Załącznik
do Zarządzenia nr 3/2018/2019 Dyrektora Szkoły Podstawowej nr 5 w Nowym Dworze Mazowieckim
z dnia 10.09.2018 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Szkoły Podstawowej nr 5
im. Janusza Kusocińskiego
w Nowym Dworze Mazowieckim

SPIS TREŚCI

PODSTAWA PRAWNA

1. Konstytucja RP (art. 47 i 51).
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).
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).
4. Kodeks pracy.

PODSTAWOWE POJĘCIA

Szkoła – w tym dokumencie jest rozumiana jako Szkoła Podstawowa nr 5 im. Janusza Kusocińskiego w Nowym Dworze Mazowieckim, ul. Chemików 1a;
Polityka – w tym dokumencie jest rozumiana jako „Polityka bezpieczeństwa" obowiązująca w Szkole Podstawowej nr 5 im. Janusza Kusocińskiego w Nowym Dworze Mazowieckim;
Instrukcja – w tym dokumencie rozumiana jest jako „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej nr 5 im. Janusza Kusocińskiego w Nowym Dworze Mazowieckim;
Administrator Danych Osobowych (ADO) –Szkoła Podstawowa nr 5 im. Janusza Kusocińskiego w Nowym Dworze Mazowieckim, której przedstawicielem jest dyrektor;
Inspektor Ochrony Danych Osobowych (IODO) – pracownik szkoły wyznaczony przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony danych osobowych, oraz przygotowania dokumentów wymaganych przez przepisy o ochronie danych osobowych w Szkole Podstawowej nr 5 im. Janusza Kusocińskiego w Nowym Dworze Mazowieckim. IODO powołany jest zarządzeniem Dyrektora Szkoły Podstawowej nr 5 im. Janusza Kusocińskiego w Nowym Dworze Mazowieckim;
Administrator Systemu Informatycznego (ASI) – osoba odpowiedzialna za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w tym systemie;
Użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole;
Identyfikator użytkownika – jest to ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
Zabezpieczenie danych w systemie informatycznym – wdrożenie i wykorzystywanie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
Wysoki poziom bezpieczeństwa – musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną,
Sieć lokalna – połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych;
Sieć publiczna – sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z poźn. zm.).

1. Wykaz miejsc, w których przetwarzane są dane osobowe

LP.	ADRES – BUDYNEK	POMIESZCZENIA	ZABEZPIECZENIE
1.	ul. Chemików 1a 05-100 Nowy Dwór Mazowiecki	• gabinet dyrektora	• kluczami dysponuje dyrektor i sekretarz szkoły • klucze przechowywane są w portierni w zamkniętej skrzynce na klucze – kluczem dysponuje portier
		• gabinet wicedyrektora	• kluczami dysponuje dwóch wicedyrektorów • klucze przechowywane są w portierni w zamkniętej skrzynce na klucze – kluczem dysponuje portier
		• sekretariat	• kluczami dysponuje dyrektor i sekretarz szkoły • klucze przechowywane są w portierni w zamkniętej skrzynce na klucze – kluczem dysponuje portier
		• gabinet pedagoga • gabinet psychologa • gabinet logopedy	• kluczami dysponuje pedagog / psycholog / logopeda • klucze przechowywane są w portierni w zamkniętej skrzynce na klucze – kluczem dysponuje portier
		• gabinet pielęgniarki szkolnej	• kluczami dysponuje pielęgniarka • klucze przechowywane są w portierni w zamkniętej skrzynce na klucze – kluczem dysponuje portier
		• biblioteka	• kluczami dysponuje bibliotekarz • klucze dostępne w pokoju nauczycielskim
		• pokój nauczycielski	• drzwi wyposażone w zamek elektroniczny – 4 cyfrowy – nauczyciele mają przydzielone kody dostępu • zapasowy klucz znajduje się w portierni – kluczem dysponuje dyrektor
		• pokój nauczycieli w-f	• kluczami dysponują nauczyciele wychowania fizycznego • klucze dostępne w portierni
		• sale lekcyjne	• kluczami dysponują nauczyciele • klucze dostępne w pokoju nauczycielskim • zapasowe klucze dostępne w portierni

		• świetlica	• kluczami dysponują nauczyciele świetlicy • klucze dostępne w portierni
		• kierownik gospodarczy	• kluczami dysponuje kierownik • klucze dostępne w portierni
		• księgowość i kadry	• kluczami dysponuje księgowa / kadrowa • klucze dostępne w portierni
		• główny księgowy	• kluczami dysponuje główna księgowa • klucze dostępne w portierni
		• kasa	• kluczami dysponuje kasjer • klucze dostępne w portierni
		• archiwum	• kluczami dysponuje dyrektor • klucze dostępne są w portierni

Klucze dostępne w portierni przechowywane są w zamkniętej szafce, portiernia zamykana jest na klucz, kluczem dysponuje starszy woźny lub portier/stróż nocny.

2. Dane przetwarzane w systemach informatycznych

KATEGORIE OSÓB KTÓRYCH DANE SĄ PRZETWARZENE	**RODZAJ OPROGRAMOWANIA**	**MIEJSCA PRZETWARZANIA**	**OSOBY PRZETWARZAJĄCE DANE**
Pracownicy	SIO VULCAN MS Office (Word, Excel, Outlook)	sekretariat księgowość / kadry gabinet dyrektora gabinet wicedyrektora	sekretarz szkoły księgowy / karowy dyrektor wicedyrektor
Rodzice	MS Office (Word, Excel, Outlook)	sekretariat księgowość / kadry gabinet dyrektora gabinet wicedyrektora kierownik gospodarczy	sekretarz szkoły księgowy / karowy dyrektor wicedyrektor kierownik gospodarczy
	VULCAN e-dziennik	sekretariat gabinet dyrektora gabinet wicedyrektora wszystkie sale lekcyjne sale gimnastyczne pokój nauczycielski gabinety specjalistów	sekretarz szkoły dyrektor wicedyrektor nauczyciele nauczyciele nauczyciele n-le specjaliści
Kontrahenci / dostawcy / wykonawcy usług	MS Office (Word, Excel, Outlook)	sekretariat księgowość / kadry gabinet dyrektora gabinet wicedyrektora kierownik gospodarczy	sekretarz szkoły księgowy / karowy dyrektor wicedyrektor kierownik gospodarczy
Uczniowie	SIO	sekretariat księgowość/kadry	sekretarz szkoły księgowy / kadrowy

	VULCAN	sekretariat gabinet dyrektora gabinet wicedyrektora wszystkie sale lekcyjne sale gimnastyczne pokój nauczycielski gabinety specjalistów	sekretarz szkoły dyrektor wicedyrektor nauczyciele nauczyciele pokój nauczycielski n-le specjaliści
	VULCAN MOL-net	biblioteka	n-l bibliotekarz
	MS Office (Word, Excel, Outlook)	sekretariat gabinet dyrektora gabinet wicedyrektora wszystkie sale lekcyjne sale gimnastyczne pokój nauczycielski gabinety specjalistów kierownik gospodarczy	sekretarz szkoły dyrektor wicedyrektor nauczyciele nauczyciele pokój nauczycielski n-le specjaliści kierownik gospodarczy
Specjaliści spoza szkoły – sąd, poradnia, policja, inne instytucje	MS Office (Word, Excel, Outlook)	sekretariat gabinet dyrektora gabinet wicedyrektora gabinet pedagoga	sekretarz szkoły dyrektor wicedyrektor pedagog

3. Zbiory danych przetwarzanych tradycyjnie

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	MIEJSCE PRZETWARZANIA /ODPOWIE-DZIALNY	MIEJSCE PRZECHO-WYWANIA	ZABEZPIECZENIE
Pracownicy	Akta osobowe	księgowość/kadry kadrowa	księgowość/ kadry	szafa pancerna, klucz u kadrowej
	Ewidencja akt osobowych	księgowość/kadry kadrowa	księgowość/ kadry	szafa pancerna, klucz u kadrowej
	Orzeczenia lekarskie do celów sanitarno-epidemiologicznych	księgowość/kadry kadrowa	księgowość/ kadry	szafa pancerna, klucz u kadrowej
	Oświadczenia i wnioski do funduszu socjalnego	księgowość/kadry kadrowa	księgowość/ kadry	szafa pancerna, klucz u kadrowej
	Listy obecności pracowników	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz
	Zaświadczenia	sekretariat /sekretarz szkoły	sekretariat	szafa pancerna, klucz u sekretarza szkoły

	Protokoły powypadkowe pracowników	księgowość/kadry kadrowa	księgowość/ kadry	szafa pancerna, klucz u kadrowej
	Dokumentacja bhp	gabinet dyrektora/ dyrektor szkoły, inspektor bhp	gabinet dyrektora	szafa na klucz, klucz u dyrektora / inspektora bhp
	Arkusz organizacyjny	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Dokumentacja nadzoru pedagogicznego	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Dokumentacja awansów zawodowych nauczycieli	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz, klucz u dyrektora
	Ewidencja zwolnień lekarskich;	księgowość/kadry kadrowa	księgowość/ kadry	szafka na klucz, klucz u kadrowej
	Podania; życiorysy/CV	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz, klucz u dyrektora
	Notatki służbowe	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Dokumentacja dotycząca polityki kadrowej – opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp.;	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz, klucz u dyrektora
	Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
Uczniowie	Dokumentacja uczniów; Karty zapisu dziecka/ucznia	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Księga uczniów	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły

	Księga dzieci	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Arkusze ocen	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Dzienniki nauczania indywidualnego	pokój nauczycielski, sale lekcyjne/ wychowawca, nauczyciele	nauczyciele / wychowawcy	szafka w pokoju nauczycielskim zamykanym drzwiami z elektronicznym zamkiem zatrzaskowym, nauczycielom przydzielono kody dostępu do pokoju
	Dziennik wychowawcy świetlicy	świetlica/ wychowawcy świetlicy	świetlica	szafka na klucz
	Dziennik pedagoga	gabinet pedagoga/ pedagog	gabinet pedagoga	szafka na klucz
	Pomoc społeczna, stypendia, wyprawki, obiady	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz
	Księga wydanych legitymacji i legitymacje	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Księga wydanych kart rowerowych i karty rowerowe	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Rejestr zaświadczeń i zaświadczenia	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz
	Księga absolwentów	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Świadectwa i duplikaty	sekretariat /sekretarz szkoły	sekretariat	szafka na klucz, klucz u sekretarza szkoły
	Protokoły powypadkowe	sekretariat /sekretarz szkoły	sekretariat	gabinet pedagoga/ pielęgniarki szkolnej
	Karta zdrowia ucznia	gabinet pedagoga/ pielęgniarki szkolnej; pielęgniarka	gabinet pedagoga/ pielęgniarki szkolnej	szafka na klucz
	Karty szczepień	gabinet pedagoga/ pielęgniarki szkolnej; pielęgniarka	gabinet pedagoga/ pielęgniarki szkolnej	szafka na klucz
	Karty biblioteczne	biblioteka	biblioteka	szafka na klucz

		n-l bibliotekarz		
	Dokumentacja pomocy psychologiczno - pedagogicznej (opinie, orzeczenia)	gabinet pedagoga szkolnego,	sekretariat, gabinet pedagoga szkolnego	szafa na klucz
	Ewidencja uczniów przystępujących do egzaminów zewnętrznych	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafa na klucz, klucz u dyrektora
	Dokumenty zarchiwizowane	sekretariat/ Sekretarz szkoły	pomieszczenie gospodarcze	pomieszczenie zabezpieczona, klucze dostępne w sekretariacie
	Protokoły rad pedagogicznych, księga uchwał;	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafa stalowa, klucz u dyrektora
	Umowy zawierane z osobami fizycznymi;	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Ewidencja decyzji – zwolnienia z obowiązkowych zajęć, odroczenia obowiązku szkolnego	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafa stalowa, klucz u dyrektora
	Deklaracje uczęszczania na religię, sprzeciw od zajęć z wychowania do życia w rodzinie	gabinet dyrektora szkoły/dyrektor szkoły	gabinet dyrektora szkoły	szafa stalowa, klucz u dyrektora

4. System przetwarzania danych osobowych

„DANE OSOBOWE” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

„PRZETWARZANIE” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie,

rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

W skład systemu wchodzą:

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

Sposób przepływu danych pomiędzy poszczególnymi systemami:

- przenoszenie,
- eksport/import danych,
- kopiowanie,
- usuwanie,
- generowanie w postaci list do wydruków

MS Office → VULCAN → MS Office
VULCAN → PDF (Acrobat Reader lub inny)
MS Office – SIO

Sposób przekazywania danych: manualny

Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu wysokiego poziom bezpieczeństwa.

5. Cele i zasady funkcjonowania polityki bezpieczeństwa

Realizując Politykę bezpieczeństwa informacji zapewnia się:

1. **zgodność przetwarzania danych osobowych z prawem, rzetelność i przejrzystość procesu** - rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2. **ograniczenie celu przetwarzania danych** – dane będą zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie może odbywać się do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub statystycznych;
3. **minimalizację danych** – dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4. **prawidłowość przetwarzania danych** – dane muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
5. **ograniczenie przechowywania** – dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie

publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą;

6. **integralność i poufność** – dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
7. **rozliczalność** - administrator danych osobowych jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie.

Polityka bezpieczeństwa informacji w Szkole Podstawowej nr 5 w Nowym Dworze Mazowieckim ma na celu zredukowanie możliwości wystąpienia naruszeń bezpieczeństwa prowadzących do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych i ich negatywnych konsekwencji w tym zakresie, tj.:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji Szkoły;
4) strat finansowych ponoszonych w wyniku nałożonych kar;
5) 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, aby dane te były:

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

6. Prawa osób, których dane osobowe są przetwarzane

1. Prawo dostępu do informacji czy i w jakim zakresie przetwarzane są jego dane osobowe.
2. Prawo do sprostowania danych osobowych.
3. Prawo do usunięcia danych – prawo do bycia zapomnianym.
4. Prawo do ograniczenia przetwarzania.
5. Prawo do przenoszenia danych.
6. Prawo do sprzeciwu wobec przetwarzania danych w sposób zautomatyzowany i profilowanie.

7. Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grożą sankcje wynikająca z przepisów RODO i kary pracownicze na zasadach określonych w kodeksie pracy.

Administrator Danych Osobowych (ADO) – Dyrektor Szkoły:

- formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- wyznacza inspektora ochrony danych osobowych,
- decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik,**
- odwołuje upoważnienie**,**
- odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.
- prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny,
- ułatwia podmiotom danych wykonywanie ich praw,
- nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie, czas na udzielenie informacji przez ADO to maksymalnie miesiąc,
- weryfikuje tożsamość osób wnoszących żądania udzielenia informacji,
- potwierdza, czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli to następuje, udziela wskazanych rozporządzeniem informacji,
- ułatwia osobie, której dane dotyczą, wykonywanie jej praw,
- informuje osobę, której dane dotyczą, o działaniach, jakie podjął, w związku z jej żądaniami opartymi,
- uzasadnia odrzucenie żądania osoby, której dane dotyczą, i poucza ją o prawie skargi,
- umożliwia dostęp do jej danych osobie, której one dotyczą,
- dokonuje sprostowania i uzupełniania danych,
- usuwa dane,
- ogranicza przetwarzanie danych,
- powiadamia o sprostowaniu lub usunięciu danych osobowych bądź o ograniczeniu ich przetwarzania,
- dokonuje przenoszenia danych.

Inspektor Ochrony Danych (IOD) – pracownik Szkoły wyznaczony przez Dyrektora:

- egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Szkole w imieniu ADO,
- prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa **załącznik,**
- ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik**,

- określa potrzeby w zakresie stosowanych w Szkole zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,
- udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
- informowanie administratora oraz pracowników o obowiązkach związanych z ochroną danych osobowych (o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych) i doradzanie im w tej sprawie,
- monitoruje proces przetwarzania danych osobowych zachodzących w szkole,
- przeprowadza audyty,
- monitoruje operacje przetwarzania danych osobowych w systemach informatycznych,
- dokonuje oceny ryzyka związanego z przetwarzaniem danych osobowych,
- współpracuje z organem nadzorczym,
- pełni funkcję punktu kontaktowego w kwestiach związanych z przetwarzaniem danych osobowych w placówce.

Administrator Systemu Informatycznego (ASI) – pracownik Szkoły wyznaczony przez Dyrektora:

- zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami IOD,
- doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
- przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
- nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ADO:

- chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły,
- zapoznaje się zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów.

8. Zasady udzielania dostępu do danych osobowych

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

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

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

9. Udostępnianie i powierzanie danych osobowych

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

Udostępnienie danych może nastąpić **na pisemny wniosek** zawierający następujące elementy:

- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

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

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

10. Udzielenie informacji na temat przetwarzania danych osobowych

Każda osoba fizyczna, ma prawo zwrócić się z **wnioskiem** do administratora o udzielenie informacji, czy przetwarzane są jej dane osobowe. Jeżeli ma to miejsce, osoba ta jest także uprawniona do uzyskania dostępu do tych danych oraz następujących informacji:

a) cele przetwarzania;
b) kategorie przetwarzanych danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców;
d) planowany okres przechowywania danych osobowych lub kryteria ustalania tego okresu;
e) o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz o zasadach ich podejmowania, znaczeniu i przewidywanych konsekwencjach takiego przetwarzania.

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę.

Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Prawo do uzyskania kopii, nie może niekorzystnie wpływać na prawa i wolności innych.

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

11. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

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

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

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

12. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

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

13. Analiza ryzyka związanego z przetwarzaniem danych osobowych

RYZYKO: Możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia.

Ryzyko przetwarzania danych osobowych:

- zniszczenie (zn)
- utracenie (ut)
- zmodyfikowanie (zm)
- nieuprawnione ujawnienie (nu)
- nieuprawniony dostęp (nd)

Identyfikacja zagrożeń

Rys. 1 Poradnik RODO „Podejście oparte na ryzyku, cz. 2. - GIODO, grudzień 2017 r.

Skutek	Poziom	Opis	
		finanse	reputacja
Bardzo wysoki	5	powyżej 1 mln zł	negatywne opinie w mediach międzynarodowych
Wysoki	4	w zakresie 500 tys. – 1 mln zł	negatywne opinie w mediach krajowych
Średni	3	w zakresie 100 – 500 tys. zł	negatywne opinie w mediach lokalnych
Niski	2	w zakresie 5 – 100 tys. zł	negatywne opinie bez udziału mediów
Bardzo niski	1	poniżej 5 tys. zł	brak wpływu na reputację

Tabela 1. Przykładowe skutki ze względu na finanse i reputację

Prawdopodobieństwo	Poziom	Opis
Prawie pewne	5	zdarzenie występuje co najmniej raz w tygodniu
Prawdopodobne	4	zdarzenie występuje co najmniej raz w miesiącu
Możliwe	3	zdarzenie występuje co najmniej raz na kwartał
Mało prawdopodobne	2	zdarzenie występuje co najmniej raz na pół roku
Rzadkie	1	zdarzenie nie występuje lub występuje raz w roku

Tabela 2. Przykładowe prawdopodobieństwo wystąpienia zdarzenia

			SKUTEK				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			1	2	3	4	5
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	Ś	W	W

	Poziom ryzyka	Opis działania
	Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
	Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
	Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
	Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

Tabela 3. Przykładowa macierz ryzyka

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA	Prawdo-podo-bieństwo	Skutek	Poziom ryzyka
dane przetwarzane w sposób tradycyjny	oszustwo, kradzież, sabotaż;	1	2	N
	zdarzenia losowe (powódź, pożar);	1	1	N
	zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);	3	1	N
	niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;	1	2	N
	pokonanie zabezpieczeń fizycznych;	1	1	N
	podsłuchy, podglądy;	2	1	N
	ataki terrorystyczne;	1	1	N
	brak rejestrowania udostępniania danych;	1	2	N
	niewłaściwe miejsce i sposób przechowywania dokumentacji;	3	1	N
dane przetwarzane w systemach informatycznych	nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów;	3	1	N
	niewłaściwa administracja systemem;	2	1	N
	niewłaściwa konfiguracja systemu;	2	1	N
	zniszczenie (sfałszowanie) kont użytkowników;	1	1	N
	kradzież danych kont;	1	1	N
	pokonanie zabezpieczeń programowych;	1	1	N

	zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);	3	1	N
	niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;	1	2	N
	zdarzenia losowe (powódź, pożar);	1	1	N
	niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych;	2	1	N
	naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione;	2	1	N
	przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci;	2	1	N
	przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci;	2	1	N
	przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych	3	1	N
	brak rejestrowania zdarzeń tworzenia lub modyfikowania danych;	3	1	N

14. Sposób zabezpieczenia danych

FORMA PRZETWARZANIA DANYCH	**STOSOWANE ŚRODKI OCHRONY**
dane przetwarzane w sposób tradycyjny	• przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; • przechowywanie danych osobowych w szafach zamykanych na klucz; • przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ADO; • zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania; • wprowadzenie polityki czystego biurka; • szkolenia okresowe pracowników w zakresie ochrony danych osobowych;
dane przetwarzane w systemach informatycznych	• kontrola dostępu do systemów; • zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; • systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; • składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach;

	• przydzielenie pracownikom indywidualnych kont użytkowników i haseł; • stosowanie indywidualnych haseł logowania do poszczególnych programów; • właściwa budowa hasła; • okresowe testowanie zastosowanych rozwiązań;

15. Określenie wielkości ryzyka

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

16. Identyfikacja obszarów wymagających szczególnych zabezpieczeń

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, mimo niskiego poziomu ryzyka naruszenia ochrony danych osobowych, stosuje się podwyższony poziom bezpieczeństwa. Administrator Danych Osobowych i Administrator Systemów Informatycznych przeprowadzają **okresową analizę ryzyka dla poszczególnych systemów** i na tej podstawie przedstawiają Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia stałej ochrony przetwarzanym danym.

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

1.1. Dane osobowe w systemach informatycznych może przetwarzać wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.
1.2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada Administrator Systemów Informatycznych.
1.3. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ABI.
1.4. 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.
1.5. 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.

2.1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system co 60 dni.
2.2. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.
2.3. Na komputerach wykorzystywanych do przetwarzania danych osobowych stosuje się szyfrowanie dysków twardych, programy pocztowe zostały przekonfigurowane z wykorzystaniem szyfrowania SSL, a dane przesyłane pocztą elektroniczną powinny dodatkowo być spakowane w zahasłowane archiwa 7zip.
2.4. Jeżeli do przenoszenia danych osobowych będą wykorzystywane nośniki zewnętrzne powinny one posiadać sprzętową opcję szyfrowania (np. szyfrowane pendrivy).
2.5. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
    2.5.1. rozpoczęcie i zakończenie pracy przez użytkownika systemu,
    2.5.2. operacje wykonywane na przetwarzanych danych,
    2.5.3. przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
    2.5.4. nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,

2.5.5. błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

2.6. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
2.6.1.identyfikatora osoby, której dane dotyczą,
2.6.2.osoby przesyłającej dane,
2.6.3.odbiorcy danych,
2.6.4.zakresu przekazanych danych osobowych,
2.6.5.daty operacji,
2.6.6.sposobu przekazania danych.

2.7. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe.

2.8. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada ASI.

3. Zasady bezpieczeństwa podczas pracy w systemie informatycznym:

3.1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
3.1.1. loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła,
3.1.2. loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.

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

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

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

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

3.6. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:
3.6.1.podejrzenia naruszenia bezpieczeństwa systemu;
3.6.2.braku możliwości zalogowania się użytkownika na jego konto;
3.6.3.stwierdzenia fizycznej ingerencji w przetwarzana dane;
3.6.4.stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

3.7. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:
3.7.1.nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);

3.7.2. wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
3.7.3. różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
3.7.4. inne nadzwyczajne sytuacje.

4. Tworzenie kopii zapasowych

4.1. Kopie zapasowe wykonywane są do zaszyfrowanych archiwów 7.zip, dostęp do danych w celu ich przywrócenia będzie możliwy po zalogowaniu się na konto administratora hasłem, które będzie zmieniane po każdorazowym użyciu. Hasło będzie przekazywane do Dyrekcji i udostępniane ASI w przypadku zaistnienia sytuacji wymagającej przywrócenia danych z kopii zapasowej.
4.2. Pełne kopie zapasowe zbiorów danych tworzone są 4 razy w ciągu roku.
4.3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
4.4. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest ASI.
4.5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.
4.6. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

5. Udostępnienie danych.

5.1. Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.
5.2. Do podmiotów, dla których dopuszczalne jest udostępnianie danych przez szkołę należą:
5.2.1. Organ Nadzorujący [w związku z awansem zawodowym, wyniki badań psychologiczno-pedagogicznych dzieci i młodzieży],
5.2.2. Organ Prowadzący [wykaz z czasem pracy pracowników, udostępnianie dzienników zajęć, wykazy wygenerowane z SIO],
5.2.3. Dzienniki lekcyjne [dane rodziców w zakresie opisanym rozporządzeniem]
5.2.4. Strona www [dane osobowe ucznia i np. jego osiągnięcia, publikowanie list z wynikami, ocenami, zdjęciem – tylko za zgodą],
5.2.5. Szkolna tablica ogłoszeń [publikowanie list z wynikami, ocenami, zdjęciem – tylko za zgodą],
5.2.6. Formularz zgłoszeniowy do szkoły [dane osobowe: nr telefonu, PESEL dziecka, itp. – tylko za zgodą],
5.2.7. Podmioty świadczące usługi w zakresie oświaty [w zależności od celu],

6. Przeglądy i konserwacje systemów

6.1. Przeglądy i konserwacje tj. testy zabezpieczeń, testy kondycji dysków twardych i innych podzespołów, testy temperatur oraz wydajności systemów operacyjnych, wykonywane są raz w miesiącu (na koniec miesiąca).
6.2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.
6.3. Prace te powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
6.4. Przed rozpoczęciem prac przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

7. Niszczenie wydruków i nośników danych

7.1. 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 / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski).
7.2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
7.3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

1. Istota naruszenia danych osobowych

1.1. 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:

1.1.1. nieautoryzowany dostęp do danych,

1.1.2. nieautoryzowane modyfikacje lub zniszczenie danych,

1.1.3. udostępnienie danych nieautoryzowanym podmiotom,

1.1.4. nielegalne ujawnienie danych,

1.1.5. pozyskiwanie danych z nielegalnych źródeł.

2. Postępowanie w przypadku naruszenia danych osobowych.

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

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

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

2.4. IOD podejmuje następujące kroki:

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

2.4.2. 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,

2.4.3. rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu ADO,

2.4.4. nawiązuje kontakt ze specjalistami spoza Szkoły (jeśli zachodzi taka potrzeba).

2.5. IOD dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik** i przekazuje go ADO.

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

3. Sankcje karne

3.1. 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.

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

Załączniki

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych
Załącznik nr 2 – Rejestr osób upoważnionych do przetwarzania danych osobowych i rejestr osób upoważnionych do przebywania w miejscu przetwarzania danych osobowych
Załącznik nr 3 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych
Załącznik nr 4 – Informacja o zawartości zbioru danych
Załącznik nr 5 – Raportu z naruszenia bezpieczeństwa danych osobowych

_____ Nowy Dwór Mazowiecki, dnia 25.05.2018 r.

(pieczęć Szkoły)

UPOWAŻNIENIE nr 01/2018
do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) – dalej RODO (GDPR), niniejszym upoważniam do przetwarzania danych osobowych:

(imię, nazwisko)

nauczyciel

(stanowisko)

w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Upoważnienie obejmuje uprawnienie do przetwarzania danych poprzez zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, usuwanie danych osobowych uczniów rodziców i prawnych opiekunów oraz nauczycieli w systemie dziennika elektronicznego, w arkuszach ocen, wykazach i innych dokumentach szkolnych zgodnie z przepisami prawa oświatowego.
Upoważnienie obejmuje następujące kategorie danych osobowych: dane identyfikacyjne ucznia (nazwisko, imiona, data i miejsce urodzenia, numer PESEL, adres poczty elektronicznej), adres zamieszkania i zameldowania, dane o stanie zdrowia, dane o rodzicach (imię, nazwisko adres zamieszkania, adresy poczty elektronicznej, numery telefonów), imiona i nazwiska nauczycieli prowadzących zajęcia.

Okres ważności upoważnienia:

od: 25.05.2018 r. do odwołania upoważnienia

_____
(Administrator Danych Osobowych)

Przyjmuję do wiadomości i stosowania.

_____
(Podpis osoby upoważnionej)

Prowadzony w formie elektronicznej w arkuszu kalkulacyjnym Ms Excel

REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upowa-żnienia	Imię i nazwisko	Identyfikator użytkownika*	Kategorie osób	Data nadania upoważnienia	Data odwołania upoważnienia	Uwagi

* Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie

Prowadzony w formie elektronicznej w arkuszu kalkulacyjnym Ms Excel

REJESTR OSÓB UPOWAŻNIONYCH DO PRZEBYWANIA W MIEJSCU PRZETWARZANIA DANYCH OSOBOWYCH

Nr upowa-żnienia	Imię i nazwisko	Data nadania upoważnienia	Data odwołania upoważnienia	Uwagi

_____ Nowy Dwór Mazowiecki, dnia _____ r.
(imię i nazwisko)

_____
(stanowisko)

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Szkole zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa informacji Szkoły Podstawowej nr 5 im. J. Kusocińskiego w Nowym Dworze Mazowieckim" i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole.

Zostałem/am zapoznany/a z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – RODO, oraz przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 10 i 11 Ustawy o ochronie danych osobowych, odpowiedzialności cywilnej, administracyjnej i karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Szkole Podstawowej nr 5 im. J. Kusocińskiego w Nowym Dworze Mazowieckim może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

_____
(czytelny podpis pracownika)

Nowy Dwór Maz., dnia _____ r.

_____
(pieczęć Szkoły)

_____
(imię i nazwisko)

_____

_____
(adres)

INFORMACJA
o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia _____ r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Szkole Podstawowej nr 5 im. J. Kusocińskiego w Nowym Dworze Mazowieckim, działając na podstawie art. 15 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1), informuję, że zbiór danych zawiera następujące Pani/Pana kategorie danych osobowych: _____
_____

Powyższe dane przetwarzane są w Szkole Podstawowej nr 5 im. J. Kusocińskiego w Nowym Dworze Mazowieckim w celu _____
_____
z zachowaniem wymaganych zabezpieczeń i zostały uzyskane _____ (podać sposób).

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

Zgodnie art. 15 ust. 1 pkt e-f RODO (Dz.U.UE.L.2016.119.1), przysługuje Pani/Panu prawo sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, prawo do wniesienia sprzeciwu wobec takiego przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego. Jednocześnie na podstawie art. 15 ust. 3 RODO ma Pani/Pan prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu.

_____
(podpis Administratora Bezpieczeństwa Informacji)

_____ Nowy Dwór Mazowiecki, dnia _____ r.

(pieczęć Szkoły)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Szkole Podstawowej nr 5 im. J. Kusocińskiego w Nowym Dworze Mazowieckim

1. Data: _____ r. Godzina: _____

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

_____

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

3. Lokalizacja zdarzenia: _____

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

_____
_____
_____

5. Przyczyny wystąpienia zdarzenia:

_____
_____
_____

6. Podjęte działania:

_____
_____
_____

7. Postępowanie wyjaśniające:

_____
_____
_____

_____ _____

(podpis IOD) *(podpis ABI)*