Polityka Ochrony Danych Osobowych
w Szkole Podstawowej w Chomentowie, Chomentów 72
28-305 Sobków .

1. WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

Przetwarzanie danych osobowych - to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2. OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator / podmiot przetwarzający nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

2.1. OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.

2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:

a. nazwę zbioru (opis kategorii osób)

b. opis celów przetwarzania

c. charakter, zakres, kontekst danych osobowych

d. odbiorcy danych

e. funkcjonalny opis operacji przetwarzania

f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing),

g. informacja o konieczności wpisu do rejestru czynności przetwarzania

h. informacja o konieczności przeprowadzenia oceny skutków dla zbioru

2.2. OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków Administrator zobowiązany jest do spełnienia wobec danych osobowych obowiązków prawnych. W szczególności należy zapewnić, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9)

2. dane te są adekwatne w stosunku do celów przetwarzania

3. dane te są przetwarzane przez określony czas (retencja danych)

4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody)

5. opracowano klauzule informacyjne,

6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28)

2.3. ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania.

2.3.1. DEFINICJE

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych

2. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

3. Zagrożenie - potencjalne naruszenie (potencjalny incydent)

4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)

5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów

2.3.2. WYZNACZANIE ZAGROŻEŃ

1. Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania

2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów

2.3.3. WYLICZANIE RYZYKA DLA ZAGROŻEŃ

1. Administrator określa prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania

2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A

3. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne

4. Proponowaną Skalę skutków prezentuje Tabela B

5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S

Tabela A

Prawdopodobieństwo wystąpienia zagrożenia	**Skala**
Niskie	**1**
Średnie	**2**
Wysokie	**3**

Tabela B

SKUTKI WYSTĄPIENIA ZAGROŻENIA	**Skala**
małe (do 10000 PLN, incydent prasowy lokalny)	**1**
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	**2**
duże (od 100000 PLN, naruszenie prawa)	**3**

2.3.4. PORÓWNANIE WYLICZONYCH RYZYK ZE SKALĄ I OKREŚLENIE DALSZEGO POSTĘPOWANIA Z RYZYKIEM

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem

2. Proponowaną skalę Ryzyka prezentuje Tabela C

Poziom ryzyka	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	**1-2**
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	**3-6**
ryzyko jest nieakceptowalne (musimy obniżyć)	**9**

2.3.5. REAKCJA NA WARTOŚĆ RYZYKA

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń

2. Działania obniżające ryzyko, które może zastosować Administrator:

a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)

b. Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji)

c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie nośników z danymi wynoszonych poza firmę).

2.4. PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne .

2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń .

3. UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych

2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa

3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.

4. Upoważnienia nadawane są w formie udokumentowanego zakresu obowiązków.

5. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia

6. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO.

4. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia w formie pisemnej o stwierdzeniu podatności lub wystąpieniu incydentu Administratora oraz Inspektora Ochrony Danych Osobowych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów

b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych

c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)

b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych)

c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator prowadzi postępowanie wyjaśniające w toku, którego:

a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki

b. inicjuje ewentualne działania dyscyplinarne

c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu

d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

5. REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

5.1. GOSPODARKA KLUCZAMI

Pracownicy administracji klucze do pomieszczeń służbowych pobierają ze skrzynki na klucze.

Po zakończeniu pracy klucze są oddawane .

Do otwierania pomieszczeń dla potrzeb wykonywania czynności związanych ze sprzątaniem wykorzystywane są klucze od poszczególnych pomieszczeń, przekazane upoważnionym pracownikom obsługi .

Prowadzony jest rejestr pobieranych kluczy.

ZASADY PRZECHOWYWANIA KLUCZY

Klucze od pomieszczeń szkolnych przechowuje się w wydzielonej gablocie .

Klucze zapasowe deponowane są w sejfie.

Pracownicy nie mogą używać dorabianych osobiście kluczy do pomieszczeń biurowych, szkolnych.

ZASADY DYSPONOWANIA KLUCZAMI

Osoby uprawnione do posiadania kluczy do pomieszczeń służbowych nie mogą ich udostępniać osobom innym i są zobowiązane do osobistego ich zwrotu po zakończonej pracy.

Osoby, które zagubiły klucz ponoszą odpowiedzialność materialną.

EWIDENCJA PRZYJMOWANIA I WYDAWANIA KLUCZY ZAPASOWYCH

Wydawanie, przyjmowanie kluczy zapasowych jest odnotowywane przez osobę mającą do nich dostęp .

Nie oddanie klucza powoduje po zakończeniu pracy wszczęciem poszukiwań.

Osoby, które zagubiły klucz zapasowy ponoszą odpowiedzialność materialną w zakresie zakupu i montażu zamka.

Wydawanie kluczy zapasowych uprawnionym pracownikom może odbywać się tylko w uzasadnionych przypadkach za zgodą Administratora

ODPOWIEDZIALNOŚĆ

Od momentu pobrania kluczy do momentu ich zdania, na upoważnionej osobie spoczywa pełna odpowiedzialność za mienie znajdujące się w danym pomieszczeniu.

Zabrania się wynoszenia kluczy od pomieszczeń poza szkołę.

Utrzymanie skutecznego zabezpieczenia wszystkich pomieszczeń podlega nadzorowi Administratora.

Przed wyjściem z pomieszczenia, pracownicy zobowiązani są do:

-uporządkowania swoich stanowisk pracy,

-wykonania czynności zabezpieczających, polegających na:

1) wyłączeniu i zabezpieczeniu urządzeń elektronicznych (projektorów, komputerów, drukarek, ekranów itp.),

2) pochowaniu używanych pomocy i akcesoriów (wskaźniki, piloty, kable itp.) w przystosowanych do tego celu biurkach i szafkach oraz ich zamknięcie na klucz,

3) zamknięciu okien i drzwi (nie dotyczy przerw śródlekcyjnych, podczas których otwieramy okna w celu wywietrzenia pracowni).

4) zamknięciu szaf meblowych i zabezpieczenie kluczy do szaf w sposób uniemożliwiający dostęp osób nieupoważnionych do zasobu szafy

Pracownik wchodzący do danego pomieszczenia, w przypadku stwierdzenia powyższych uchybień informuje o tym Administratora

Za zniszczenia i uchybienia wymienione odpowiada osoba, która wcześniej dysponowała kluczami.

Za nieprzestrzeganie niniejszej instrukcji mogą być wyciągnięte sankcje wynikające z art. 363 § 1 kodeksu cywilnego.

5.2.POLITYKA CZYSTEGO BIURKA

1. Polityka czystego biurka obowiązuje wszystkich pracowników zatrudnionych w Szkole Podstawowej w Chomentowie i jest częścią Polityki Ochrony Danych Osobowych obowiązującej od 25.05.2018 r.

2. Za pracowników uważa się każdą osobę zatrudnioną na podstawie stosunku pracy, a także zleceniobiorców, stażystów, praktykantów, osoby współpracujące oraz samozatrudnione na rzecz administratora danych.

3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. Należy unikać przechowywania dokumentów niepotrzebnych do bieżących zadań.

4. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.

5. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć np. w niszczarce.

6. Ekrany monitorów komputerów powinny być ustawione tak by uniemożliwiały widok osobom postronnym.

7. Na biurku nie powinny znajdować się napoje w otwartych pojemnikach grożących rozlaniem.

8. Po zakończeniu pracy na biurku powinny pozostać tylko przybory biurowe.

9. Niniejsza Polityka obowiązuje od dnia 25.05.2018 r.

6. SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO

2. Za przeprowadzenie szkolenia odpowiada Administrator

3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia szkolenia.

6.1. ZGODNIE Z POLITYKĄ BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH WYMAGA SIĘ TEGO, ABY :

1) Dostęp do danych osobowych miały osoby posiadające upoważnienie do przetwarzania danych.

2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych.

3) Dane były chronione przed dostępem do nich osób nieupoważnionych.

4) Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz.

5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.

6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych.

7) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy.

8) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

9) Szafy, w których przechowywane są dane, powinny być zamykane na klucz.

10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.

11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.

12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie muszą być chowane do szaf.

13) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy.

14) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.

15) W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.

16) Nie należy udostępniać osobom nieupoważnionym tych komputerów.

17) W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności.

18) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.

19) Jeśli nie ma możliwości skasowania danych z nośnika (np. płyta CD-ROM), należy go zniszczyć fizycznie.

20) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.

21) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

22) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

23) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

7. REJESTR OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Na terenie Szkoły Podstawowej w Chomentowie 72, 28-305 Sobków upoważnia się do przetwarzania danych osobowych wszystkie osoby, które zapoznały się z klauzulą informacyjną, Polityka Ochrony Danych Osobowych oraz zostały wpisane do rejestru zatwierdzonego przez Administratora dołączonego do niniejszego dokumentu.

8. AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu Administrator stosuje procedurę audytów.

9. PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.