Polityka Ochrony Danych Osobowych w Domu Kultury
w Zakrzewie

I. Wstęp.

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Domu Kultury w Zakrzewie, zwanym dalej „ośrodkiem", 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.

Dane osobowe wymagające ochrony Administrator danych podzielił na zbiory danych i umieścił w „Rejestrze czynności przetwarzania danych osobowych", który stanowi odrębny dokument prowadzony w formie elektronicznej.

II. Definicje.

1. Zgodnie z art. 4 RODO:

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

2) **„przetwarzanie"** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3) **„ograniczenie przetwarzania"** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4) **„profilowanie"** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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;

5) **„pseudonimizacja”** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) **„zbiór danych”** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) **„administrator”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

8) **„podmiot przetwarzający”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

9) **„odbiorca”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

10) **„strona trzecia”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

11) **„zgoda”** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

12) **„naruszenie ochrony danych osobowych”** oznacza 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;

13) **„dane genetyczne”** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne

informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

14) **„dane biometryczne”** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

15) **„dane dotyczące zdrowia”** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

16) **„organ nadzorczy”** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO.

2. Poza tym w „Polityce ochrony Danych Osobowych” stosuje się definicje:

1) **„aktywa”** – należy przez to rozumieć środki materialne i niematerialne mające wpływ na przetwarzanie danych;

2) **„ryzyko” –** należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;

3) **„zarządzanie ryzykiem”** – należy przez to rozumieć realizowany przez administratora danych osobowych proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki;

4) **„ocena ryzyka”** – należy przez to rozumieć czynność polegającą na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie projektowania systemu bezpieczeństwa danych;

5) **„bezpieczeństwo informacji”** – należy przez to rozumieć zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

6) **„dostępność”** — należy przez to rozumieć właściwość określającą, że zasób systemu jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie;

7) **„integralność”** — należy przez to rozumieć właściwość określającą, że zasób systemu nie został zmodyfikowany w sposób nieuprawniony;

8) **„poufność”** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

9) **„zagrożenie”** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia naruszenia, mogącego mieć wpływ na ich ujawnienie bądź utratę;

10) **„anonimizacja”** - należy przez to rozumieć nieodwracalne przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie.

III. Zapewnienie o przetwarzaniu danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:

1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO,

2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych,

3) Administrator przechowuje dane osobowe przez konkretnie określony czas,

4) wobec osób, których dane są przetwarzane dopełniono obowiązku informacyjnego (art. 12, 13, 14 RODO) wraz ze wskazaniem im prawa: dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym”,

5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano im dane kontaktowe,

6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umówprzetwarzania danych osobowych z podmiotami przetwarzającymi (art. 28 RODO).

2. Potwierdzenie przetwarzania danych osobowych zgodnie z prawem znajduje sięw „Rejestrze czynności przetwarzania danych osobowych”.

IV. Upoważnienia.

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

2. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.

3. Upoważnienia określają zakres operacji na danych.

4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych.

5. Administrator prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych.

V. Polityka zarządzania ryzykiem.

1. Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych obejmuje:

1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem,
2) zasady i tryb identyfikacji ryzyka,
3) zasady i tryb dokonywania analizy ryzyka,
4) zasady określania właściwej reakcji na ryzyko.

2. Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich samodzielnych stanowisk wskazanych w Regulaminie Organizacyjnym ośrodka.

3. Zarządzanie ryzykiem jest procesem ciągłym.

4. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:

1) rozpoznanie – czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością ośrodka w zakresie ochrony danych osobowych i dokonywanie ich pomiaru,

2) ocenę ryzyka i jego istotności,

3) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań,

4) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

5. Zakresy zadań i obowiązków.

5.1. Za realizację polityki zarządzania ryzykiem odpowiada Administrator danych poprzez:

1) kształtowanie i wdrażanie polityki zarządzania ryzykiem,
2) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem,
3) wyznaczanie poziomu akceptowalnego dla każdego ryzyka,
4) podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

5.2. Pracownicy na samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:

1) identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych,
2) przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z IOD,
3) proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk,
4) wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.

5.3. Pracownicy na samodzielnych stanowiskach są zobowiązani do współpracy z Administratorem danych i IOD.

6. Analiza ryzyka

6.1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

6.2. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

6.3. Przyjęto, że analiza ryzyka przeprowadzana jest dlapojedynczego aktywa lub grupy aktywów charakteryzujących się podobieństwem celów i sposobów przetwarzania.

7. Proces analizy ryzyka.

7.1. Identyfikacja ryzyk

7.1.1. Identyfikacja ryzyk prowadzona jest dla wszystkich zbiorów danych na poziomie jednostki i na poziomie poszczególnych samodzielnych stanowisk pracy.

7.1.2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia. Ze względu na ich źródło ryzyka dzielą się na:

1) zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne,
2) wewnętrzne – ryzyko to obejmuje działania wewnętrzne ośrodka i może być zarządzane wewnątrz jednostki.

7.1.3. Każdy pracownik ma prawo i obowiązek zgłaszania Administratorowi danych lub IOD ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań w zakresie ochrony danych osobowych.

7.2. Inwentaryzacja aktywów

Inwentaryzacji aktywów dokonuje się w zakresie następujących grup aktywów:

a) sprzęt,
b) personel,
c) siedziba,
d) oprogramowanie,
e) dokumenty w formie papierowej,
f) formaty plików w postaci elektronicznej,
g) sieć,
h) organizacja,
i) inne – w zależności od wprowadzanych zmian technicznych i organizacyjnych.

7.3. Identyfikacja zagrożeń

Inwentaryzacji zagrożeń dokonuje się w zakresie następujących grup zagrożeń:

a) zniszczenia fizyczne,

b) zniszczenia naturalne,
c) utrata podstawowych usług,
d) naruszenia bezpieczeństwa informacji,
e) awarie techniczne,
f) nieautoryzowane działania,
g) naruszenia bezpieczeństwa funkcji,
h) zagrożenia osobowe.

7.4. Identyfikacja podatności

Podatność- jest to słabość, która może być wykorzystana przez zagrożenie, powodując

Niekorzystne skutki, np. luka w systemie informatycznym. Słabość aktywa lub zabezpieczenia, która może być wykorzystana do urzeczywistnienia się zagrożenia.

Przykłady podatności:

- Brak staranności przy pozbywaniu się nośników,
- wrażliwość na zmiany temperatury,
- brak kopii zapasowych,
- wrażliwość na zmiany napięcia,
- nieobecność personelu,
- brak regularnych audytów,
- złe zarządzanie hasłami,
- brak fizycznej ochrony budynków, drzwi i okien.

7.5. Szacowanie poziomu ryzyka.

Szacowanie poziomu ryzyka składa się z następujących etapów:

1. Ocena prawdopodobieństwa wystąpienia zagrożenia (OP) w skali 1- 5 dla następujących zagrożeń:
   a) zniszczenia fizyczne i naturalne,
   b) utrata podstawowych usług i awarie techniczne,
   c) naruszenia bezpieczeństwa informacji,
   d) nieautoryzowane działania i naruszenia bezpieczeństwa funkcji, w tym zagrożenia osobowe zewnętrzne.
2. Ocena oddziaływania na finanse ośrodka (OF) w skali 1 – 3.
3. Ocena oddziaływania na reputację ośrodka (OR) w skali 1 – 5.
4. Ocena poziomu ryzyka (PR) wg wzoru **PR=(OP/4)*(OF+OR)**
   Uzyskany wynik porównuje się z tabelą korelacji prawdopodobieństwa wystąpienia ryzyka i oddziaływania na finanse i reputację ośrodka oraz interpretuje się go wg tabeli opisującej wymagane działania w zależności od poziomu ryzyka (poziom ryzyka: niski, średni, wysoki, krytyczny, z czego tylko poziom niski jest poziomem akceptowalnym).
5. Ocena zastosowanych zabezpieczeń technicznych i fizycznych (Z.TECH.) oraz organizacyjnych i personalnych (Z.ORG.) w czterostopniowej skali:
   - poziom wysoki: wartość 6
   - poziom średni: wartość 4,5
   - poziom niski: wartość 3
   - brak zabezpieczeń: wartość 1,5

Oceny poziomu ryzyka ze względu na zastosowane zabezpieczenia fizyczne i techniczne oraz organizacyjne i personalne dokonuje się wg wzoru: **zabezpieczenia=Z.TECH.*Z.ORG**. , a wynik porównuje się z tabelą korelacji zabezpieczeń technicznych i organizacyjnych.

6. Porównanie wyników oceny poziomu ryzyka ze względu na zagrożenia (ppkt 4) z oceną poziomu ryzyka ze względu na zastosowane zabezpieczenia (ppkt 5).

   Wynik porównania wskazujący, że zastosowane zabezpieczenia są adekwatne do istniejącego ryzyka wynikającego z zagrożeń powoduje akceptację danego stanu. W przeciwnym razie należy podjąć odpowiednie działania, zgodnie z pkt 8 („Postępowanie z ryzykiem").

7.6. Wszystkie wzory narzędzi i tabel ujętych w pkt 7 stanowią odrębny dokument, który jest częścią całej dokumentacji stanowiącej analizę ryzyka dla wszystkich aktywów, które tego wymagają. Dokumentacja ta przechowywana jest w ośrodku.

7.7. Pracownicy ośrodka zobowiązani są do systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich Administratorowi danych lub IOD.

8. Postępowanie z ryzykiem.

8.1. Dla każdego istotnego, zidentyfikowanego ryzyka wskazuje się optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1) akceptacja ryzyka – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści; zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne,

2) dzielenie (przeniesienie ryzyka) – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz,

3) unikanie ryzyka – dotyczyć to będzie grypy ryzyk dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu,

4) modyfikowanie (redukcja ryzyka) – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji, lub znacznego ograniczenia.

9. Ocena skutków dla ochrony danych.

Zgodnie z art. 35 RODO:

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych

osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z IOD.

3. Ocena oceny skutków dla ochrony danych zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w pkt 1; oraz

e) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

4. Pkt 9.podpkt 1 - 3 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) RODO ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega Administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

VI. Instrukcja postępowania z naruszeniami.

Celem instrukcji jest minimalizacja skutków wystąpienia naruszeń bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania naruszeń w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu naruszeniaAdministratora lub Inspektora Ochrony Danych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych naruszeń bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
3) 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 naruszenia, Administrator lub IOD prowadzi postępowanie wyjaśniające, w toku którego:

1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
2) proponuje ewentualne działania dyscyplinarne,
3) proponuje sposób postępowania na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
4) rekomenduje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje wszelkie incydenty i naruszenia ochrony danych osobowych, w tym ich okoliczności, skutki oraz podjęte działania zaradcze; prowadzi „Rejestr naruszeń ochrony danych Osobowych" stanowiący odrębny dokument.

6. Zabrania się osobom upoważnionym do przetwarzania danych osobowych podejmowania działań mogących prowadzić do naruszeń ochrony danych osobowych.

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, tj. UODO (Urząd Ochrony Danych Osobowych).

VII. Regulamin Ochrony Danych Osobowych.

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania - załącznik nr1 – „Regulamin Ochrony Danych Osobowych".

Po zapoznaniu się z „Regulaminem Ochrony Danych Osobowych" pracownicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich poprzez złożenie pisemnego oświadczenia w ośrodku.

VIII. Procedura przywracania dostępności danych osobowych.

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, co stanowi element „Regulaminu Ochrony danych osobowych".

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

IX. 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 danych oraz IOD .

3. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

X. Postanowienia końcowe.

1. „Polityka ochrony danych osobowych" obowiązuje od 25 maja 2018 roku.
2. Traci moc dotychczasowa „Polityka Bezpieczeństwa" dotycząca ochrony danych osobowych w ośrodku.

Zakrzewo, 2018-05-25.

……
(Administrator Danych osobowych)