Ośrodek Kultury w Wieliszewie
Gminne Centrum Kultury
Łajski, ul. Stanisława Moniuszki 2
05-119 Legionowo
NIP: 536-17-86-510

Zarządzenie Nr 42/2021
Dyrektora Ośrodka Kultury w Wieliszewie
z dnia 16.06.2021

w sprawie: wprowadzenia procedur z zakresu ochrony danych osobowych

Na podstawie art. 17 ustawy z dnia 17 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (t.j. Dz.U. z 2020 r. poz. 194), w związku z ROZPORZĄDZENIEM 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), zarządzam, co następuje:

§1

Celem zapewnienia funkcjonowania adekwatnej, skutecznej i efektywnej kontroli zarządczej, w zakresie przetwarzania ochrony danych osobowych, wprowadza się do stosowania w Ośrodku Kultury w Wieliszewie następujące procedury:

- incydenty i naruszenia bezpieczeństwa informacji;
- weryfikacji tożsamości na odległość;
- niszczenia zebranych danych osobowych;

§2

Polecam wszystkim pracownikom zatrudnionym w Ośrodku Kultury w Wieliszewie, zatrudnionym na podstawie umowy o pracę, zapoznanie się z w/w procedurami.

§3

Wykonanie zarządzenia powierzam pracownikowi merytorycznemu, Specjaliście ds. kultury.

§4

Zarządzenie wchodzi z dniem podpisania.

DYREKTOR
Ośrodka Kultury w Wieliszewie
dr Dariusz Skrzydlewski

Ośrodek Kultury w Wieliszewie
Gminne Centrum Kultury
Łajski, ul. Stanisława Moniuszki 2
05-119 Legionowo
NIP: 536-17-86-510

Załącznik Nr 1 do Zarządzenia Nr 42/2021
Dyrektora Ośrodka Kultury w Wieliszewie
z dnia 16.06.2021 r.

Procedura: Incydenty i naruszenia bezpieczeństwa informacji

Celem dokumentu jest opisanie procedury reagowania na zaistniałe incydenty naruszenia bezpieczeństwa przetwarzania danych osobowych **w Ośrodku Kultury w Wieliszewie.**

§1. Zakres stosowania

Procedurę należy stosować do wszystkich incydentów z naruszeniem bezpieczeństwa oraz incydentów dotyczących systemów teleinformatycznych.

§2. Naruszenie bezpieczeństwa informacji

Przez **naruszenie bezpieczeństwa informacji** należy rozumieć wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących polityk bezpieczeństwa, nawet, jeśli nie prowadzą do wyżej wymienionych skutków. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata (np. kradzież lub zniszczenie) lub nieuzasadniona modyfikacja danych lub części danych (nawet, jeśli możliwe jest całkowite odtworzenie utraconych danych) a także możliwość dostępu do danych dla osób nieupoważnionych.

§3. Incydent naruszenia bezpieczeństwa

Przez **incydent związany z bezpieczeństwem informacji** należy rozumieć pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia pracy jednostki i zagrażają bezpieczeństwu informacji. Na możliwość wystąpienia naruszenia bezpieczeństwa informacji mogą wskazywać:

a) nietypowy stan pomieszczeń przetwarzania (naruszone plomby, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia, które zostały wcześniej wyłączone przez użytkownika);
b) zaginięcie sprzętu lub nośników informacji (nośników danych, dokumentów papierowych, itp.);
c) nieuzasadnione modyfikacje lub usunięcie danych, niezgodności w wcześniej prowadzonych danych;
d) wszelkie działania niezgodne z dokumentami opisującymi bezpieczeństwo oraz celowe próby ingerencji w sprzęt i oprogramowanie bez zgody odpowiednich pracowników.

§4. Rejestr incydentów i naruszeń

Rejestr incydentów i naruszeń – należy przez to rozumieć wykaz incydentów i naruszeń bezpieczeństwa informacji **w Ośrodku Kultury w Wieliszewie.**

§5. Kategorie incydentów i zdarzeń:

Podział incydentów i zdarzeń:

1. Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu, zalaniu itp.), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2. Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki użytkowników, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3. Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), wyszczególnić możemy:
   - nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do danych z sieci wewnętrznej,
   - nieuprawniony transfer danych,
   - pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
   - bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2. Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym np. pozostawienie serwisantów bez nadzoru.
4. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.

6. Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7. Stwierdzono próbę modyfikacji danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8. Nastąpiła niedopuszczalna manipulacja danymi w systemie.
9. Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10. Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11. Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.
12. Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
13. Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
14. Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

§6. Reagowanie na incydent

1. Użytkownik powiadamia ustnie, telefonicznie lub za pomocą poczty elektronicznej swojego przełożonego. Przełożony przekazuje informację o incydencie IOD oraz ASI.
2. ASI niezwłocznie rejestruje incydent w dzienniku incydentów i zdarzeń, wzór stanowi załącznik do niniejszej procedury,
3. Każde naruszenie bezpieczeństwa ASI odnotowuje w dzienniku incydentów, o czym informuje IOD.
4. Jeśli incydent jest ewidentnym naruszeniem bezpieczeństwa i winny jest znany, konsekwencje wobec pracownika, który naruszył bezpieczeństwo wyciąga bezpośredni przełożony. Konsekwencje muszą być zgodne z Regulaminem Pracy i Kodeksem Pracy,
5. W uzasadnionych przypadkach po analizie IOD zgłasza incydent Urzędowi Ochrony Danych Osobowych,
6. Ostatnim etapem zamykania naruszenia bezpieczeństwa jest usunięcie skutków naruszenia bezpieczeństwa poprzez wprowadzenie dodatkowych zabezpieczeń,
7. W szczególnych przypadkach IOD może poinformować organy ścigania o zaistniałej sytuacji.

§7. Reakcja na incydenty związane z naruszeniem bezpieczeństwa danych osobowych

1. Jeżeli zostaje stwierdzone naruszenie ochrony danych osobowych realizowane są działania zgodnie z **PBI**.
2. O naruszeniu bezzwłocznie należy informować Inspektora Ochrony Danych i Administratora Danych Osobowych.
3. Inspektor Ochrony Danych podejmuje działania zgodnie z przepisami prawa w szczególności ustawy o ochronie danych osobowych i aktami wykonawczymi, a od 25 maja 2018 r. 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, zwane RODO).
4. Każdy incydent związany z naruszeniem bezpieczeństwa danych osobowych musi być zarejestrowany w dzienniku incydentów i zdarzeń.
5. Naruszenie bezpieczeństwa w dzienniku incydentów i zdarzeń powinno być wyraźnie wyszczególnione.

§8. Zmiana klasyfikacji incydentu

Na każdym z etapów postępowania z incydentem należy zwracać uwagę na odpowiednią jego klasyfikację. Klasyfikację incydentu należy zmienić jeśli w trakcie prac incydent zostanie inaczej zdiagnozowany.

DYREKTOR
Ośrodka Kultury w Wieliszewie
dr Dariusz Skrzydlewski

Ośrodek Kultury w Wieliszewie
Gminne Centrum Kultury
Łajski, ul. Stanisława Moniuszki 2
05-119 Legionowo
NIP: 536-17-86-510

Załącznik Nr 2 do Zarządzenia Nr 42/2021
Dyrektora Ośrodka Kultury w Wieliszewie
z dnia 16.06.2021 r.

Procedura weryfikacji tożsamości na odległość.

Celem dokumentu jest opisanie procedury weryfikacji tożsamości na odległość klientów i kontrahentów **Ośrodka Kultury w Wieliszewie.**

§1. Informacje ogólne

1. Administrator Danych ocenia, czy dokonywanie weryfikacji osób poprzez podanie danych osobowych jest adekwatne do celów, w których dane osobowe są przetwarzane, m.in. dla celu związanego z eliminacją możliwości oszustw.
2. Należy się bezwzględnie stosować do zasady ograniczonego celu przetwarzania danych oraz do zasady minimalizacji danych, a zatem przetwarzamy tyle danych, ile jest niezbędnych na daną chwilę.
3. Podczas weryfikacji tożsamości osoby fizycznej należy zadbać o spełnienie obowiązku informacyjnego z art. 13 RODO. Każda osoba, której tożsamość jest weryfikowana za podania danych osobowych ma prawo wiedzieć w jakim celu oraz jakie dane będą przetwarzane.
4. Przesłanką przetwarzania danych osobowych w ramach weryfikacji tożsamości na odległość jest art. 6 ust. 1 lit. f RODO, a zatem przetwarzanie danych osobowych jest w tym wypadku niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów administratora
5. Wszelkie budzące wątpliwość kwestie należy bezwzględnie konsultować z inspektorem ochrony danych osobowych: iod@wieliszew.pl, tel. 539-504-536.

§2. Przebieg weryfikacji na odległość

1. W razie braku możliwości stwierdzenia weryfikacji osoby na żywo, należy zaproponować weryfikację jej poprzez rozmowę telefoniczną.
2. Weryfikacja może odbyć się w następujący sposób:
   a) Pracownik informuje rozmówcę o celu przetwarzania danych osobowych;
   b) W celu weryfikacji tożsamości rozmówcy, pracownik prosi o podanie danych osobowych, na przetwarzanie których rozmówca wyraził wcześniej zgodę. Dane osobowe mogą dotyczyć: imienia, nazwiska, trzy ostatnie numeru PESEL, daty urodzenia, adresu e-mail, miejsca zamieszkania uczestnika zajęć lub rodzina/opiekuna prawnego.
   c) Po pozytywnej weryfikacji tożsamości, pracownik udostępnia wąski zakres danych dotyczących uczestnika zajęć. Są nimi: informacja o obecności na zajęciach, informacje

o zobowiązaniach finansowych w stosunku do Ośrodka Kultury w Wieliszewie obejmujące kwotę i zakres zaległości.

d) W przypadku negatywnej weryfikacji tożsamości, pracownik odmawia podania danych i o tym fakcie informuje pracownika merytorycznego odpowiedzialnego za ochronę przetwarzania danych osobowych w Ośrodku Kultury w Wieliszewie.

3. Pracownik nie ma prawa udostępniać w/w danych osobowych drogą elektroniczną.

DYREKTOR
Ośrodka Kultury w Wieliszewie
dr Dariusz Skrzydlewski

Ośrodek Kultury w Wieliszewie
Gminne Centrum Kultury
Łajski, ul. Stanisława Moniuszki 2
05-119 Legionowo
NIP: 536-17-86-510

Załącznik Nr 3 do Zarządzenia Nr 42/2021
Dyrektora Ośrodka Kultury w Wieliszewie
z dnia 16.06.2021 r.

Procedura niszczenia zebranych danych osobowych.

Celem dokumentu jest opisanie procedury niszczenia danych osobowych zebranych na nośnikach papierowych i elektronicznych w **Ośrodku Kultury w Wieliszewie.**

§1. Niszczenie dokumentów papierowych zawierających dane osobowe.

1. Raz w roku Dyrektor Ośrodka Kultury w Wieliszewie w drodze zarządzenia powołuje komisję ds. likwidacji danych osobowych.
2. Komisja jest złożona z minimum trzech pracowników Ośrodka, a do jej zadań należy:
   a) przegląd dokumentacji zawierającej dane osobowe;
   b) ocena celowości, przydatności i zasadności dalszego przetwarzania;
   c) dokonanie selekcji powyższej dokumentacji;
   d) kontrola i nadzór nad prawidłowym procesem niszczenia dokumentacji.
3. Członkowie komisji dokonują przeglądu dokumentacji zawierającą dane osobowe, oceniają celowości, przydatności, zasadności dalszego przetwarzania oraz dokonują selekcji.
4. Celem dokonania selekcji jest wyodrębnienie dokumentacji przeznaczonej do zniszczenia. Po jej dokonaniu pisemnie informują Dyrektora o dokonanej analizie dokumentacji.
5. Po uzyskaniu zgody Dyrektora, komisja przystępują do procesu niszczenia dokumentacji.
6. Niszczenie wyselekcjonowanej dokumentacji, ich zbiorów polega na:
   a) trwałym fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod
   b) anonimizacji danych osobowych, zbiorów polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.
7. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie.
8. W uzasadnionych przypadkach dokumentacja papierowa może być niszczona za pośrednictwem firmy wyspecjalizowanej w niszczeniu dokumentacji. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.
9. Potwierdzeniem zakończenia procesu zniszczenia dokumentacji jest sporządzony przez komisję protokół zniszczenia, a w uzasadnionych przypadkach protokół zniszczenia przekazany przez wyspecjalizowaną firmę.
10. Protokół zniszczenia jest zatwierdzany przez Dyrektora Ośrodka Kultury w Wieliszewie.

§2. Niszczenie dokumentów papierowych zawierających dane osobowe.

1. Raz w roku Dyrektor Ośrodka Kultury w Wieliszewie w drodze zarządzenia powołuje komisję ds. likwidacji danych osobowych.
2. Komisja jest złożona z minimum trzech pracowników Ośrodka, a do jej zadań należy:
3. Przegląd zbędnych nośników danych (dyski twarde, pendrive itp.) zawierającej dane osobowe;
   a) ocena celowości, przydatności i zasadności dalszego przetwarzania danych na nośnikach danych;
   b) dokonanie selekcji powyższych nośników danych;
   c) kontrola i nadzór nad prawidłowym procesem niszczenia;
   d) współpraca z Administratorem Sieci Informatycznej (ASI) na każdym etapie pracy.
4. Członkowie komisji w porozumieniu z ASI dokonują przeglądu zbędnych nośników zawierających dane osobowe, oceniają celowości, przydatności, zasadności dalszego przetwarzania oraz dokonują selekcji.
5. Celem dokonania selekcji jest wyodrębnienie nośników danych przeznaczonych do zniszczenia. Po jej dokonaniu pisemnie informują Dyrektora o dokonanej analizie. Pisemne uzasadnienie powinno zawierać przynajmniej: rodzaj nośnika, nr seryjny/produktu, nazwę nośnika, pojemność nośnika, imię i nazwisko użytkownika.
6. Po uzyskaniu zgody Dyrektora, komisja w porozumieniu z ASI przystępują do procesu niszczenia nośników danych.
7. W odniesieniu do nośników przenośnych oraz nośników danych zainstalowanych w komputerach – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
   a) za pomocą specjalistycznego oprogramowania;
   b) przy użyciu demagnetyzacji;
   c) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników;
8. Administrator Sieci Informatycznej przy obecności przynajmniej dwóch członków komisji dokonuje właściwego usunięcia danych z nośników a następnie sprawdza prawidłowości usunięcia informacji.
9. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
10. W uzasadnionych przypadkach nośniki danych mogą być niszczone za pośrednictwem firmy wyspecjalizowanej w niszczeniu tego typu urządzeń. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.
11. Potwierdzeniem zakończenia procesu zniszczenia jest sporządzony przez komisję protokół zniszczenia, a w uzasadnionych przypadkach protokół zniszczenia przekazany przez wyspecjalizowaną firmę.
12. Protokół zniszczenia jest zatwierdzany przez Dyrektora Ośrodka Kultury w Wieliszewie.

DYREKTOR
Ośrodka Kultury w Wieliszewie
dr Dariusz Skrzydlewski