**Polityka bezpieczeństwa danych osobowych**

**Domu Kultury „Krzemień” w Szczecinie**

**1. Źródła prawa**

Dom Kultury „Krzemień” w Szczecinie zapewnia bezpieczeństwo przetwarzanych danych osobowych na podstawie:

* Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 4 maja 2016 r. L nr 119 poz. 1 ze zm.) – dalej: RODO;
* Ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 tekst jedn. ze zm.) ‒ dalej: ustawa o ochronie danych osobowych;
* Ustawy z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. z 19 kwietnia 2019 r. poz. 730),
* wytycznych Europejskiej Rady Ochrony Danych,
* wskazówek Prezesa Urzędu Ochrony Danych Osobowych,
* niniejszej *Polityki bezpieczeństwa danych osobowych* (zwanej dalej: instrukcją).

**2. Cel dokumentu**

1. Niniejsza instrukcja jest dokumentem mającym na celu przede wszystkim określenie środków, procedur i zasad zapewniających ochronę przed zagrożeniem i potencjalnym zagrożeniem danych osobowych przetwarzanych przez instytucję kultury: Dom Kultury „Krzemień” w Szczecinie – zwana dalej: instytucją lub administratorem.
2. Do kategorii osób, których dane osobowe instytucja przetwarza, należą:

* pracownicy instytucji
* osoby realizujące umowy o pracę oraz umowy cywilno-prawne
* uczestnicy zajęć
* uczestnicy imprez
* uczestnicy warsztatów
* uczestnicy szkoleń
* uczestnicy konkursów
* sponsorzy
* kontrahenci
* stażyści
* praktykanci
* wolontariusze
* osoby otrzymujące newsletter,
* klienci i pracownicy kawiarni (monitoring)
* użytkownicy serwisu www

3. Instrukcję przechowuje się w wersji elektronicznej oraz w wersji papierowej w siedzibie instytucji jako administratora danych. Instrukcję udostępnia się do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych,celem zapoznania się z jej treścią.

**3. Definicje**

1. **Administrator Danych Osobowych** (ADO)   
   Administratorem danych osobowych jest Dom Kultury „Krzemień” w Szczecinie, z siedzibą przy ul.Krzemiennej 10, 70-742 Szczecin; [www.krzemien.art](http://www.krzemien.art)
2. **Inspektor Ochrony Danych (IOD)** – instytucja powołała inspektora ochrony danych (IOD)

**4. Przetwarzanie danych osobowych**

**4.1. Czynności przetwarzania**

1. Instytucja jako administrator gromadzi przetwarzane dane osobowe w zbiorach danych i nie podejmuje takich czynności przetwarzania, które wiązałyby się z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka naruszenia zasad ochrony danych osobowych.

2. Obszar przetwarzania danych osobowych obejmuje budynek i pomieszczenia instytucji oraz teren zielony wokół budynku zlokalizowanego przy ul.Krzemiennej 10 , a także wszystkie komputery i inne nośniki danych, które zawierają dane osobowe przetwarzane przez instytucję.

3. Dane osobowe przetwarzane będą w celu czynności związanych z wykonywaniem zadań publicznych i komercyjnych o charakterze kulturalnym, edukacyjnym, sportowym i rozrywkowym.

**4.2. Zgody, upoważnienia i przygotowanie merytoryczne osób przetwarzających dane**

1. Instytucja przetwarza dane osobowe za zgodą osób, których dane dotyczą.

2. W przypadkach określonych w art. 18 RODO osoba, której dane dotyczą, ma prawo ograniczenia przetwarzania danych osobowych.

3. Każda osoba przetwarzająca dane osobowe powinna być pisemnie upoważniona do przetwarzania zgodnie z upoważnieniem do przetwarzania danych osobowych

4. Każda osoba przed dopuszczeniem do czynności polegających na przetwarzaniu danych osobowych będzie przeszkolona w zakresie przepisów RODO. Za przeprowadzenie szkolenia odpowiada inspektor ochrony danych. Po zakończeniu szkolenia jego uczestnicy potwierdzają pisemnie znajomość tych zasad i deklarują ich stosowanie.

5. Inspektor ochrony danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

**4.3. Zasady przetwarzania danych**

1. Wszystkie osoby mają obowiązek przetwarzać dane osobowe zgodnie z obowiązującymi przepisami prawa określającymi zasady ochrony danych osobowych, zgodnie z innymi przepisami oraz zgodnie z niniejszą instrukcją.

2. Instytucja jako administrator danych osobowych przetwarza je z poszanowaniem zasad określonych we właściwych przepisach, tj.:

* przetwarza je zgodnie z zasadami określonymi w art. 6 i 9 RODO;
* zabezpiecza dane osobowe przed naruszeniami;
* przetwarza dane zgodnie z zasadami rzetelności i przejrzystości, przetwarzania w konkretnych i prawnie uzasadnionych celach, a także przetwarzania tylko w zakresie niezbędnym dla osiągnięcia celu przetwarzania danych;
* przechowuje dane przez okres niezbędny i uzasadniony potrzebami ich przetwarzania, a także sprawdza ich prawidłowość oraz dokonuje ich aktualizacji;
* usuwa lub poddaje anonimizacji dane osobowe po upływie okresu przetwarzania.

**4.4. Naruszenie zasad prawidłowego przetwarzania danych osobowych**

1. Naruszenie zasad przetwarzania i ochrony danych osobowych, a także próba ich naruszenia to m.in.:

* przekroczenie zakresu upoważnienia, a także przetwarzanie danych niezgodnie z celem ich przetwarzania oraz niezgodnie z obowiązującymi zasadami określonymi właściwymi przepisami;
* niezachowanie tajemnicy związanej z zasadami przetwarzania danych osobowych, a także niedopełnienie (umyślnie lub nieumyślnie) obowiązku zapewnienia ochrony danych;
* udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym (nieuzasadnione i nieuprawnione kopiowanie i udostępnianie danych, a także uszkodzenie, utrata, zmiana itp.);
* naruszenie innych niż wymienione wyżej praw osób, których dane są przetwarzane.

2. W razie wymienionych wyżej okoliczności osoba upoważniona do przetwarzania danych osobowych ma obowiązek podjąć czynności niezbędne do ograniczenia skutków naruszenia i powiadomić administratora niezwłocznie, w najkrótszym możliwym czasie. Zakres tych czynności należy dopasować do konkretnej sytuacji.

3. Inspektor ochrony danych prowadzi rejestr naruszeń ochrony danych osobowych

**4.5. Inspektor ochrony danych**

1. W instytucji został powołany Inspektor Ochrony Danych

Kontakt z Inspektorem Ochrony Danych:

* Mariusz Andryszak
* mandryszak@spnt.pl
* 797 599 363

2. Instytucja zapewnia, że inspektor ochrony danych jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w instytucji, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Inspektor ochrony danych nie będzie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie będzie on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega Administratorowi.

**5. Środki techniczne i organizacyjne niezbędne dla prawidłowego przetwarzania danych**

**5.1. Zakres środków**

1. Instytucja zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, dostępności, rozliczalności i ciągłości przetwarzanych danych osobowych.

2. Instytucja stosuje środki ochrony, które są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych elementów procesu przetwarzania danych osobowych.

3. Środki techniczne i organizacyjne w tym zakresie obejmują w szczególności:

* ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, a także do sprzętu (komputery, nośniki danych) jedynie do osób odpowiednio upoważnionych (osoby nieposiadające upoważnienia mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej, co dotyczy również korzystania ze sprzętu wykorzystywanego do przetwarzania danych osobowych);
* stosowanie odpowiednich sprzętów i urządzeń (szafy, szafki, biurka, niszczarki itp.) do zabezpieczania danych osobowych;
* ochronę danych przechowywanych w komputerach i innych nośnikach danych m.in. poprzez tworzenie kopii zapasowych, stosowanie programów antywirusowych, stosowanie szyfrów i haseł itd.

**5.2. Audyt środków**

Administrator zapewnia regularne testowanie, pomiar i ocenę skuteczności stosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych , nie rzadziej jednak aniżeli raz na rok.

**6. Prawa osób**

Instytucja zapewnia, poprzez odpowiednie i adekwatne do potrzeb nakłady oraz obsługę, przestrzeganie praw osób, których dane dotyczą, i innych osób w szczególności poprzez:

* żądania od Administratora dostępu do danych osobowych,
* żądania od Administratora sprostowania danych osobowych,
* żądania usunięcia danych przetwarzanych bezpodstawnie,
* żądania ograniczenia przetwarzania danych,
* wniesienia sprzeciwu wobec przetwarzania danych osobowych,
* wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w razie uznania, że przetwarzanie Państwa danych osobowych narusza przepisy o ochronie danych.

**7. Bezpieczeństwo danych osobowych**

**7.1. Wdrożenie odpowiednich środków**

1. Instytucja wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób trzecich. Wdrożenie to odbywa się z uwzględnieniem zasady adekwatności w zakresie stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

2. Instytucja zapewnia w powyższym zakresie:

* zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
* zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
* regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

**7.2. Analiza ryzyka**

Instytucja dokonuje analizy ryzyka naruszenia praw lub wolności osób trzecich poprzez analizę możliwości wystąpienia naruszeń z uwzględnieniem każdego rodzaju prawdopodobieństwa wystąpienia zagrożeń.

**7.3. Reagowanie na incydenty**

W razie stwierdzenia naruszeń osoba, która stwierdziła takie zdarzenie, ma obowiązek:

1. Niezwłocznie poinformować o stwierdzonych zdarzeniach inspektora ochrony danych (IOD);
2. Do czasu pojawienia się na miejscu inspektora ochrony danych pozostawić miejsce w stanie nienaruszonym.
3. Inspektor ma obowiązek poinformować administratora o naruszeniu i wraz z nim przeciwdziałać naruszeniu.

**7.4. Zgłaszanie naruszeń**

1. W przypadku naruszenia ochrony danych osobowych, instytucja bez zbędnej zwłoki – w miarę możliwości, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

**8. Zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych**

W oparciu o wymogi bezpieczeństwa informacji określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Instytucja posiada: *Instrukcję zarządzania systemami informatycznym służącym do przetwarzania danych,* stanowiącej załącznik do niniejszej Polityki bezpieczeństwa danych osobowych

**9**. **Monitoring Wizyjny**

W celu zapewnienia bezpieczeństwa osób, mienia oraz danych i informacji budynek Domu Kultury „Krzemień” oraz jego bezpośrednie otoczenie objęte są monitoringiem wizyjnym. Administratorem danych systemu monitoringu jest Dom Kultury „Krzemień”.

**10. Eksportowanie danych**

Instytucja zapewnia, że przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy – z zastrzeżeniem innych przepisów RODO – instytucja spełni warunki określone w rozdziale V RODO, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Dzieje się to zawsze za zgoda osoby, której dane dotyczą.

**11. Postanowienia końcowe**

Niniejsza polityka oraz pozostała dokumentacja bezpieczeństwa funkcjonująca w Domu Kultury „Krzemień” w Szczecinie została zaakceptowana przez Dyrektora Domu Kultury oraz będzie komunikowana wszystkim pracownikom, którzy zostaną zobligowani do ich stosowania.

Nad przestrzeganiem Polityki czuwa Dyrektor Domu Kultury „Krzemień” oraz Inspektor Ochrony Danych.

Zastosowanie formy komunikacji: publikacja Polityki na stronie internetowej, spotkania, szkolenia, audyt wewnętrzny.