoły" są przetwarzane tylko w drugim zakresie. Na polecenie dyrektora szkoły sekretarka, zajmująca się sprawami kadrowymi, przygotowuje w programie „MS office" umowy o pracę, porozumienia, przeszeregowania, wypowiedzenia, w tym wypowiedzenia zmieniające, informacje o warunkach zatrudnienia, korespondencję w sprawie zatrudnienia i wysokości zarobków lub rozwiązania stosunku pracy i świadectwa pracy. Dane te są niezwłocznie wprowadzane do bazy danych komputera . Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła.
4) Z teczek akt osobowych pracowników szkoły dane są przekazywane przez osoby zajmujące się sprawami kadrowymi, sekretarki, wicedyrektorów i dyrektora w sposób tradycyjny do programów SIO – system informacji oświatowej i arkusza organizacyjnego i uaktualniane dwa razy do roku: 31 marca i 31 września. Wprowadzanie danych do SIO jest możliwe po wprowadzeniu identyfikatora i hasła. Dostęp do tych danych mają organ prowadzący i nadzorujący szkołę, w przypadku SIO do danych osobowych ma dostęp również MEN.

4. Wykaz zbiorów danych osobowych:

1) Przetwarzanych w systemach informatycznych:

— budżet,
— zbiór danych finansowo – księgowych,
— faktury,
— kadry,
— dane dzieci,

Zbiór danych Osobowych	Program Informatyczny Służący do Przetwarzania Zbioru danych	Miejsce Przetwarzania	Odpowiedzialny
Pracownicy	SIO	Sekretariat	Sekretarz szkoły
	PABS	Gabinet dyrektora	Dyrektor szkoły
	VULCAN	Sekretariat	Sekretarz szkoły
Uczniowie	SIO	Sekretariat	Sekretarz szkoły
	VULCAN	Gabinet dyrektora	Dyrektor szkoły
	VULCAN	Sekretariat	Sekretarz szkoły
	HERMES	Gabinet dyrektora	Dyrektor szkoły
	PAKIET OFFICE	Gabinet dyrektora	Dyrektor szkoły
		Gabinet wicedyrektora	Wicedyrektor szkoły
		Sekretariat	Sekretarz szkoły
		Pedagog	Pedagog szkoły

2) Zbiorów prowadzonych manualnie:

— rejestr wniosków o rozpoczęcie postępowania kwalifikacyjnego,
— rejestr aktów nadania stopnia awansu zawodowego,
— rejestr wniosków o pomoc z Zakładowego Funduszu Świadczeń Socjalnych,
— dokumentacja przebiegu nauczania,
— dzienniki zajęć ,
— dokumentacja związana z procedurą nadania stopnia awansu zawodowego
— podania osób ubiegających się o pracę,
— rejestr zaświadczeń o zatrudnieniu i wynagrodzeniu.

Zbiór Danych Osobowych – **Pracownicy**			
Dokumentacja Służąca do Przetwarzania Zbioru danych	**Miejsce Przetwarzania /odpowiedzialny**	**Miejsce Przechowywania**	**Zabezpieczenie**
Akta osobowe	Sekretariat / sekretarze szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora
Ewidencja akt osobowych			
Orzeczenie lekarskie do celów sanitarno – epidemiologicznych			
Oświadczenia i wnioski do funduszu socjalnego	Gabinet wicedyrektora/wicedyrektor	Gabinet wicedyrektora	SSWiN, CCTV, Szafa pancerna, klucz u wicedyrektora
Listy obecności pracowników	Sekretariat / sekretarze szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora
Zaświadczenia			
Protokoły powypadkowe	Gabinet wicedyrektora/wicedyrektor	Gabinet wicedyrektora	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora
Arkusz	Gabinet dyrektora/	Gabinet dyrektora	SSWiN, CCTV, Klucz

organizacyjny	dyrektor szkoły		u dyrektora szkoły
Dokumentacja nadzoru pedagogicznego			
Dokumentacja awansów zawodowych nauczycieli			
Ewidencja zwolnień lekarskich	Sekretariat / sekretarze szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora
Podania, życiorysy CV			
Notatki służbowe	Gabinet dyrektora/ dyrektor szkoły	Gabinet dyrektora	SSWiN, CCTV, Klucz u dyrektora szkoły
Dokumentacja dotycząca polityki kadrowej- opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp.			
Ewidencja osób zatrudnionych przy przetwarzania danych osobowych	Sekretariat / sekretarz szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora

Zbiór Danych Osobowych – **Uczniowie**			
Dokumentacja Służąca do Przetwarzania Zbioru danych	**Miejsce Przetwarzania /odpowiedzialny**	**Miejsce Przechowywania**	**Zabezpieczenie**
Skierowania uczniów do szkoły	Sekretariat / sekretarz szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora
Księga uczniów			
Arkusze ocen	Gabinet dyrektora/ dyrektor szkoły	Gabinet dyrektora	SSWiN, CCTV, Klucz u dyrektora szkoły
Dzienniki lekcyjne/pedagoga, psychologa/ świetlicy/bibliotekarza/ rewalidacyjnych	Pokój nauczycielski/wychowawcy, nauczyciele	Pokój nauczycielski/gabinet dyrektora	SSWiN, CCTV, Szafa z przegrodami/ Gabinet dyrektora
Dzienniki zajęć pozalekcyjnych			
Pomoc społeczna, stypendia, wyprawki, obiady	Gabinet pedagoga/pedagog	Gabinet pedagoga	SSWiN, CCTV, Szafka zamykana na klucz
Księga druków ścisłego zarachowania	Sekretariat / sekretarz szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u

			sekretarza szkolnego i dyrektora
Rejestr wydawanych zaświadczeń	Sekretariat / sekretarz szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora
Księga absolwentów			
Dokumentacja ubezpieczeniowa			
Protokoły powypadkowe			
Karta zdrowia ucznia	Gabinet pielęgniarki/pielęgniarka	Gabinet pielęgniarki szkolnej	SSWiN, CCTV, Szafka zamykana na klucz. Klucz u pielęgniarki.
Listy klasowe			
Karty biblioteczne	Biblioteka szkolna/bibliotekarz	Biblioteka szkolna	SSWiN, CCTV, Szafka na klucz
Ewidencja uczniów przystępujących do sprawdzianu OKE	Gabinet dyrektora/ dyrektor szkoły	Gabinet dyrektora	SSWiN, CCTV, Klucz u dyrektora szkoły
Dokumentacja pomocy psychologiczno – pedagogicznej	Gabinet pedagoga/pedagog	Gabinet pedagoga	SSWiN, CCTV, Szafka zamykana na klucz
Dokumenty zarchiwizowane	Sekretariat/sekretarz szkoły	Pomieszczenie: archiwum	SSWiN, CCTV, Szafy zabezpieczone/klucz w sekretariacie
Protokoły rad pedagogicznych, księga opinii i uchwał	Gabinet dyrektora/ dyrektor szkoły	Gabinet dyrektora	SSWiN, CCTV, Klucz u dyrektora szkoły
Umowy zawierane z osobami fizycznymi	Sekretariat / sekretarz szkoły	Sekretariat	SSWiN, CCTV, Szafa pancerna, klucz u sekretarza szkolnego i dyrektora

§ 8

Środki techniczne i organizacyjne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Szkoła przetwarza dane osobowe na podstawie przepisów prawa. Dane osobowe mogą być udostępniane zgodnie z art. 29 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych.

1) W celu zapewnienia ochrony danych osobowych stosuje się odpowiednie rozwiązania organizacyjne i techniczne:

a. budynek szkoły objęty jest systemem kontroli dostępu ;
b. każdy pracownik szkoły przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się oraz stosowania przepisów ustawy ochronie danych osobowych i instrukcji wewnątrzszkolnych;
c. pomieszczenia, w których przetwarzane są dane zamykane są na klucz, jeżeli nie przebywa w nim osoba uprawniona
d. monitory ustawione są w sposób uniemożliwiający oglądanie ekranu z miejsc ogólnodostępnych.
e. bieżące naprawy komputera, dokonywane są w obecności użytkownika systemu.
f. Inspektor Ochrony Danych jest osobą uprawnioną do nadzoru instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie

pozyskanych programów, niezbędnych do wykonywania ustalonych i statutowych zadań szkoły i posiadających ważną licencję użytkownika.

g. wykorzystywanie akt i dokumentów, zawierających dane osobowe (dzienniki zajęć), do pracy w domu jest kategorycznie zabronione.
h. dane z nośników przenośnych nie będących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD – ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;
i. po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora
j. pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie
k. przed atakami z sieci zewnętrznej wszystkie komputery administratora danych chronione są środkami dobranymi przez administratora bezpieczeństwa informacji. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. We wszystkich takich przypadkach należy informować Inspektora ochrony danych oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
l. Inspektor Ochrony Danych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
m. osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator bezpieczeństwa przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
n. do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń Inspektor ochrony danych
o. w szkole nie używa się komputerów przenośnych do przetwarzania danych osobowych
p. odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest Inspektor ochrony danych
q. Inspektor ochrony danych przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza osoby przetwarzające dane osobowe, są obowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.
r. z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez Inspektor Ochrony Danych i administratora danych, w której usunięto dane osobowe.
s. udostępnianie danych osobowych policji, służbie miejskiej i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną.

t. osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

2) Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy. Niezależnie od rozwiązania stosunku pracy osoby, popełniające przestępstwo, będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51 i 52. ustawy oraz art. 266. Kodeksu karnego.

3) Monitoring szkolny

— Dla zapewnienia bezpieczeństwa uczniów, pracowników i ochrony mienia dyrektor szkoły, w uzgodnieniu z organem prowadzącym szkołę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub terenem wokół szkoły w postaci środków technicznych umożliwiających rejestrację obrazu

— Monitoring nie stanowi środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły

— Monitoring nie obejmuje pomieszczeń, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, pomieszczeń, w których uczniom jest udzielana pomoc psychologiczno-pedagogiczna, pomieszczeń przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeń sanitarnohigienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne ze względu na istniejące zagrożenie dla realizacji celu określonego w ust. 1 i nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób.

— Nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, szkoła lub placówka przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nie dłuższy niż 3 miesiące od dnia nagrania.

— Po upływie okresu, o którym mowa w ust. 4, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

— Dyrektor szkoły informuje uczniów i pracowników szkoły lub placówki o wprowadzeniu monitoringu, w sposób przyjęty w danej szkole nie później niż 14 dni przed uruchomieniem monitoringu.

— Dyrektor szkoły przed dopuszczeniem osoby do wykonywania obowiązków służbowych informuje ją na piśmie o stosowaniu monitoringu.

— W przypadku wprowadzenia monitoringu dyrektor szkoły oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem.

— Dyrektor szkoły uzgadnia z organem prowadzącym szkołę odpowiednie środki techniczne i organizacyjne w celu ochrony przechowywanych nagrań obrazu oraz danych osobowych uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, uzyskanych w wyniku monitoringu.”.

§ 9
Przeglądy polityki bezpieczeństwa

1. Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.
2. Inspektor ochrony danych analizuje czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

a. zmian w budowie systemu informatycznego,

b. zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
c. zmian w obowiązującym prawie.

§ 10 .

Postanowienia końcowe.

1. Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązania jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści (załącznik nr 2).
2. Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur ochrony danych jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi włącznie z rozwiązaniem stosunku pracy na podstawie art. 52. Kodeksu pracy.

Katowice 24 maja 2018r.

Wprowadzono: Zarządzenie Nr 17/2019 Dyrektora Zespołu Szkół nr 3 w Katowicach z dnia 25 listopada 2019 roku w sprawie wprowadzenia Polityki ochrony danych osobowych

Załączniki:

1. Instrukcja zarządzania systemem informacji
2. Upoważnienie do przetwarzania danych osobowych
3. Odwołanie
4. Upoważnienie do przetwarzania danych osobowych
5. Rejestr osób upoważnionych do przetwarzania danych osobowych
6. Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami
7. Raport z naruszenia bezpieczeństwa danych osobowych

Załącznik nr 1

Instrukcja zarządzania systemem informatycznym
w Zespole Szkół nr 3 w Katowicach

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

§1

Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w szkole.

§2

1) Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada administrator sieci informatycznej (ASI).
2) ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez administratora danych osobowych.

§3

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.

§4

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.

2. Zabezpieczenie danych w systemie informatycznym

§5

1) Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.
2) W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.

§6

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.

§7

1) Stosuje się aktywną ochronę antywirusową.

3. Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§8

W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła,
2) loguje się do programów i systemów wymagających dodatkowego wprowadzania unikalnego identyfikatora i hasła.

§9

1. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z systemu lub uruchomienie wygaszacza ekranu chronionego hasłem.
2. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor w sposób uniemożliwiający wgląd w wyświetlaną treść.

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

§10

Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
— podejrzenia naruszenia bezpieczeństwa systemu,
— braku możliwości zalogowania się użytkownika na jego koncie,
— stwierdzenia fizycznej ingerencji w przetwarzane dane,
— stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

§11

Na fakt naruszenia 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.

Udostępnianie danych

§12

1. Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.
2. Do podmiotów, dla których dopuszczalne jest udostępnianie danych przez szkołę należą:

— organ nadzorujący,
— organ prowadzący
— dzienniki lekcyjne (dane rodziców),
— strona www szkoły (dane osobowe ucznia, jego osiągnięcia, imiona i nazwiska pracowników, plan zajęć, informacje o pracy szkoły oraz za zgodą zdjęcia),
— szkolna tablica ogłoszeń (informacje o pracy szkoły, listy przyjętych uczniów, itp.),
— wniosek o przyjęcie do szkoły,
— podmioty świadczące usługi w zakresie oświaty, np. towarzystwo ubezpieczeniowe,
— podmioty nadzorujące realizację projektu EFS.

Przeglądy i konserwacja systemów

§13

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

Niszczenie wydruków i nośników danych

§14

1. 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.
2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

Instrukcja postępowania w sytuacji naruszenia danych

§15

1. Istota naruszenia danych osobowych

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.

2. Postępowanie w przypadku naruszenia danych osobowych

§16

1. Każdy pracownik szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informacje mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ADO lub IDO.
2. Każdy pracownik szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.
3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowania zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ADO lub IDO.

§17

1. IDO 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 ADO.

2. IDO dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport i przekazuje go ADO.
3. ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze.

Sankcje karne

§18

1. 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.
2. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza się odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych

Załącznik nr 2

Katowice, dnia _____

(pieczęć szkoły)

UPOWAŻNIENIE NR ...../20.....
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 10, poz. 926 z późn. zm.) upoważniam

Panią/Pana .....

Zatrudnioną/zatrudnionego w Zespole Szkół nr 3 w Katowicach
na stanowisku .....
do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w zakresie wynikającym z zajmowanego stanowiska pracy, w okresie od
dnia ..... do .....
Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w szkole.

.....
(podpis administratora danych osobowych)

Przyjmuję do wiadomości i stosowania
.....
(podpis osoby upoważnionej)

Załącznik nr 3

Katowice, dnia .....

.....
(pieczęć szkoły)

ODWOŁANIE UPOWAŻNIENIA NR ...../20.....
do przetwarzania danych osobowych

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 10, poz. 926 z późn.zm.) odwołuję z dniem ..... upoważnienie do przetwarzania danych osobowych wystawione

dla Pani/Pana .....

Administrator Danych Osobowych
.....
(pieczątka i podpis)

Załącznik nr 4

(pieczęć szkoły)

Ewidencja osób upoważnionych do przetwarzania danych osobowych, zgodnie z art. 39, pkt. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych Dz. U. z 2014r. poz. 1182 z późn. zm.

Lp.	Imię i nazwisk osoby upoważnionej	Stanowisk	Data nadania	Data ustania	Zakres upoważnienia do przetwarzania danyc osobowych	Nazwa programu oraz identyfikator w systemie informatyczny	Miejsce
1							
2							

Załącznik nr 5

Raport z naruszenia ochrony danych osobowych
w Zespole Szkół nr 3 w Katowicach

1. Data: (dzień. miesiąc. rok.) Godzina: (00:00)
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   _____
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeżeli występuje)

3. Lokalizacja zdarzenia: _____
   (*np. numer pokoju, nazwa pomieszczenia*)
4. Rodzaj naruszenia bezpieczeństwa:
   _____
5. Podjęte działania:
   _____
6. Przyczyny wystąpienia zdarzenia:
   _____
7. Postępowanie wyjaśniające:
   _____
8. Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnych naruszeń ochrony danych osobowych.
   _____

(Data i podpis Inspektora Ochrony Danych)