Polityka bezpieczeństwa informacji w Szkole Podstawowej nr 7 im. Fryderyka Chopina w Sochaczewie

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa informacji, zwanej dalej „Polityką bezpieczeństwa" w Szkole Podstawowej nr 7 im. Fryderyka Chopina w Sochaczewie, zwanej dalej „Szkołą", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

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

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

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

a)przetwarzane zgodnie z prawem,
b)zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
c)merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
d)przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.4

§ 2

Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

- Konstytucja RP (art. 47 i 51)
- Rozporządzeniu 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 /Dz. Urz. UE.L nr 119, str.1/,
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 2018 r., poz.1000/,

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Szkole rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   e) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   f) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest tata, jak deklarowana;
   g) niezawodność – zamierzone zachowania i skutki spójne;
   h) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
   i) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

1. Administratorem danych osobowych przetwarzanych w Szkole jest Dyrektor Szkoły.
2. Administrator danych osobowych powołał inspektora ochrony danych, zgodnie art. 37 RODO. Zadania inspektora ochrony danych zawarte są w art. 39 RODO.

Rozdział 2
Definicje

§ 6

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1. **administrator danych osobowych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

2. **inspektor ochrony danych** – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
3. **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz.1000),
4. **RODO** – 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 /Dz. Urz. UE.L nr 119, str. 1/,
5. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
6. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
7. **przetwarzane danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
8. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
9. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
10. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
11. **administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
12. **odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
13. **strona trzecia –** osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
14. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
15. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 7

1. W Szkole przetwarzane są dane osobowe pracowników, uczniów i ich rodziców/opiekunów prawnych jak również kandydatów do pracy i kandydatów do szkoły, stażystów i praktykantów, zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera uregulowania, dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Innymi dokumentami regulującymi ochronę danych osobowych w Szkole są:
   a) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole,
   b) ewidencja osób upoważnionych do przetwarzania danych osobowych,
   c) rejestr czynności przetwarzania danych osobowych,
   d) procedura postępowania w przypadku naruszenia ochrony danych osobowych,
   e) procedura monitoringu wizyjnego.

§ 8

Politykę Bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w systemie: SIO, Optivum kadry, e-dziennik.
2. wszystkich informacji dotyczących danych pracowników, uczniów, kandydatów do pracy, kandydatów do szkoły, stażystów i praktykantów.
3. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia.
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób trzecich, mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez Politykę Bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:
   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
   b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   c) wszystkich pracowników, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez Politykę Bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści, praktykanci oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

§ 10

1. Dane osobowe gromadzone są w zbiorach*:*
   a) Dane pracownicze,
   b) Dane dzieci i ich rodziców/opiekunów,
   c) E-dziennik,
   d) Dzieci i ich rodzice/opiekunowie z rekrutacji, które nie dostały się do szkoły,
   e) Dane finansowo-księgowe,
   f) Składnica akt,
   g) Rejestr korespondencji,
   h) Strona internetowa szkoły,
   i) Dane osób, ubiegających się o pracę,
   j) Dane stażystów, praktykantów.

Rozdział 5
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 12

1. Dane osobowe przetwarzane są w Szkole Podstawowej nr 7 im. Fryderyka Chopina w Sochaczewie, mieszczącej się przy ulicy Chopina 99.

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Zabezpieczenie
1.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet Dyrektora	Kluczami dysponuje Dyrektor
2.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Sekretariat	Kluczami dysponuje Sekretarz Szkoły oraz osoba sprzątająca
3.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet kierownika administracji i intendenta	Kluczami dysponują osoby pracujące w tym gabinecie oraz osoba sprzątająca
4.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Biblioteka	Kluczami dysponują osoby pracujące w bibliotece oraz osoba sprzątająca
5.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet pedagoga	Kluczami dysponuje pedagog oraz osoba sprzątająca
6.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet psychologa	Kluczami dysponuje psycholog oraz osoba sprzątająca

7.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet medyczny	Kluczami dysponują pielęgniarki oraz osoba sprzątająca
8.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Pomieszczenie stanowisk do spraw kadrowych	Kluczami dysponują osoby tu pracujące oraz osoba sprzątająca
9.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Pokój nauczycielski	Kluczami dysponują nauczyciele oraz osoba sprzątająca
10.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet wicedyrektora	Kluczami dysponuje wicedyrektor oraz osoba sprzątająca
11.	Ul. Chodakowska 4, 96-500 Sochaczew	Gabinet wicedyrektora (klas I-III)	Kluczami dysponuje wicedyrektor oraz osoba sprzątająca

Rozdział 6
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 13

1. Zabezpieczenia organizacyjne:
   a) opracowano i wdrożono Politykę Bezpieczeństwa przetwarzania danych osobowych,
   b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole,
   c) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
   d) stworzono procedurę monitoringu wizyjnego,
   e) opracowano i na bieżąco prowadzi się rejestr czynności przetwarzania danych osobowych
   f) wyznaczono inspektora ochrony danych**,**
   g) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
   h) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami, dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
   i) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
   j) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   k) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
   l) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.
2. Zabezpieczenia techniczne:
   a) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,

b) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła,

3. Środki ochrony fizycznej:
   a) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,
   b) urządzenia, służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
   c) dokumenty i nośniki informacji, zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

Rozdział 7
Udostępnianie danych osobowych

§ 14

1. Udostępnianie danych osobowych policji, służbie miejskiej i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem.
2. Udostępnianie informacji policji odbywa się według następującej procedury:
   1) udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:
      a) oznaczenie wnioskodawcy,
      b) wskazanie przepisów uprawniających do dostępu do informacji,
      c) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
      d) wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.
   2) udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego, może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
   3) 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. Policjant jest obowiązany do pokwitowania lub potwierdzenia.
   4) jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
   5) jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępniania informacji.

Rozdział 8
Zadania administratora danych osobowych i inspektora ochrony danych

§ 15

Do najważniejszych obowiązków administratora danych osobowych i administratora bezpieczeństwa informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa i innymi dokumentami wewnętrznymi,
3. przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy Szkoła wprowadza nowy rodzaj przetwarzania danych osobowych,
4. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
5. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
7. nadzór nad bezpieczeństwem danych osobowych,
8. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
9. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 9
Zadania administratora systemu informatycznego

§ 16

1. Administrator systemu informatycznego odpowiedzialny jest za:
   a) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   b) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   c) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
   d) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   e) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   f) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
   g) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   h) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   i) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

j) przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
k) wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
l) zarządzanie licencjami, procedurami ich dotyczącymi,
m) prowadzenie profilaktyki antywirusowej.

2. Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych oraz Polityki Bezpieczeństwa Szkoły przez administratora danych i inspektora ochrony danych.

Rozdział 10
Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych

§ 17

1. Corocznie do dnia 30 czerwca inspektor ochrony danych przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do administratora danych osobowych.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 11
Postanowienia końcowe

§ 18

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych i inspektor ochrony danych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką Bezpieczeństwa i innymi związanymi z nią dokumentami, obowiązującymi u administratora danych osobowych,
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
5. Polityka Bezpieczeństwa wchodzi w życie z dniem 25 maja 2018r.

Załączniki:

1. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Szkole.
2. Procedura postępowania w przypadku naruszenia ochrony danych osobowych.
3. Procedura dotycząca monitoringu wizyjnego w Szkole.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Szkole.
5. Wykaz zbiorów danych osobowych.
6. Rejestr czynności przetwarzania danych osobowych.
7. Wzór komunikatu o naruszeniu ochrony danych osobowych.
8. Wzór zgłoszenia naruszenia ochrony danych osobowych.
9. Oświadczenie o znajomości Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
10. Upoważnienie do przetwarzania danych osobowych.
11. Odwołanie upoważnienia do przetwarzania danych osobowych
12. Raport z naruszenia bezpieczeństwa danych osobowych.

ZAŁĄCZNIK NR 1

Instrukcja zarządzania systemem informatycznym w Szkole Podstawowej nr 7 im. Fryderyka Chopina w Sochaczewie

Rozdział 1
Postanowienia ogólne

§ 1

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Szkoły przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Rozdział 2
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

§ 2

1. Za bezpieczeństwo danych osobowych w systemie informatycznym i za właściwy nadzór odpowiedzialny jest Administrator Danych.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych,
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego użytkownika systemu informatycznego ustalony jest odrębny Identyfikator i hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, zostaje niezwłocznie wyrejestrowany z systemu informatycznego, w którym są przetwarzane, zaś hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

Rozdział 3
Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 3

1. W systemie informatycznym stosuje się uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do uwierzytelnienia użytkownika na poziomie dostępu do systemu operacyjnego stosuje się hasło oraz Identyfikator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.
3. Minimalna długość hasła przydzielonego użytkownikowi wynosi osiem znaków alfanumerycznych i znaków specjalnych.
4. Zabrania się używania identyfikatora lub hasła drugiej osoby.
5. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) Identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   c) informacji o odbiorcach, którym dane osobowe zostały udostępnione.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu

§ 4

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
5. Przy opuszczaniu stanowiska na dłuższy czas, należy ustawić wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

Rozdział 5
Tworzenie kopii zapasowych zbiorów danych oraz sposób, miejsce i okres ich przechowywania

§ 5

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Szkoły.
2. Do archiwizowania danych służą płyty CD, DVD, pen-drive z zapisem danych z systemu.

3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje, jak datę dokonania zapisu, identyfikator użytkownika, wykonującego kopię, opis zawartości.

§ 6

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników, zawierających dane osobowe z miejsca pracy.
6. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:
   a)ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
   b)pozostawiania haseł w miejscach widocznych dla innych osób,
   c)udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
   d)udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
   e)używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
   f)przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
   g)kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,
   h)samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez ASBI,
   i)używania nośników danych udostępnionych przez osoby postronne,
   j)przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (nie służbowego),
   k)otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych” nadawców,
   l)używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą;

Rozdział 6
Sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

§ 7

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej.
2. Użytkowany system jest automatycznie skanowany .
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
   a) uruchomić program antywirusowy i skontrolować użytkowany system,
   b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.
5. Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
   a) zakończyć pracę w systemie komputerowym,
   b) odłączyć zainfekowany komputer od sieci,
   c) powiadomić o zaistniałej sytuacji Administratora Danych lub Inspektora Ochrony Danych.
6. Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

§ 8

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem. W szczególności zabronione jest otwieranie linków bądź pobieranie załączników od nieznanego nadawcy.

Rozdział 7
Sposoby realizacji w systemie wymogów dotyczących przetwarzania danych

§ 9

1. Informacje o odbiorcach danych zapisywane są w systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

Rozdział 8
Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

§ 10

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy, zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
   a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do przetwarzania danych,
   b) przed rozpoczęciem tych czynności dane i programy, znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
   c) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

Rozdział 9
Postanowienia końcowe

§ 11

1. W sprawach nieokreślonych niniejszą instrukcją, należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Niniejsza instrukcja wchodzi w życie z dniem 25 maja 2018r.

ZAŁĄCZNIK NR 2

Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych

1. Celem procedury jest określenie sposobu postępowania gdy:

   - stwierdzono naruszenie zabezpieczeń danych osobowych,
   - w przypadku danych przetwarzanych w formie papierowej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych,
   - w przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.

2. Procedura określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych.

3. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

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

4. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt Administratorowi lub Inspektorowi Ochrony Danych, a następnie postępować stosownie do podjętej przez niego decyzji.

5. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
   - opisanie symptomów naruszenia zabezpieczeń danych osobowych,

- określenie sytuacji i czasu, w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
- określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
- określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

6. Administrator lub Inspektor Ochrony Danych podejmuje wszelkie działania, mające na celu:

   - minimalizację negatywnych skutków zdarzenia,
   - wyjaśnienie okoliczności zdarzenia,
   - zabezpieczenie dowodów zdarzenia,
   - umożliwienie dalszego bezpiecznego przetwarzania danych.

7. W celu realizacji zadań wynikających z niniejszej procedury Administrator Danych lub Inspektor Ochrony Danych ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

   - żądania wyjaśnień od pracowników,
   - korzystania z pomocy konsultantów,
   - nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

8. Polecenia Administratora Danych lub Inspektora Ochrony Danych wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

9. Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Danych lub Inspektorem Ochrony Danych traktowana będzie jako naruszenie obowiązków pracowniczych.

10. W przypadku naruszenia ochrony danych osobowych Administrator Danych bez zbędnej zwłoki – nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

11. W przypadku, gdy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych Inspektor Ochrony Danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje komunikat naruszenia ochrony danych, w którym przedstawia charakter naruszenia; kategorię i przybliżoną liczbę osób, których dane dotyczą; liczbę wpisów, których dotyczy naruszenie;

możliwe konsekwencje naruszenia ochrony danych oraz środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych oraz ograniczające możliwość wystąpienia zdarzenia w przyszłości.

12. Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

	Forma naruszenia	**Sposób postępowania**
1.	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych	Niezwłocznie zakończyć działanie programu
2.	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do danych przez jakiekolwiek innej osoby niż osoby, której identyfikator został przydzielony	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska
3.	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych	Natychmiast zabezpieczyć informację z hasłem w sposób uniemożliwiający odczytanie
4.	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy
5.	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty
6.	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych	W miarę możliwości zabezpieczyć dokumenty.

7.	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie	Zabezpieczyć niewłaściwie zniszczone dokumenty
8.	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię
9.	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	Wezwać nieuprawnioną osobę, odczytującą dane do zaprzestania czynności, wyłączyć monitor
10.	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych	Zabezpieczyć (zamknąć) pomieszczenie
11.	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość
12.	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji
13.	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji
14.	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji

15.	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami

ZAŁĄCZNIK NR 3

Procedura dotycząca monitoringu wizyjnego
w Szkole Podstawowej nr 7 im. Fryderyka Chopina
w Sochaczewie

I. Założenia ogólne

1. Monitoring wizyjny może być wykorzystywany jedynie w celach podnoszenia poziomu bezpieczeństwa w szkole.
2. Budynek szkolny posiada oznaczenia „Obiekt monitorowany".
3. Monitoring jest obsługiwany przez osoby wyznaczone przez dyrektora szkoły.
4. Sprzęt zainstalowany w placówce posiada stosowne atesty i certyfikaty.
5. Rejestracji i zapisowi podlega tylko obraz.

II. Celem monitoringu jest:

1. zwiększenie bezpieczeństwa społeczności szkolnej oraz osób przebywających na terenie placówki,
2. ograniczenie zachowań zagrażających zdrowiu, bezpieczeństwu uczniów,
3. wyjaśnianie sytuacji konfliktowych,
4. ustalanie sprawców czynów nagannych (bójki, zastraszanie, wyłudzanie, zniszczenia mienia, kradzieże itp.) w szkole i jej otoczeniu,
5. ograniczanie dostępu do szkoły i jej terenu osób nieuprawnionych i niepożądanych,
6. zapewnienie bezpiecznych warunków nauki, wychowania i opieki.

III. Zasady wykorzystania zapisów monitoringu wizyjnego

1. Szkoła Podstawowa im. Fryderyka Chopina posiada monitoring wizyjny wewnętrzny i zewnętrzny.

2. Zapisy z monitoringu mogą być wykorzystywane między innymi w sytuacjach:

   a) zagrażających bezpieczeństwu uczniów, nauczycieli, pracowników szkoły,

   b) niszczenia mienia szkoły,

c) niszczenia urządzeń na terenie boiska,

d) kradzieży,

e) konfliktowych (bójki, zastraszanie, wyłudzanie itp.)

g) podejrzenia o palenie papierosów i korzystanie z używek,

h) jako przykłady dobrej praktyki i promowania właściwych zachowań.

IV. Lokalizacja rejestratora

1. Urządzenie rejestrujące znajduje się w gabinecie dyrektora szkoły. Wykluczony jest dostęp do niego osób nieupoważnionych.

V. Osoby uprawnione do przeglądania zarejestrowanego materiału

1. Do przeglądania zarejestrowanych zapisów monitoringu uprawnieni są:

   a) dyrektor szkoły,
   b) wicedyrektorzy szkoły,
   c) nauczyciele zatrudnieni w szkole,
   d) pedagog szkolny,
   e) psycholog szkolny.

2. Zapis z monitoringu może zostać odtworzony rodzicom/prawnym opiekunom uczniów tylko na ich pisemny wniosek i tylko w uzasadnionych przypadkach, za zgodą dyrektora szkoły i w terminie ustalonym przez dyrektora szkoły (zapis monitoringu udostępniany jest rodzicom/opiekunom wyłącznie w sytuacjach bezpośrednio zagrażających bezpieczeństwu ucznia). Nie udostępnia się zapisu monitoringu rodzicom/opiekunom uczniów na jakichkolwiek nośnikach z możliwością wynoszenia ich ze szkoły ze względu na ochronę wizerunku dzieci i pracowników szkoły.

3. Nagrania mogą być udostępniane organom ścigania na pisemną prośbę w celu wyjaśnienia prowadzonej sprawy.

4. Osoby obserwujące bieżące zapisy i osoby przeglądające zapisy zobowiązane są do nieujawniania danych zarejestrowanych przez monitoring.

5. W przypadku zarejestrowania wypadku, w razie zaistniałej potrzeby, dyrektor szkoły powołuje – na piśmie - inspektora BHP lub społecznego inspektora pracy do wglądu w zapis z monitoringu.

VI. Archiwizacja i przechowywanie materiału pochodzącego z monitoringu

1. Zapisy wideo przechowywane są na dysku twardym rejestratora przez 30 dni, a później są nadpisywane.

2. W sytuacji uznania materiału nagranego za dowód w sprawie, zapis utrzymywany jest przez okres konieczny do rozstrzygnięcia przebiegu zdarzenia, którego zapis dotyczy. Przegrany na nośniki - odpowiednio opisane - materiał przechowywany jest w gabinecie dyrektora w zamykanej na klucz szafie.

VII. Przepisy końcowe

1. Monitoring wizyjny może być systematycznie modernizowany, jeżeli wynika to z potrzeb szkoły oraz możliwości finansowych.

2. W sprawach nie uregulowanych niniejszą procedurą, ostateczną decyzję podejmuje dyrektor szkoły.

ZAŁĄCZNIK 4

Ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko służbowe	Okres upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator(Nazwa programu przetwarzanych danych osobowych w systemie informatycznym)

ZAŁĄCZNIK NR 5

Wykaz zbiorów danych osobowych ze wskazaniem programów do przetwarzania tych danych

L.p.	Nazwa zbioru	Zastosowane programy	Uwagi
1.	Dane pracownicze	Ewidencja papierowa, elektroniczna ewidencja pracownicza	Teczki akt osobowych, VULCAN, sekretariat, SIO, PEFRON
2.	Dane uczniów i związane z nimi dane rodziców/opiekunów prawnych	Ewidencja papierowa, elektroniczna ewidencja	SIO, OKE, Hermes, sekretariat, Optivum
3.	Rejestr uczniów realizujących obowiązek szkolny w innych placówkach	Ewidencja papierowa, elektroniczna ewidencja	SIO, OKE, VULCAN, sekretariat, Optivum
4.	Zamówienia publiczne	Ewidencja papierowa, elektroniczna ewidencja	Forma papierowa
5.	Archiwum	Ewidencja papierowa	Forma papierowa
6.	Upoważnienia do odbioru dzieci	Ewidencja papierowa	Znajdują się u nauczycieli
7.	Rejestr korespondencji	Ewidencja papierowa	Znajduje się w sekretariacie
8.	Dane kontrahentów	Ewidencja papierowa	Znajdują się w pokoju kierownika gospodarczego
9.	Dane serwisu internetowego szkoły	zs.sochaczew@wp.pl	

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami(Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r.)

Lp.	Nazwa zbioru danych	Struktura zbiorów	Przepływ danych	Uwagi
1.	Dane pracownicze	Imię, imiona, nazwisko, data i miejsce urodzenia, imiona rodziców, adres zamieszkania, nr telefonu, wykształcenie, przebieg dotychczasowego zatrudnienia, PESEL, NIP, nr dowodu osobistego	Papierowa i elektroniczna ewidencja pracownicza	Składowana na potrzeby kadrowe
2.	Dane uczniów	Imię, imiona, nazwisko, data urodzenia, miejsce urodzenia, imiona rodziców, adres zamieszkania, PESEL	Papierowa i elektroniczna ewidencja	Na potrzeby szkoły
3.	Rejestr uczniów	Imię, imiona, nazwisko, data urodzenia, miejsce urodzenia, imiona rodziców, adres zamieszkania, PESEL	Papierowa i elektroniczna ewidencja	Na potrzeby szkoły
4.	Zamówienia publiczne	Nazwa firmy, adres, nr telefonu	Ewidencja papierowa	Na potrzeby szkoły
5.	Archiwum	Tak jak w pkt. 1 i 2 oraz dane księgowe	Ewidencja papierowa	Na potrzeby szkoły
6.	Upoważnienia do odbioru dzieci	Imię i nazwisko opiekunów odbierających dzieci	Ewidencja papierowa	Na potrzeby szkoły
7.	Rejestr korespondencji	Pisma przychodzące i wychodzące, nr korespondencji, nazwa	Ewidencja papierowa	Na potrzeby szkoły
8.	Dane kontrahenta	Nazwa firmy, NIP, termin płatności, nr konta, nazwa banku	Ewidencja papierowa	Na potrzeby szkoły
9.	Kopie faktur	Nazwa firmy, NIP, termin płatności, nr konta, nazwa banku	Ewidencja papierowa	Na potrzeby szkoły
10.	Dane serwisu internetowego szkoły		Ewidencja elektroniczna	Składowana na potrzeby wizerunku szkoły

ZAŁĄCZNIK NR 6

Rejestr czynności przetwarzania danych osobowych

DANE ADMINISTRATORA, IOD		DANE KONTAKTOWE
Nazwa administratora	Szkoła Podstawowa im. Fryderyka Chopina	Ul. Chopina 99, 96-500 Sochaczew Tel. (46) 863-37-77
Imię i nazwisko inspektora ochrony danych	Iwona Woźnicka-Pietrzak	Tel. (46) 863-37-77

Kategorie osób, których dane dotyczą	**Kategorie danych osobowych**	**Cel przetwarzania danych osobowych**	**Odbiorca lub kategoria odbiorców, którym mogą być przekazywane dane osobowe**	**Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**	**Informacja dotyczącą przekazywania danych do państwa trzeciego**	**Planowane terminy usunięcia danych**
Kandydaci, rodzice/opie-kunowie prawni	Imię, nazwisko, data urodzenia oraz numer PESEL kandydata (w przypadku braku numeru PESEL - serię i numer paszportu lub innego dokumentu potwierdzającego tożsamość); adres poczty elektronicznej i numery telefonów rodziców kandydata , oświadczenie o miejscu zamieszkania rodziców kandydata i kandydata, oświadczenie o wielodzietności rodziny kandydata, orzeczenie o potrzebie kształcenia specjalnego wydane ze względu na niepełnosprawność, orzeczenie o	Przeprowa-dzenie rekrutacji do szkoły podstawowej	Dane nie są przekazywane innym odbiorcom	Zamykane na klucz szafy w zamykanym gabinecie dostępnym tylko dla upoważnionych osób, kontrola dostępu do systemu informatycznego, dostępy tylko dla	Dane nie są przekazywane	1 rok [art. 160 ust. 2 ustawy z 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz. 59)]

	niepełnosprawności lub o stopniu niepełnosprawności lub orzeczenie równoważne, prawomocny wyrok sądu rodzinnego orzekający rozwód lub separację lub akt zgonu oraz oświadczenie o samotnym wychowywaniu dziecka oraz niewychowywaniu żadnego dziecka wspólnie z jego rodzicem, dokument poświadczający objęcie dziecka pieczą zastępczą			upoważnionych osób, system antywirusowy		
Uczniowi, rodzice/opie-kunowie prawni	Dane identyfikacyjne ucznia (imię, nazwisko, data i miejsce urodzenia, numer PESEL), adres zamieszkania ucznia, Dane o rodzicach (imię, nazwisko adres zamieszkania - jeżeli są różne od adresu zamieszkania ucznia), Datę rozpoczęcia nauki, oddział do którego przyjęto oraz datę ukończenia szkoły albo datę i przyczynę jej opuszczenia	Prowadzenie księgi uczniów, rejestracja tematów zajęć i przebiegu nauczania	Dane są przekazywane do Systemu Informacji Oświatowej na podstawie art. 14 Ustawy z dnia 15 kwietnia 2011 r. o Systemie Informacji Oświatowej Dz. U. 2017, poz. 2159)	Ściśle kontrolowany dostęp do danych - dostęp tylko dla uprawnionych, zarejestrowanych użytkowników. Komputery używane do dostępu do danych zabezpieczono przed atakami z sieci zewnętrznej systemem antywirusowym. Transmisja danych do oraz z serwera bazy danych systemu zabezpieczona jest kryptograficznie.	Dane nie są przekazywane	Po okresie pobierania nauki dokumenty trafiają do składnicy akt
Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych	Rekrutacja pracowników	Dane nie są przekazywane innym odbiorcom	Zamykane na klucz szafy w gabinetach zamykanych, dostępnych tylko dla upoważnionych osób	Dane nie są przekazywane	Po zakończeniu okresu rekrutacji

Pracownicy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem Pracy; dane o Oddziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA -zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA -zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny; dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zajęcia komornicze itp.) numery kont dla przelewów bankowych pracownika	Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy; przekazywanie informacji o zwolnieniach	ZUS, MZEA	Zamykane na klucz szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, system antywirusowy.	Dane nie są przekazywane	50 lat, po tym czasie dokumenty trafiają do składnicy akt

ZAŁĄCZNIK NR 7

Komunikat o naruszeniu ochrony danych w Szkole Podstawowej nr 7 im. Fryderyka Chopina w Sochaczewie

Komunikat o naruszeniu ochrony danych osobowych z dnia ……

1.	**Charakter naruszenia ochrony danych:**	
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	
3.	**Liczba wpisów, których dotyczy naruszenie:**	
4.	**Możliwe konsekwencje naruszenia ochrony danych:**	
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	

……..

(podpis dyrektora w imieniu administratora danych)

ZAŁĄCZNIK NR 8

Zgłoszenie naruszenia ochrony danych osobowych Prezesowi UODO

……..
(miejscowość, data)

Administrator danych
.....

Urząd Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

ZGŁOSZENIE
W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016r., zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu …… w Szkole Podstawowej nr 7 im. Fryderyka Chopina w Sochaczewie.

1.	**Charakter naruszenia ochrony danych:**	
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	
3.	**Liczba wpisów, których dotyczy naruszenie:**	

4.	**Możliwe konsekwencje naruszenia ochrony danych:**	
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	
6.	**Dane inspektora ochrony danych**	

……

(podpis dyrektora)

ZAŁĄCZNIK NR 9

……., dn……..

…….
(imię i nazwisko pracownika)

OŚWIADCZENIE

1. Oświadczam, że znana mi jest treść:

a) Dokumentacji ochrony danych osobowych obowiązującej w Szkole Podstawowej nr 7 w Sochaczewie, zawartej w Polityce Bezpieczeństwa i Instrukcji Przetwarzania Danych Osobowych,
b) Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926 ze zmianami),
c) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

2. Jednocześnie zobowiązuję się nie ujawniać informacji, z którymi zapoznałam się w związku z wykonywaną pracą, a w szczególności nie będę:

a) ujawniać danych zawartych w zbiorach danych, do których uzyskałam dostęp za upoważnieniem administratora danych,
b) ujawniać szczegółów technologicznych używanych w systemach informatycznych oraz oprogramowania,
c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą dokumentacją.

……..……. ……
(data, miejscowość) *(podpis pracownika)*

ZAŁĄCZNIK NR 10

……., dn……..

UPOWAŻNIENIE
do przetwarzania danych osobowych

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)

- udziela się Pani/Panu[1]:

……
(imię i nazwisko pracownika)

……
(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem jest Szkoła Podstawowa nr 7 w Sochaczewie oraz do przetwarzania danych osobowych powierzonych szkole przez podmioty trzecie.

Jest Pan/Pani[1] upoważniony/upoważniona[1] do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani[1] zadań oraz polecenia służbowego.

Upoważnienie traci moc z chwilą ustania stosunku pracy.

……
…
(data i podpis Administratora Bezpieczeństwa Informacji)

[1] Niepotrzebne skreślić

ZAŁĄCZNIK NR 11

……., dn……..

ODWOŁANIE UPOWAŻNIENIA
do przetwarzania danych osobowych

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)

- odwołuje się z dniem …….
……

upoważnienie do przetwarzania danych osobowych, których Administratorem jest Szkoła Podstawowa nr 7 w Sochaczewie oraz do przetwarzania danych osobowych powierzonych szkole przez podmioty trzecie wystawione dla Pani/Pana:

……
(imię i nazwisko pracownika)

……
(stanowisko służbowe)

……
…
(data i podpis Administratora Bezpieczeństwa Informacji)

ZAŁĄCZNIK NR 12

……., dn……..

RAPORT
z naruszenia bezpieczeństwa danych osobowych

1. Data…….Godzina……
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   ……
   (Imię i nazwisko, stanowisko służbowe)
3. Lokalizacja zdarzenia
   ……...
   ……
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące ……
   ……
   ……
   ……
5. Przyczyny wystąpienia zdarzenia……..
   ……
   ……
6. Podjęte działania ……..
   ……..
   ……..
7. Postępowanie wyjaśniające ……

…….
…….

……
…
(data i podpis Administratora Bezpieczeństwa Informacji)