Polityka bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie

SPIS TREŚCI

Podstawa prawna:

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz.926 z późn.zm.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U. z 2004 r. Nr 100, poz.1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

ROZDZIAŁ I
Postanowienia ogólne

§ 1. 1. Polityka bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie, zwana dalej Polityką bezpieczeństwa, określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, zbiorach ewidencyjnych;
2) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, stypendialne, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.

2. Podstawowe pojęcia:

1) *Ustawa* – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz.926 z późn.zm),
2) *Administrator danych osobowych* – rozumie się Dyrektora Szkoły Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie,
3) *Lokalny administrator danych osobowych* – rozumie się pracowników administracyjnych szkoły, wicedyrektorów, pedagoga szkolnego, wychowawców klas, wychowawców świetlicy, nauczycieli, bibliotekarzy;
4) *Administrator sieci* – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;
5) *Nośniki danych osobowych* – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;
6) *Osoba upoważniona (użytkownik)* – osoba posiadająca upoważnienie wydane przez administratora danych osobowych;
7) *Administrator bezpieczeństwa informacji* – osoba powołana zarządzeniem dyrektora, której zadaniem jest nadzorowanie i koordynowanie w szkole zasad postępowania przy przetwarzaniu danych osobowych;
8) *Dane osobowe* – w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
9) *Przetwarzanie danych* – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
10) *Zbiór danych* – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
11) *System informatyczny* – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

12) *Identyfikator użytkownika (login)* - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
13) *Hasło* – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
14) *Uwierzytelnianie* – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
15) *Poufność danych* – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 2. 1. Dyrektor Szkoły Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4) przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.

2. Dyrektor Szkoły Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie dąży do systematycznego unowocześniania stosowanych na terenie szkoły informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

ROZDZIAŁ II
Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych.

§ 3. 1. Dane osobowe gromadzone i przetwarzane są w budynku szkolnym, mieszczącym się Szkole Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie przy ul. Podzamcze 9.

2. Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są:

1) pokój głównej księgowej;
2) sekretariat szkoły - obszar za biurkiem ze wszystkimi urządzeniami oraz szafa pancerna;
3) pokój kadrowej - wydzielona jego część z biurkiem na komputer oraz szafa pancerna;
4) gabinet dyrektora;
5) gabinety wicedyrektorów;
6) gabinet intendenta;
7) sala informatyczna nr 44 /poza zajęciami lekcyjnymi/;
8) biblioteka szkolna – obszar za biurkiem i na zapleczu;
9) gabinet pedagoga – obszar za biurkiem;

10) pokój nauczycielski ;
11) świetlice szkole;
12) sale lekcyjne;
13) archiwum szkolne.

ROZDZIAŁ III
Wykaz zbiorów danych wraz ze wskazaniem programów i opis struktury przetwarzania tych danych w Szkole Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie

§ 4.1. Zbiory danych przetwarzanych w systemach informatycznych:

Zbiór danych osobowych	Program informatyczny służący do przetwarzania zbioru danych	Struktura danych
pracownicy	Kadry Optivum Vulcan	PESEL/ NIP/ imię(imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imiona rodziców/ stan cywilny i rodzinny/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia zatrudnienia/ wysokość wynagrodzenia/ ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia
	Płatnik	PESEL/ NIP/ imiona/ nazwisko/ adres/ data i miejsce urodzenia/ stan rodzinny
	QNT QWARK Płace	PESEL/ NIP/ imię(imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imiona rodziców/ stan cywilny i rodzinny/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo/ dane osoby kontaktowej/ wykształcenie/ staż pracy/ wysokość wynagrodzenia/ warunki zatrudnienia/ tytuł zawodowy/ nieobecności w pracy/ numer konta bankowego
	QNT QWANT Księgowość	PESEL/ NIP/ imię(imiona) i nazwisko/ adres/ numer konta bankowego

	Inwentarz Optivum Vulcan	PESEL/ NIP/ imię(imiona) i nazwisko/adres
	SIO	PESEL/ płeć/ wykształcenie/ staż pracy/ warunki zatrudnienia/ tytuł zawodowy/ uzyskane kwalifikacje/ nieobecności w pracy
	Arkusz organizacyjny Vulcan	PESEL/ imię i nazwisko/ staż pracy/ tytuł zawodowy/ ukończone kursy/ uzyskane kwalifikacje/ warunki zatrudnienia/ nieobecności w pracy
uczniowie	Sekretariat Optivum Vulcan	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ nr telefonu/ e-mail/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ numer legitymacji szkolnej
	Świadectwa	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ informacje o wynikach w nauce
	MOL	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/ klasa

§ 4.2. Zbiory danych przetwarzanych tradycyjnie:

Zbiór danych osobowych	Dokumentacja służąca do przetwarzania zbioru danych	Struktura danych
Pracownicy	Akta osobowe	PESEL/ NIP/ imię(imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imiona rodziców/ stan cywilny i rodzinny/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia zatrudnienia/ wysokość wynagrodzenia/ ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia
	Ewidencja akt osobowych	Imię i nazwisko/ data i miejsce urodzenia/ adres
	Orzeczenia lekarskie dla celów sanitarno-epidemiologicznych	PESEL/ Imię i nazwisko/ adres/ informacja o stanie zdrowia

	Oświadczenia i wnioski do funduszu socjalnego	Imię i nazwisko/ adres/ wysokość dochodów/ stan rodzinny
	List płac	PESEL/ imię i nazwisko/ stanowisko/ wysokość wynagrodzenia
	Karty wynagrodzeń	imię i nazwisko/ stanowisko/ wysokość wynagrodzenia
	Informacje o zarobkach (PIT)	PESEL/ NIP/ imię i nazwisko/ data urodzenia/ adres/ wysokość zarobków
	Zaświadczenia	PESEL/ NIP/ imię i nazwisko/ data urodzenia/ adres/ wysokość zarobków/ warunki pracy
	Dokumentacja ubezpieczeniowa	PESEL/ NIP/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ wysokość zarobków/ stanowisko/ informacja o stanie zdrowia
	Protokoły powypadkowe	imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ stanowisko/ informacja o stanie zdrowia
	Dokumentacja awansów zawodowych nauczycieli	Imię i nazwisko/ data i miejsce urodzenia/ adres/ wykształcenie/ historia pracy/ uzyskane kwalifikacje
Uczniowie	Dokumentacja uczniów	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ nr telefonu/ e-mail/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ numer legitymacji szkolnej/ obywatelstwo/ osoba kontaktowa/ wykształcenie/ historia nauki/ wyznanie/ informacje o stanie zdrowia/ orzeczenia i opinie z poradni psychologiczno-pedagogicznej
	Księga uczniów	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/

	Arkusze ocen	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ wyznanie/ informacja o wynikach nauczania
	Dzienniki lekcyjne, nauczania indywidualnego, zajęć pozalekcyjnych, specjalistycznych, pedagoga, logopedy, wychowawcy świetlicy	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ numery telefonów/ obywatelstwo/ informacja o wynikach nauczania/ nieobecności w szkole
	Księga wydanych legitymacji i legitymacje	Imiona i nazwisko/ data i miejsce urodzenia/ adres/ klasa/ numer legitymacji
	Rejestr zaświadczeń i zaświadczenia	Imiona i nazwisko/ data i miejsce urodzenia/ adres/ klasa
	Księga absolwentów	Imiona i nazwisko/ numer w księdze uczniów/ numer świadectwa/ data ukończenia szkoły
	Świadectwa i duplikaty	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ informacje o wynikach w nauce
	Dokumentacja ubezpieczeniowa	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/
	Protokoły powypadkowe	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/informacje o stanie zdrowia
	Karty zdrowia ucznia	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/imiona rodziców(prawnych opiekunów)/ informacje o stanie zdrowia
	Karty szczepień	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/imiona rodziców(prawnych opiekunów)/ informacje o stanie zdrowia

	Karty biblioteczne	Imiona i nazwisko/ data i miejsce urodzenia/ adres/ klasa

ROZDZIAŁ IV

System przetwarzania danych osobowych

§ 5.1. 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.

2. Sposób przepływu danych pomiędzy poszczególnymi systemami jest następujący:

KADRY → PŁATNIK
Z aplikacji Kadry Optivum Vulcan do programu Prokom Płatnik przykazywane są dane dotyczące zarejestrowania i wyrejestrowania pracowników.
Sposób przekazywania danych: manualny.

PŁACE → PŁATNIK
Z aplikacji QNT QWARK do programu Prokom Płatnik przekazywane są dane dotyczące składek na ubezpieczenie społeczne i zdrowotne.
Sposób przekazywania danych: manualny.

PŁACE → BANK PEKAO S.A.
Z aplikacji QNT QWARK do programu Pekaobiznes24 przekazywane są dane dotyczące należnych kwot przelewanych na konta pracowników.
Sposób przekazywania danych: manualny.

ROZDZIAŁ V

Opis zdarzeń naruszających ochronę danych osobowych

§ 6. Rodzaje zagrożeń naruszających ochronę danych osobowych:

1. Zagrożenia losowe:

1) zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona , jednak nie dochodzi do naruszenia danych osobowych;
2) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

2. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:

1) nieuprawniony dostęp do systemu z zewnątrz;
2) nieuprawniony dostęp do systemu z wewnątrz;

3) nieuprawnione przekazanie danych;
4) bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

3. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

1) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;
2) niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;;
3) awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;
4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu ;
5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;
9) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
10) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowywanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);
11) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).

4. Szczegółowe zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

ROZDZIAŁ VI
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

§ 7. 1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:

1) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;

2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach pancernych lub metalowych;
3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
4) budynek, w którym są przetwarzane dane chroniony jest całodobowo przez dozorców; pomieszczenia z danymi osobowymi wyposażone są w kraty lub drzwi z zamkami atestowanymi.

§ 8. 1. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:

1) podłączenie urządzenia końcowego (komputera, drukarki) do sieci komputerowej Szkoły Podstawowej nr 23 im. Olimpijczyków Polskich w Lublinie dokonywane jest przez administratora sieci;
2) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych;
3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania;
4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi;
5) udostępnianie kluczy do pomieszczeń, w których przetwarzane są dane osobowe tylko osobom upoważnionym;
6) ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe.

§ 9. 1. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

1) odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych UPS;
2) ochrona przed utratą danych poprzez cykliczne wykonywanie kopii zapasowych;
3) zapewnienie właściwej temperatury i wilgotności w pomieszczeniach;
4) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w pomieszczeniach gaśnic.

§ 10. 1. Organizację ochrony danych osobowych realizuje się poprzez:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów;
3) kontrolowanie pomieszczeń budynku;
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
5) wyznaczenie administratora bezpieczeństwa informacji.