Publiczna Szkoła Podstawowa nr 6
im. Marii Skłodowskiej - Curie
ul. Pawła Stalmacha 20
47 - 220 KĘDZIERZYN - KOŹLE
NIP 749-16-34-426 ; Regon 000698271
tel. 77 483 29 52 , 77 486 56 39
psp6@kedzierzynkozle.pl

Zarządzenie Dyrektora nr 02/09/2017-2018

Publicznej Szkoły Podstawowej nr 6 im. Marii Skłodowskiej-Curie w Kędzierzynie-Koźlu

z dnia 1 września 2017 r.

w sprawie wdrożenia dokumentacji ochrony danych osobowych w Publicznej Szkole Podstawowej nr 6 im. Marii Skłodowskiej-Curie w Kędzierzynie-Koźlu

Na podstawie § 3 ust.3 oraz § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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.Nr 100, poz.1024 z 2004r.), zarządza się co następuje:

§1.

Ustala się Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu zwaną dalej „dokumentacją ochrony danych osobowych", która stanowi załącznik nr 1 do niniejszego zarządzenia.

§2.

Zobowiązuje się pracowników Publicznej Szkoły Podstawowej nr 6 w Kędzierzynie-Koźlu do stosowania zasad określonych w dokumentacji ochrony danych osobowych.

§3.

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR SZKOŁY
mgr Małgorzata Nowacka
.....
(pieczątka, data, podpis)

Zał. nr 1 do Zarządzenia Nr 02/09/2017-2018

Dyrektora PSP nr 6 w Kędzierzynie-Koźlu

z dnia 01.09.2017 r.

Dokumentacja
ochrony danych osobowych
Publicznej Szkoły Podstawowej nr 6
im. Marii Skłodowskiej-Curie
w Kędzierzynie-Koźlu

01.09.2017

SPIS TREŚCI

Spis treści

1. WPROWADZENIE

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu z siedzibą przy ul. Pawła Stelmacha 20 oraz ul. 1 Maja 3, 47-200 Kędzierzyn-Koźle zwanej dalej **placówką oświatową.**

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy zbiorach osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym wyrażone w Polityce bezpieczeństwa oraz w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników.

Do najważniejszych należy ewidencja :

- zbiorów danych osobowych,
- miejsc ich przetwarzania
- osób upoważnionych do przetwarzania danych,

a także lista środków organizacyjnych i technicznych służących bezpieczeństwu danych.

2. PODSTAWY PRAWNE

USTAWA ORAZ AKTY WYKONAWCZE

Przepisy ochrony danych osobowych zawarte są w ustawie o ochronie danych osobowych oraz wydanych do niej aktach wykonawczych.

Listę aktów prawnych stanowią:

- 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
- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U z 2016 r. poz.922)
- Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 3 listopada 2006r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2006, Nr 203, poz. 1494) – art. 13.3 ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 94, poz. 923) – art. 22a ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) – art. 39a ustawy
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) – art. 46a ustawy.
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwoływania administratora bezpieczeństwa informacji
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

Niniejszy dokument powstał w oparciu o **art. 36 ust. 2 oraz 39 a ustawy o ochronie danych osobowych**, które zobowiązują Administratora danych do wykonania dokumentacji opisującej środki organizacyjne i techniczne służące ochronie przetwarzanych danych osobowych.

Szczegółowy zakres dokumentu określa Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wydane do art. 39a ustawy.

DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

Generalny Inspektor Ochrony Danych Osobowych – organ do spraw ochrony danych osobowych.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Dane wrażliwe - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Administrator danych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych.

Administrator bezpieczeństwa informacji (ABI) – osoba nadzorująca stosowanie środków technicznych i organizacyjnych przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

Administrator systemu informatycznego (ASI) – osoba lub osoby odpowiedzialna/e za prawidłowe funkcjonowanie systemu informatycznego. ASI jest powoływany przez ADO.

Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzanie danych - 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.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom

Dokumentacja przetwarzania danych – dokumentacja opisująca sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, określoną w przepisach wydanych na podstawie art. 39 a ustawy.

Zagrożenia danych – polega z jednej strony na możliwości ich utraty, zniszczenia lub zafałszowania, z drugiej strony zaś na możliwości ich nieuprawnionego rozpowszechnienia.

Zabezpieczenia – praktyki, procedury i mechanizmy zmniejszające ryzyko, chroniące przed zagrożeniami, ograniczające następstwa , wykrywające niepożądane incydenty i ułatwiające odtworzenie prawidłowego stanu systemu.

Pracownik – osoba mianowane, zatrudniona na umowę o pracę, umowę cywilno-prawną, stażysta lub praktykant świadczący pracę dla Publicznej Szkoły Podstawowej nr 6 w Kędzierzynie-Koźlu.

Instytucja – Publiczna Szkoła Podstawowa nr 6 w Kędzierzynie-Koźlu.

Instrukcja – instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu.

Sprawdzenie – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora Ochrony Danych Osobowy, zwanego dalej „Generalnym Inspektorem".

Sprawozdanie – dokument zawierający elementy określone w art. 36 c ustawy, opracowany przez ABI po dokonaniu sprawdzenia, którego celem jest zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Państwa trzecie – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

3. ANALIZA I CHARAKTERYSTYKA ZAGROŻEŃ BEZPIECZEŃSTWA

W rozdziale scharakteryzowano możliwe do wystąpienia zagrożenia bezpieczeństwa przetwarzania danych osobowych.

3.1. CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

- **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona, lecz nie dochodzi do naruszenia poufności danych.

- **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych,
- **zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

3.2. SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

- **przełamane zabezpieczenia tradycyjnych** – zerwane plomby na drzwiach, szafach, segregatorach,
- **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych** na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
- **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- **jakość danych w systemie** lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- **naruszenie lub próba naruszenia integralności** systemu lub bazy danych w tym systemie,
- **próba lub modyfikacja danych** oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- **niedopuszczalna manipulacja** danymi osobowymi w systemie,
- **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu,
- **praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa** od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
- **ujawnienie istnienia nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki", itp.,

- **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych,
- **rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3.3. LISTA POTENCJALNYCH ZAGROŻEŃ PRZETWARZANIA DANYCH

Poniżej przedstawiono listy potencjalnych zagrożeń bezpieczeństwa danych z podziałem na zagrożenia miejsc przetwarzania oraz rodzajów danych tj. zbiorów przetwarzanych tradycyjnie (papierowo) oraz z wykorzystaniem systemów informatycznych. W każdym przypadku, w sytuacji stwierdzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić Administratora danych i sporządzić raport.

1. Zagrożenia miejsc przetwarzania danych :
   - włamanie od strony okien – wybite szyby, niedomknięte skrzydło,
   - włamanie od strony drzwi – zerwane plomby, uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach,
   - oddziaływanie czynników zewnętrznych – wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana,
   - pozostawienie niezamkniętych drzwi i okien – jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych,
   - pozostawienie bez nadzoru osoby nieuprawnionej do przebywania w pomieszczeniu.
2. Zagrożenia związane z przetwarzaniem danych papierowych :
   - pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy,
   - pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze,
   - pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe,
   - przechowywanie dokumentów w miejscach do tego nieprzeznaczonych,
   - wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie,
   - przetwarzanie danych przez osoby nieupoważnione,
   - nieuzasadnione sporządzanie kserokopii danych.
3. Zagrożenia związane z przetwarzaniem danych elektronicznych :
   - dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłania poprzez Internet danych nieszyfrowanych,
   - dopuszczenie do nieuzasadnionego kopiowania dokumentów i utrata kontroli nad kopiami,
   - sporządzanie kopii danych w sytuacjach nie przewidzianych procedurą,

- utrata kontroli nad kopiami danych osobowych,
- podmiana lub zniszczenie nośników z danymi osobowymi,
- pozostawienie zapisanego hasła dostępu do baz danych,
- samodzielne instalowanie jakiegokolwiek oprogramowania,
- obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania,
- opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do baz danych osobowych,
- odczytywanie dyskietek i innych nośników przed sprawdzeniem ich oprogramowaniem antywirusowym,
- niezabezpieczenie komputera zasilaczem awaryjnym podtrzymującym napięcie na wypadek braku zasilania,
- dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych,
- ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym,
- ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej,
- dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe,
- pojawienie się komunikatów,
- awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich,
- nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości baz danych,
- niezapowiedziane zmiany w wyglądzie lub zachowaniu się aplikacji służącej do przetwarzania danych,
- próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej,
- dopuszczenie, aby osoby inne niż ABI lub osoby przez ABI uprawnione, podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji,
- ślady manipulacji przy układach sieci komputerowej lub komputerach,
- obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu,
- naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

3.4. OBOWIĄZKI PRACOWNIKA

W przypadku naruszenia bądź zagrożenia naruszenia ochrony danych pracownicy są obowiązani do niezwłocznego powiadomienia ABI, sporządzenia raportu na formularzu nr 9 i przekazania go ABI oraz podjęcia następujących czynności mających na celu wyeliminowanie zagrożeń lub naruszeń w przypadku :

- ujawnienia sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom nieuprawnionym, ujawnienia informacji o sprzęcie i pozostałej infrastrukturze informatycznej bądź też w przypadku dopuszczania i stwarzania warunków , aby ktokolwiek taką wiedzę mógł

pozyskać np. Z obserwacji lub dokumentacji – należy natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji, sporządzić raport z opisem, jaka informacja została ujawniona,

- dopuszczenia do korzystania z aplikacji umożliwiającej dostęp do bazy danych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony – należy wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze, pouczyć osobę , która dopuściła do takiej sytuacji o naruszeniu procedur,
- pozostawienia w niezabezpieczonym miejscu, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych lub sieci – należy natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie oraz niezwłocznie zmienić hasło,
- dopuszczenia do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do danych osobom nieuprawnionym – należy wezwać osobę nieuprawnioną do opuszczenia stanowiska, ustalić jakie czynności zostały przez osoby nieuprawnione wykonane, przerwać działające programy .
- samodzielnego zainstalowania jakiegokolwiek oprogramowania – należy pouczyć osobę wykonywującą czynność, aby jej zaniechała oraz wezwać ASI w celu odinstalowania programów.
- zmodyfikowania parametrów systemu i aplikacji – należy wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała oraz podjąć działania powodujące przywrócenie zmodyfikowanych parametrów do stanu pierwotnego.
- pozostawienia dokumentów w otwartych pomieszczeniach bez nadzoru – należy zabezpieczyć dokumenty i pomieszczenie.
- przechowywania dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych – należy powiadomić przełożonych oraz interweniować w sprawie poprawy zabezpieczeń.
- wyrzucenia dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie – należy zabezpieczyć niewłaściwie zniszczone dokumenty oraz powiadomić przełożonych.
- dopuszczenia do kopiowania dokumentów i utraty kontroli nad kopią – należy zaprzestać kopiowania, odzyskać i zabezpieczyć wykonaną kopię
- dopuszczenia , aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane – należy wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności oraz wyłączyć monitor.
- sporządzenia kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą – należy spowodować zaprzestania kopiowania, odzyskać i zabezpieczyć kopię,
- dopuszczenia i pozostawienia bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych – należy zabezpieczyć pomieszczenie.
- podłączenia przez osoby nieuprawnione jakiekolwiek urządzeń do sieci komputerowej bądź demontowanie przez te osoby elementów obudów gniazd i torów kablowych lub dokonywanie

jakichkolwiek manipulacji – należy wezwać osoby dokonujące zakazanych czynności do ich zaprzestania oraz postarać się ustalić ich tożsamość.

- dopuszczenia lub ignorowania faktu, że osoby nieuprawnione dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej – należy wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ewentualnego opuszczenia pomieszczenia, postarać się ustalić ich tożsamość.
- dostrzeżenia śladów manipulacji przy układach sieci komputerowej lub komputerach należy zaprzestać używania sprzętu oraz oprogramowania do czasu wyjaśnienia sytuacji oraz zabezpieczenia ewentualnych śladów.
- dostrzeżenia obecności nowych kabli o nieznanym przeznaczeniu i pochodzeniu, niezapowiedzianych zmian w wyglądzie lub zachowaniu się aplikacji służącej do przetwarzania danych, nieoczekiwanych , nie dających się wyjaśnić zmian zawartości bazy danych bądź też w przypadku obecności nowych programów w komputerze lub innych zmian w konfiguracji oprogramowania - nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
- dostrzeżenia śladów włamania do pomieszczeń, szaf lub biurek, w których przetwarzane są dane – należy o tym fakcie powiadomić przełożonego.
- próby uzyskania hasła uprawniającego do dostępu do danych lub nieuzasadnionego przeglądania (modyfikowania) danych za pomocą aplikacji w bazie danych – należy dokonać takich modyfikację , dostęp do danych oraz o tym fakcie powiadomić przełożonego.

4. POLITYKA BEZPIECZEŃSTWA

Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

4.1. DEKLARACJA

Administrator danych mając świadomość, iż przetwarza dane **zwykłe** pracowników oraz dane **zwykłe i wrażliwe** uczniów, którym Publiczna Szkoła Podstawowa nr 6 w Kędzierzynie-Koźlu świadczy usługi z zakresu nauki, wychowania i opieki deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Zasady te określa w szczególności Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Dokumenty te są uzupełniane załącznikami do dokumentacji, na które składają się m.in.: wykazy zbiorów, miejsc ich przetwarzania oraz osób upoważnionych do przetwarzania danych.

W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się liczne ewidencje, które szczegółowo charakteryzują obszary objęte monitoringiem, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.

Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.

W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

4.2. CHARAKTERYSTYKA INSTYTUCJI

Publiczna Szkoła Podstawowa nr 6 w Kędzierzynie-Koźlu realizuje zadania głównie na mocy przepisów prawa zawartych w ustawie o systemie oświaty, systemie informacji oświatowej oraz Karcie Nauczyciela, a także innych aktach wykonawczych uprawniających Dyrektora szkoły do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania są zadania związane z bezpłatną opieką, wychowaniem oraz nauczaniem

4.3. WYKAZ ZBIORÓW OSOBOWYCH

Na podstawie § 4 pkt 2 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 tworzy się **wykaz zbiorów osobowych** wraz ze wskazaniem programów komputerowych służących do ich przetwarzania zgodnie z formularzem nr 1 do niniejszej dokumentacji.

Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się, zgodnie z § 6 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. środki bezpieczeństwa na poziomie **WYSOKIM**.

4.4. OPIS STRUKTURY ZBIORÓW OSOBOWYCH

Na podstawie § 4 pkt 3 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 wprowadza się do formularza nr 1 opis struktury poszczególnych zbiorów osobowych.

4.5. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

Na podstawie § 4 pkt 4 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 wprowadza się opis zasad przepływu danych do formularza nr 1 .

4.6. WYKAZ MIEJSC PRZETWARZANIA

Na podstawie § 4 pkt 1 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 tworzy się **wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych.**

Wyznaczają go pomieszczenia zlokalizowane w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu. Szczegółowy wykaz pomieszczeń, opisuje się na formularzu nr 2 do niniejszej dokumentacji.

4.7. EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 39 ust. 1 ustawy o ochronie danych osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, którą sporządza się na formularzu nr 3 do niniejszej dokumentacji.

Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.

Ewidencja stanowi podstawę wydania upoważnienia do przetwarzania danych osobowych na mocy art. 37 ustawy o ochronie danych osobowych.

4.8. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

- przetwarzanie danych osobowych w **szkole** może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie**. Wzór upoważnienia stanowi formularz nr 4 do niniejszej dokumentacji.
- ADO prowadzi **ewidencję osób upoważnionych** oraz na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych.**
- unieważnienie upoważnienia następuje na piśmie, wg wzoru - formularz nr 5 do niniejszej dokumentacji.
- zabrania się przetwarzania danych poza obszarem określonym w formularzu nr 2 do niniejszej instrukcji, za wyj. przypadków dopuszczonych przez Administratora danych.
- każdy pracownik **szkoły** co najmniej raz na rok musi odbyć **szkolenie z zakresu ochrony danych** osobowych. Za organizację szkoleń odpowiedzialny jest ABI, który prowadzi w tym

celu odpowiednią dokumentację. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.

- ponadto każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi formularz nr 6 do niniejszej dokumentacji. Podpisany dokument jest dołączany do przedmiotowej dokumentacji
- obszar przetwarzania danych osobowych określony w formularzu nr 2 do niniejszej dokumentacji, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych poprzez zamknięcie pomieszczenia na klucz.
- przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
  Wzory zgody na przebywanie w pomieszczeniach dla osób nie posiadających upoważnienia, a także odwołania tej zgody, stanowią odpowiednio formularz nr 7 oraz formularz nr 8 do przedmiotowej dokumentacji.
- pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- przetwarzanie danych podawanych dobrowolnie może odbywać się tylko na podstawie pisemnej zgody podającego te dane wg wzoru określonego w formularzu nr 10.
- dokumenty zawierające dane osobowe należ niszczyć w specjalistycznych niszczarkach.
- każdorazowe zbieranie danych z art. 24 oraz 25 ustawy o ochronie danych osobowych rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
- dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszar przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Zabiory osobowe przetwarzane elektronicznie należy zabezpieczyć poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- komputery, które przetwarzają zbiory osobowe wyszczególnione w formularzu nr 1 do dokumentacji, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.

- pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczyć stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym będącej częścią niniejszego dokumentu
- w celu zapewnienia danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego (np. WIDOWS) oraz bezpośrednio do programów przetwarzających dane.
- Szczegółowe zasady postępowanie ze zbiorami przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym będąca częścią niniejszej dokumentacji
- ABI do 31 stycznia każdego roku budżetowego sporządza na formularzu nr 11 Harmonogram sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych. Harmonogram sprawdzeń jest zatwierdzany przez ADO.
- W oparciu o harmonogram sprawdzeń ABI dokonuje sprawdzeń stanu zabezpieczenia danych osobowych prowadzonych zarówno w zbiorach tradycyjnych jak i w zbiorach elektronicznych. Fakt przeprowadzenia sprawdzenia ABI dokumentuje na formularzu nr 12 – Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
- ABI do 31 grudnia każdego roku budżetowego sporządza na formularzu nr 13 – Sprawozdanie roczne ze stanu zabezpieczenia danych osobowych. Sprawozdanie roczne ze stanu zabezpieczenia danych osobowych zatwierdzane jest przez ADO.

4.9. ŚRODKI TECHNICZNE OCHRONY DANYCH OSOBOWYCH

Zbiory danych przetwarzane w szkole zabezpiecza się poprzez:

1. **Środki ochrony fizycznej.**
   - Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi, przeszklonymi.
   - Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna nie są zabezpieczone za pomocą krat.
   - Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętej nie metalowej szafie.
   - Zbiory danych osobowych (akta osobowe) w formie papierowej przechowywane są w zamkniętej metalowej szafie.
   - Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie.
   - Pomieszczenia, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru wolno stojącymi gaśnicami.
   - Dokumenty zawierające dane osobowe po ustaniu przydatności są przechowywane na okres archiwizacji w zakładowej Składnicy Akt , a po ustaniu okresu archiwizacji są niszczone poprzez spalenie. Natomiast dokumenty zawierające dane osobowe, które nie podlegają archiwizacji, po ich wykorzystaniu są niszczone w niszczarce.

2. **Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej.**

- Zbiory danych osobowych przetwarzane są przy użyciu komputerów stacjonarnych i na laptopach.
- Komputery i laptopy służące do przetwarzania danych osobowych nie są połączone z lokalną siecią komputerową.
- Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
- Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
- Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
- Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
- Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
- Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3. **Środki ochrony w ramach systemowych narzędzi programowych i baz danych.**

- Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych.
- Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych.
- Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
- Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
- Zastosowano kryptograficzne środki ochrony danych osobowych.
- Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
- Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych opisana w pkt 6 niniejszej dokumentacji.

4. Procedura bezpieczeństwa sprzętu poza siedzibą szkoły .

- Użytkownik komputera przenośnego poza siedzibą **szkoły** ma obowiązek jego ochrony.
- Zabrania się pozostawiania komputerów przenośnych bez opieki w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nim skutecznego nadzoru.
- Osoba używająca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania, przestrzegając jednocześnie zaleceń producentów dotyczących ochrony sprzętu
- Korzystanie z komputera przenośnego w miejscach publicznych i innych nie chronionych miejscach poza siedzibą **szkoły** wymaga ostrożności, by nie ujawnić danych osobom nieupoważnionym.
- Użytkowanie komputera przenośnego/dysku zewnętrznego/pendrive poza siedzibą **szkoły** dopuszczanie jest tylko za zgodą ADO. Wzór zgody na użytkowanie komputera przenośnego/dysku zewnętrznego/pendrive poza siedzibą **szkoły** stanowi formularz nr 14.
- Użytkownik komputera przenośnego/dysku zewnętrznego/pendrive jest zobowiązany złożyć oświadczenie, którego wzór stanowi formularz nr 15,
- W przypadku utraty komputera przenośnego użytkownik niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia faktu popełnienia przestępstwa na Policji. W zawiadomieniu użytkownik, poza danymi ogólnymi, podaje okoliczności utraty komputera oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia. W szczególności w zawiadomieniu należy określić, czy utracone dane miały charakter danych osobowych.

5. Szkolenie pracowników.

- ADO, ABI lub podmiot zewnętrzny, przeprowadza okresowe szkolenia pracowników w zakresie przepisów prawa oraz uregulowań wewnętrznych. Szkolenia okresowe odbywają się nie rzadziej niż raz w roku.
- Pracownicy nowozatrudnieni przed przystąpieniem do pracy podlegają szkoleniu przez ABI z zakresu ochrony danych osobowych.
- Ze szkoleń grupowych sporządza się listę obecności pracowników biorących udział, którą przechowuje ABI.
- Każda osoba zatrudniona przy przetwarzaniu danych powinna być zaznajomiona z przepisami dotyczącymi ochrony danych, co powinno być potwierdzone złożeniem oświadczenia w formie pisemnej na formularzu nr 16.

6. Zasady aktualizacji Polityki bezpieczeństwa.

- Aktualizację Polityki bezpieczeństwa przeprowadza się na wniosek ABI lub ASI.

- Przyczynami prowadzącymi do aktualizacji Polityki bezpieczeństwa są następujące czynniki :
  - zgłoszenie ASI lub ABI przez pracownika ważnego problemu lub trudności w przestrzeganiu zasad zwartych w aktualnie obowiązującej Polityce bezpieczeństwa,
  - wykrycie przez ASI lub ABI nieprawidłowości w obowiązującej Polityce bezpieczeństwa,
  - wystąpienie zmian w obowiązujących przepisach związanych z Polityką bezpieczeństwa,
  - wejście w życie nowych przepisów, które mogą mieć wpływ na treść Polityki bezpieczeństwa,
  - likwidacja, utworzenie lub zmiany zawartości informacyjnej zbioru danych.

7. Następstwa grożące za nieprzestrzeganie Polityki bezpieczeństwa

- Pracownicy zobowiązani są do zapoznania i bezwzględnego stosowania wszystkich obowiązujących w instytucji przepisów i zarządzeń wewnętrznych dotyczących ochrony danych.
- Za nieprzestrzeganie zasad Polityki bezpieczeństwa pracownik ponosi odpowiedzialność na zasadach określonych w Kodeksie Pracy, Kodeksie Karnym oraz ustawie o ochronie danych osobowych.
- Nieprzestrzeganie Polityki bezpieczeństwa stanowi ciężkie naruszenie obowiązków pracowniczych.

4.10. POSTĘPOWANIE Z KLUCZAMI

1. Klucze główne i alarm :

a. ADO wyznacza osoby, które są upoważnione do otwierania i zamykania głównych drzwi wejściowych oraz do rozkodowywania i kodowania systemu alarmowego przed rozpoczęciem i po zakończeniu pracy,

b. osoby upoważnione, którym zostały powierzone klucze do głównych drzwi są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody ADO oraz nie udostępniania osobom trzecim.

2. Klucze dostępowe do pomieszczeń zlokalizowanych w szkole :

a. Klucze do poszczególnych pomieszczeń znajdują się w szafie zlokalizowanej w pomieszczeniu sekretariatu.

b. Osoby, które zostały upoważnione do dostępu do szafy z kluczami zlokalizowanej w pomieszczeniu sekretariatu są zobowiązane do zabezpieczenia kluczy i wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania ich bez zgody ADO oraz nie udostępniania osobom trzecim.

3. Klucze do biurek stanowiskowych i szaf :

a. Do kluczy od biurek stanowiskowych, szaf biurowych, dostęp mają upoważnione przez ADO osoby, które zobowiązane są do ich zabezpieczenia w indywidualny, właściwy do każdej sytuacji sposób, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych,

b. Osoby, które zostały upoważnione do kluczy od biurek stanowiskowych, szaf biurowych, są zobowiązane do wykorzystywania ich zgodnie z przeznaczeniem oraz nie kopiowania bez zgody ADO oraz nie udostępniania osobom trzecim.

5. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Na podstawie § 3.1 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 opracowano Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

5.1. CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczna, w której przetwarzane są dane osobowe stanowią wszystkie pracujące obecnie i przyszłe planowane serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.

2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.

3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym, na każdym stanowisku.

5.2. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. ABI lub ASI odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.

2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ASI do eksploatacji licencjonowane oprogramowanie.

3. ASI prowadzi ewidencję oprogramowania.

4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,

b. mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej,

c. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,

d. urządzenia niwelujące zakłócenia i podtrzymujące zasilanie,

e. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie,

f. mechanizmy zarządzania zmianami.

5. Użytkownikom zabrania się:

a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody ADO,

b. udostępniania stanowisk roboczych osobom nieuprawnionym,

c. wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez ADO,

d. samowolnego instalowania i używania programów komputerowych,

e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,

f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym,

g. używania komputera bez zainstalowanego oprogramowania antywirusowego.

5.3. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI.

1. Użytkowników systemu informatycznego tworzy oraz usuwa ASI na podstawie zgody ABI.

2. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.

3. Wprowadza się rejestr osób upoważnionych do przetwarzania danych osobowych, który stanowi formularz nr 3 do niniejszej dokumentacji.

4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:

a. nieobecności pracownika w pracy trwającej dłużej niż 30 dni kalendarzowych,

b. zawieszenia w pełnieniu obowiązków służbowych.

5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.

6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

5.4. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

2. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasło do systemu operacyjnego (WINDOWS) oraz osobne do baz danych osobowych i aplikacji.

3. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator, którego nazwa składa się z pierwszej litery imienia oraz nazwiska, pisane małymi literami, bez znaków polskich. W przypadku ASI identyfikator to ADMINISTRATOR.

4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika ABI, nadaje inny identyfikator odstępując od ogólnej zasady.

5. W identyfikatorze pomija się polskie znaki diakrytyczne.

6. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.

7. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały itp.) i nie może być sekwencją kolejnych znaków klawiatury.

8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu ASI i do natychmiastowej zmiany hasła.

9. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.

10. Hasła najwyższego poziomu, którymi dysponuje ASI gromadzone są w zamkniętej kopercie przez ABI.

11. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.

12. Hasło nie może być zapisywane i przechowywane.

13. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

5.5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.

3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.

5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.

6. Czas rozpoczęcia i kończenia pracy w systemach sieciowych, w tym w systemach przetwarzania danych osobowych, określa Regulamin Pracy.

7. Konieczność pracy w aplikacjach sieciowych w godzinach innych , niż określone w Regulaminie Pracy, powinno być zgłoszone ABI.

8. ASI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.

5.6. PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA.

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.

2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych nośnikach informacji – dysk zewnętrzny USB.

3. Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.

4. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfigurujących system odpowiedzialna jest ASI. Kopie przechowywane są przez ASI.

5. Kopie zapasowe mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.

6. Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii zapasowych.

7. Nośniki, na których są przechowywane kopie danych osobowych powinny być wyraźnie oznaczone.

8. Za bezpieczeństwo kopii awaryjnych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.

9. ASI zobowiązany jest do okresowego wykonywania testów odtworzenia kopii zapasowych.

10. Zewnętrzne nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.

11. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.

12. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

5.7 SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ASI w odpowiednio zabezpieczonym pomieszczeniu.

2. Dane osobowe mogą być przetwarzane na serwerach, a także na dyskach lokalnych komputerów w lokalizacji ustalonej z ABI. Zabrania się gromadzenia danych osobowych na innych, nie autoryzowanych przez ABI nośnikach danych.

3. W uzasadnionych przypadkach, za zgodą ABI, dane osobowe można przetwarzać na zewnętrznych nośnikach informacji, autoryzowanych przez ASI.

4. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.

5. Komputery przenośne oraz inne mobilne nośnik danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

6. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a. **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b. **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

c. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ABI.

6. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez ABI.

5.8. SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. ASI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.

2. System antywirusowy jest skonfigurowany w następujący sposób:

a. skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera,

b. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco.

c. automatycznej aktualizacji wzorców wirusów.

3. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.

4. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.

5. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

5.9. INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA

1. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym powinny być automatycznie odnotowane następujące dane :

a. dane o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba, że dane te traktuje się jako dane jawne,

b. sprzeciwu osoby, której dane dotyczą w przypadku zamierzenia przetwarzania jej danych w celach marketingowych lub zamierzenia przekazania jej danych innemu administratorowi.

2. Zapis pkt. 1 nie dotyczy systemów służących do przetwarzania danych ograniczonych do edycji teksu w celu udostępnienia go na piśmie i niezwłocznym usunięciu z systemu.

3. Dla każdej osoby, której dane są przetwarzane w systemie informatycznym, system powinien zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnym rozumieniu formę informacji, o którym mowa w pkt. 1.

4. W uzasadnionych przypadkach uniemożliwiających automatyczne odnotowywanie, o którym mowa w pkt. 1, prowadzi się odrębny „rejestr udostępnień", w oparciu o własne rozwiązanie organizacyjne

5. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.

5.10. PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

2. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną należy każdy z załączników zabezpieczyć ochroną kryptologiczną poprzez nadanie hasła odczytu. Hasło należy przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (telefon, fax , w bezpośredniej rozmowie).

3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

4. Zabrania się przekazywania danych przez aplikacje internetowe nie wykorzystujące odpowiedniego protokołu szyfrowania (adres internetowy musi być poprzedzony zapisem „https".

5.11. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO lub posiadające umowy na powierzenie przetwarzania danych osobowych w zakresie konserwacji i napraw.

2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ABI.

3. W przypadku uszkodzenia zestawu komputerowego, laptopa lub nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.

4. W przypadku konieczności przeprowadzenia prac serwisowych poza biblioteką dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.

5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.

6. ABI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

FORMULARZE

Formularz nr 1. Wykaz zbiorów danych osobowych.

Formularz nr 2. Wykaz miejsc przetwarzania zbiorów danych osobowych.

Formularz nr 3. Wykaz osób upoważnionych do przetwarzania danych osobowych.

Formularz nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

Formularz nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.

Formularz nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

Formularz nr 7. Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych.

Formularz nr 8. Wzór odwołania zgody na przebywanie w obszarze przetwarzania danych osobowych.

Formularz nr 9. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych.

Formularz nr 10. Wzór zgody na przetwarzanie danych.

Formularz nr 11. Harmonogram sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych w instytucji

Formularz nr 12- Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Formularz nr 13- Sprawozdanie roczne ze sprawdzenia stanu ochrony danych osobowych w instytucji.

Formularz nr 14 – Zgoda na użytkowanie komputera przenośnego/dysku zewnętrznego/pendrive poza siedzibą instytucji.

Formularz nr 15 - Oświadczenie użytkownika sprzętu komputerowego/dysku zewnętrznego/pendrive

Formularz nr 16 - Oświadczenie o zaznajomieniu się z przepisami dotyczącymi ochrony danych osobowych

Formularz nr 17 - Notatka z udostępnienia danych osobowych przez instytucję

Formularz nr 1

WYKAZ ZBIORÓW OSOBOWYCH

Administrator danych , adres jego siedziby, numer REGON	
Administrator bezpieczeństwa informacji, adres jego siedziby	

Lp.	Nazwa zbioru i cel przetwarzania danych w zbiorze	Podstawa prawna przetwarzania	Zakres danych przetwarzanych w zbiorze	Kategoria osób, których dane są przetwarzane	Podmiot, któremu powierzono przetwarzanie danych
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10					

WYKAZ MIEJSC PRZETWARZNIA DANYCH OSOBOWYCH

Lp.	Nazwa pomieszczenia	Adres
1		
2		
3		
4		
5		
6		
7		
8		
9		

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia	Imię i nazwisko	Nr zbiorów	Okres upoważnienia		Program/identyfikator	Nr unieważnienia
			OD	DO		

Kędzierzyn-Koźle, dn. .....

PSP-UP/..../20.....

(sygnatura)

WAŻNOŚĆ
od: .....
do: ***odwołania***

UPOWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2016, poz. 922) upoważniam Panią :

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

Nr zbiorów z ewidencji zbiorów	Nazwa programu / identyfikator

.....
(podpis Administratora danych)

Formularz nr 5

Kędzierzyn-Koźle, dn. .....

PSP-UU/...../20.....

(sygnatura)

UNIEWAŻNIENIE

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2016, poz. 922) unieważniam upoważnienie do przetwarzania danych osobowych wydane dnia ..... o sygnaturze PSP-UP/..../20..... dla Pani/Pana:

.....

(podpis Administratora danych)

Formularz nr 6

Kędzierzyn-Koźle, dn. .....

.....

(imię i nazwisko pracownika)

PSP-OŚ/...../20.....

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść:

   a) Dokumentacji ochrony danych osobowych obowiązującej w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu,
   b) Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz.U. 2016, poz. 922),
   c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

2. Jednocześnie zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/zapoznałam się z racji wykonywanej pracy, a w szczególności nie będę:

a) ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
b) ujawniać szczegółów technologicznych używanych w systemów 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.

.....

(podpis pracownika)

.....

(podpis administratora danych)

Kędzierzyn-Koźle, dn. .....

PSP-ZG/...../20.....

(sygnatura)

WAŻNOŚĆ
od: .....
do: *odwołania*

ZGODA

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do 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 z późn. zm.), **wyrażam zgodę Pani/Panu:**

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych.

.....
(podpis Administratora danych)

Kędzierzyn-Koźle, dn. .....

PSP-OZ/..../20....

(sygnatura)

ODWOŁANIE ZGODY

NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH

Na podstawie pkt I.2 załącznika do 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 z późn. zm.), **odwołuję zgodę** z dnia ..... o sygnaturze PSP-ZG/...../20..... udzieloną **Pani/Panu:**

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe.

.....

(podpis Administratora danych)

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w .....

1. Data: .... Godzina: .....
(dd.mm.rr) (gg:mm)

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:
.....
.....
.....

.....
(data, podpis Administrator danych)

....., dn. .....

.....
(imię i nazwisko, adres zamieszkania)

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na podstawie art. 23 ust.1 pkt 1 (oraz/lub art. 27.2 pkt 1 – dla danych wrażliwych) ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz.U. 2016, poz. 922), wyrażam zgodę na przetwarzanie niżej wymienionych moich danych osobowych.

Zgoda udzielona jest tylko do przetwarzania danych oraz ich udostępniania w podanym niżej zakresie.

Lp.	Zakres danych – zgoda	Cel przetwarzania	Odbiorcy lub kategorie odbiorców danych
1			
2			
3			

Jednocześnie zgodnie z art. 24 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. 2016, poz. 922) przyjmuję do wiadomości, że:

- Administratorem danych jest Publiczna Szkoła Podstawowa nr 6 im. Marii Skłodowskiej-Curie w Kędzierzynie-Koźlu z siedzibą przy ul. Pawła Stelmacha 20 oraz ul. 1 Maja 3, 47-200 Kędzierzyn-Koźle,
- dane będą przetwarzane wyłączenie zgodnie z określonym celem,
- dane będą udostępniane wyłącznie podanym odbiorcom,
- przysługuje mi prawo dostępu do treści danych oraz ich poprawiania,
- dane podaję dobrowolnie.

.....

(podpis)

Formularz nr 11

Harmonogram
sprawdzeń z zakresu przestrzegania zasad ochrony danych osobowych
w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu na rok.....

Zatwierdzam :

.....
(Administrator danych)

L.p.	Przedmiot sprawdzenia	Zakres poszczególnych sprawdzeń	Data rozpoczęcia	Data zakończenia	Komórka organizacyjna/ stanowisko

.....
(data, podpis Administratora bezpieczeństwa informacji)

Sprawozdanie

ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych obowiązujących w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu

1. Oznaczenie administratora danych osobowych i adres jego siedziby :.....
.....
2. Imię i nazwisko administratora bezpieczeństwa informacji : .....
3. Wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska osób biorących udział w tych czynnościach :.....
.....
.....
.....
.....
.....
.....
4. Data rozpoczęcia i zakończenia sprawdzenia : .....
5. Określenie przedmiotu i zakresu sprawdzenia :
.....
.....
.....
.....
6. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych :
.....
.....
.....
.....
7. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem :
.....
.....
.....
.....
8. Wyszczególnienie załączników stanowiących składową część sprawozdania :
.....
.....
.....
.....

.....
(data, podpis Administratora bezpieczeństwa informacji)

Sprawozdanie roczne
ze sprawdzenia stanu ochrony danych osobowych
w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu za rok.....

Zatwierdzam :

.....
(Administrator danych)

1. Oznaczenie administratora danych osobowych i adres jego siedziby :.....
.....
2. Imię i nazwisko administratora bezpieczeństwa informacji : .....
3. Imię i nazwisko administratora sieci informatycznej :.....
4. Wykaz czynności objętych sprawozdaniem.

L.p.	Czynności	Stan faktyczny	Do uzupełnienia
1	Analiza dokumentacji		
2	Analiza upoważnień do przetwarzania danych osobowych		
3	Analiza odbytych szkoleń		
4	Analiza spełnienia obowiązku rejestracji zbiorów w GIODO		
5	Analiza przypadków naruszeń przepisów		
6	Analiza umów powierzenia danych		
7	Analiza działań podjętych dla bezpieczeństwa przetwarzania danych		
8	Analiza zabezpieczeń systemu informatycznego (antywirus, firewall)		

5. Plan czynności do realizacji w celu zapewnienia bezpieczeństwa danych i spełnienia wymogów ustawowych.

L.p.	Czynności do wykonania	Data zakończenia czynności	Osoba odpowiedzialna

.....
(data, podpis Administrator bezpieczeństwa informacji)

Zgoda na użytkowanie komputera przenośnego/pendrive/dysku zewnętrznego poza siedzibą szkoły

Wyrażam zgodę na użytkowanie komputera przenośnego/pendrive/dysku zewnętrznego poza siedzibą szkoły.

Nazwisko i imię pracownika: .....

Numer ewidencyjny komputera przenośnego/pendrive/dysku zewnętrznego : .....

Czas użytkowania od ..... do ...../czas nieokreślony/czas pełnienia funkcji*

Zakres danych osobowych udostępnionych .....

.....

(Administrator Danych Osobowych)

Formularz nr 15

OŚWIADCZENIE UŻYTKOWNIKA

SPRZĘTU KOMPUTEROWEGO/PENDRIVE/DYSKU ZEWNĘTRZNEO

.....

(imię i nazwisko)

Oświadczam, że przekazany sprzęt

o numerze ewidencyjnym: .....

i numerze seryjnym .....

będzie wykorzystany wyłącznie do celów służbowych. Na wyżej wymienionym komputerze/dysku zewnętrznym/pendrive nie będę samodzielnie instalował(a) żądnego oprogramowania.

Jednocześnie oświadczam, że zostałem poinformowany(a), Administrator danych nie ponosi odpowiedzialności za nieprawidłowe funkcjonowanie komputera/dysku zewnętrznego/pendrive spowodowane samodzielnym zainstalowaniem oprogramowania na wyżej wymienionym komputerze/dysku zewnętrznym /pendrive oraz o konsekwencjach prawnych i służbowych grożących w przypadku samodzielnej instalacji oprogramowania.

Przyjmuję do wiadomości, iż dane zgromadzone na powierzonym mi komputerze/dysku zewnętrznym/pendrive oraz dostępne w wewnętrznej sieci Publicznej Szkoły Podstawowej nr 6 im. Marii Skłodowskiej-Curie w Kędzierzynie-Koźlu objęte są tajemnicą służbową i w związku z powyższym zobowiązuję się do przestrzegania odpowiednich procedur mających na celu ochronę danych osobowych, jak i tych stanowiących tajemnicę służbową przed nieuprawnionym udostępnieniem zgodnie z Polityką bezpieczeństwa.

.....

data, podpis użytkownika sprzętu

Formularz nr 16

OŚWIADCZENIE

o zaznajomieniu się z przepisami dotyczącymi ochrony danych osobowych

Ja, niżej podpisany(a)

....

(imię i nazwisko) (instytucja)

.....

(stanowisko)

oświadczam, że:

1. zapoznałam /em* się z treścią Zarządzenia Dyrektora PSP nr 6 w Kędzierzynie-Koźlu w sprawie wprowadzenia Polityki bezpieczeństwa i instrukcji przetwarzania danych w PSP nr 6 w Kędzierzynie-Koźlu,
2. zostałam/em/* przeszkolona/ny/* w zakresie przepisów prawa oraz uregulowań wewnętrznych w zakresie bezpieczeństwa danych osobowych,
3. zobowiązuję się do bezwzględnego zachowania w tajemnicy wszelkich informacji uzyskanych w związku z wykonywanym zakresem czynności na stanowisku pracy oraz przyjmuję do wiadomości, że dane osobowe przetwarzane w PSP nr 6 w Kędzierzynie-Koźlu objęte są ochroną - zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922)
4. zobowiązuję się do zachowania tajemnicy danych osobowych po ustaniu zatrudnienia w PSP nr 6 w Kędzierzynie-Koźlu,
5. zobowiązuję się do bezwzględnego zachowania w tajemnicy informacji związanych ze sposobem zabezpieczenia danych osobowych,
6. zobowiązuję się do bezwzględnego przestrzegania praw autorskich – zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.).

Kędzierzyn-Koźle, dnia ..... rok .....

.....

(podpis pracownika)

* Niepotrzebne skreślić

NOTATKA Z UDOSTEPNIENIA DANYCH OSOBOWYCH PRZEZ INSTYTUCJI

Data: .....

Osoba udostępniająca:

Imię i nazwisko: .....
Stanowisko służbowe: .....
Dział: .....

Dane osoby, której udostępniono dane:

Imię i nazwisko: .....
Stanowisko służbowe: .....
Nazwa firmy / instytucji: .....
Adres firmy / instytucji: .....
Nazwa zbioru danych: .....
Zakres udostępnionych danych:
.....
.....
.....
.....
.....
.....

Przyjmuję do wiadomości:

....
(data, podpis Administratora Bezpieczeństwa Informacji) (data, podpis osoby udostępniającej dane osobowej)