INSTRUKCJA POSTĘPOWANIA NA WYPADEK NARUSZENIA OCHRONY DANYCH OSOBOWYCH

MYŚLENICKI OŚRODEK KULTURY I SPORTU

ul. Piłsudskiego 20,
32-400 Myślenice

NIP: 6811353451, REGON: 000284888

Zatwierdzenie dokumentu:	01.02.2019 r.
sporządził (a): Krzysztof Dybeł	
zatwierdził: Administrator Danych	p.o. Dyrektora Myślenickiego Ośrodka Kultury i Sportu mgr Piotr Szewczyk

INSPEKTOR OCHRONY DANYCH OSOBOWYCH
inż. Krzysztof Dybeł

Spis treści

1. TERMINY I DEFINICJE

Terminologia obowiązująca w niniejszym dokumencie została zdefiniowana w „Polityce bezpieczeństwa danych osobowych" (BA01-Polityka bezpieczeństwa DO) oraz „Instrukcji zarządzania systemami informatycznymi „(BA02-Instrukcja zarządzania SI). Pozostałe terminy zostały zdefiniowane poniżej.

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;

Incydent bezpieczeństwa informacji - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych, działań związanych z przetwarzaniem danych osobowych i zagrażają ich bezpieczeństwu.

Instrukcja postępowania – Instrukcja postępowania na wypadek naruszenia danych osobowych.

2. CELE INSTRUKCJI POSTĘPOWANIA

„Instrukcja postępowania" służy realizacji wymogów prawnych odnoszących się do przestrzegania praw i wolności osób których dane osobowe są przetwarzane w Myślenickim Ośrodku Kultury i Sportu.

„Instrukcja postępowania" ma umocowanie w następujących aktach prawnych:

a) 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.

„Instrukcja postępowania" jest jednym z fundamentów dokumentacji ochrony danych osobowych obowiązującym w Myślenickim Ośrodku Kultury i Sportu.

Podstawowymi celami „Instrukcji postępowania" jest:

- zapewnienie obsługi incydentów związanych z bezpieczeństwem danych osobowych,
- zapewnienie obsługi naruszeń ochrony danych osobowych zgodnie z wymogami RODO,
- stworzenie mechanizmów pozwalających na właściwą identyfikację naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa,
- stworzenie mechanizmów minimalizujących w przyszłości wystąpienie naruszeń i incydentów.

Powyższe cele będą realizowane poprzez:

- wskazanie czym jest naruszenie ochrony danych osobowych,
- wskazanie czym jest incydent bezpieczeństwa danych osobowych,
- enumeratywne wskazanie przykładów naruszenia ochrony danych osobowych i incydentów,
- przeprowadzenie procesu zgłoszenia do organu nadzorczego zgodnie z wymogami RODO,
- przeprowadzenie procesu informacyjnego dla osób których dane osobowe zostały naruszone,
- przeprowadzenie działań wyjaśniających przyczyny naruszenia,
- przeprowadzenie działań mających na celu zapobieganie w przyszłości podobnych zdarzeń.

3. ZAKRES INSTRUKCJI POSTĘPOWANIA

„Instrukcja postępowania na wypadek naruszenia ochrony danych osobowych" określa tryb postępowania w przypadku stwierdzenia incydentu bezpieczeństwa informacji, naruszenia ochrony danych osobowych lub powzięcia podejrzenia o takim naruszeniu.

„Instrukcja postępowania" opisuje sposoby identyfikacji incydentów bezpieczeństwa danych osobowych, oraz naruszenia ochrony danych osobowych.

Określa sposób zgłaszania naruszeń do organu nadzorczego. Oraz określa sposób zgłaszania naruszeń osobom fizycznym w przypadku naruszenia ich danych osobowych.

Stosowanie się do „Instrukcji postępowania" ma służyć wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych.

Obowiązek stosowania się do „Instrukcja postępowania" dotyczy wszystkich pracowników oraz współpracowników Myślenickiego Ośrodka Kultury i Sportu mających udział w przetwarzaniu danych osobowych.

Naruszenie zasad ochrony danych osobowych wynikających z przepisów prawa oraz przepisów wewnętrznych w tym „Instrukcji postępowania" stanowi pogwałcenie obowiązków pracowniczych, które może być sankcjonowane zgodnie z przepisami prawa, m.in. Kodeksem Pracy, Kodeksem Karnym, Kodeks Cywilnym.

4. NARUSZENIE (INCYDENT) OCHRONY DANYCH OSOBOWYCH

4.1. Naruszenie ochrony danych osobowych, może być spowodowane:

- niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;
- niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;
- umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe lub osób odpowiedzialnych za ich ochronę.

4.2. Za incydent ochrony danych osobowych uważa się w szczególności:

- pozostawienie istotnych zasobów informacyjnych (w tym danych osobowych) bez należytego dozoru;
- brak możliwości fizycznego dostępu do danych np.: zagubiony klucz do pomieszczenia, lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami,
- chwilowy brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć;
- próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia w którym jest przetwarzany; sytuacja, która wskazuje na np.: zmianę ułożenia kolejności dokumentów, pozostawienie otwartego pomieszczenia lub magazynu z danymi (np. szafy), nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;
- różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;
- próba nielegalnego logowania się do systemu lub włamania do systemu;
- zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych,

- niesprawne działanie lub nieuprawnione wyłączenie jakiegokolwiek elementu systemu zabezpieczeń,
- wystąpienie warunków, które stwarzają zagrożenie dla przechowywanych danych (zbyt wysoka temperatura, nadmierna wilgotność, pole elektromagnetyczne lub elektrostatyczne),
- stan pomieszczeń, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieuprawnione.

4.3. Za naruszenie ochrony danych osobowych uważa się w szczególności:

- kradzież lub zaginięcie dokumentacji zawierające dane osobowe;
- zmieniona, usunięta w nieuprawniony sposób zawartość w dokumentacji (np. brak części teczki osobowej);
- zniszczona dokumentacja, komputery, nośniki danych (akt wandalizmu, zalanie pożar);
- nieuprawniony dostęp do danych osobowych (wysłanie mailem do nieuprawnionych podmiotów);
- trwały brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć;
- zmieniona w sposób nieuprawniony zawartość bazy danych;
- nieuprawnione usunięcie danych osobowych w systemie;
- utrata kopii zapasowych;
- nieskuteczne niszczenie nośników informacji zawierających dane osobowe (nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;

5. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

5.1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na wystąpienie zdarzenia, które zostały opisane w pkt. 4 „Naruszenie (incydent) ochrony danych osobowych" niniejszej instrukcji, pracownik lub osoba wykonująca prace na rzecz Myślenickiego Ośrodka Kultury i Sportu zobowiązana jest do bezzwłocznego powiadomienia o tym fakcie przełożonego oraz Administratora (danych osobowych).

5.2. Pracownik lub osoba wykonująca prace na rzecz Myślenickiego Ośrodka Kultury i Sportu do momentu przybycia Administratora (danych osobowych) bądź upoważnionej przez niego osoby powinien:

- zabezpieczyć dostęp do pomieszczenia lub urządzenia,
- powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony,
- zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora (danych osobowych) lub osoby upoważnionej.

5.3. Po przybyciu na miejsce incydentu lub naruszenia danych osobowych, Administrator Danych lub osoba przez niego upoważniona następujące czynności:

- ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych,
- wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia,
- podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony,

- w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając upoważnionemu użytkownikowi stosowne polecenia i wskazówki do obsługi urządzeń,

5.4. W przypadku zakwalifikowaniu zdarzenia jako incydent lub naruszenie ochrony pracownik lub osoba wykonująca prace na rzecz Myślenickiego Ośrodka Kultury i Sportu w porozumieniu z Administratorem Danych przygotowuje "Notatkę z naruszenia ochrony danych osobowych":

- notatka powinna zawierać wnioski określające zakres działań organizacyjnych i technicznych pozwalających zlikwidować skutki naruszenia lub incydentu ochrony danych osobowych;
- notatka powinna zawierać opis środków zapobiegających ponownemu wystąpieniu naruszenia lub incydentu ochrony danych osobowych,
- Administrator Danych gromadzi notatki jako dowód na wystąpienie zdarzeń oraz sposobów postępowania;
- wzór notatki określony jest w załączniku nr 1 do niniejszej instrukcji.

5.5. W przypadku zakwalifikowaniu zdarzenia jako "naruszenie ochrony" oraz stwierdzeniu że zdarzenie doprowadziło do naruszenia praw i wolności osób których dane są przetwarzane dane osobowe pracownik lub osoba wykonująca prace na rzecz Myślenickiego Ośrodka Kultury i Sportu w porozumieniu z Administratorem Danych przygotowuje "Notatkę z naruszenia ochrony danych osobowych":

5.6. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 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.

5.7. Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO). Zgłoszenia naruszenia dokonuje się elektronicznie za pomocą odpowiedniego formularza, który znajduje się na stronie Urzędu Ochrony Danych Osobowych /www.uodo.gov.pl/.

5.8. Aktualny (na dzień wydania dokumentacji) wzór zgłoszenie naruszenia ochrony danych osobowych stanowi załącznik nr 2 do niniejszej instrukcji.

6. ZARZĄDZANIE DOKUMENTEM

Dokument wchodzi w życie z dniem podpisania przez Administratora.

Właścicielem tego dokumentu jest Administrator Danych lub upoważniona przez niego osoba.

Dokumentacja niniejszej polityki zawiera:

Załącznik nr 1. Notatka z naruszenia DO.

Załącznik nr 2. Zgłoszenie naruszenia ochrony danych.

Załączniki stanowią integralną część dokumentu – wymagają nadzoru, jednak dokonywane w nich zmiany (zawartość, sposób prezentacji) nie wymagają aktualizacji polityki bezpieczeństwa.

Aktualna wersja oraz data wydania jest wymaganym elementem identyfikacji załącznika.

7. HISTORIA DOKUMENTU.

Data / wydanie	Opis zmiany
20.09.2018 r. / v1	Utworzenie dokumentu.

Załącznik nr 1 do
Instrukcji postępowania na wypadek naruszenia ochrony danych osobowych

Notatka z naruszenia ochrony danych osobowych _____	**incydent / naruszenie***
Data zgłoszenia i godzina zgłoszenia:	
Imię, Nazwisko zgłaszającego:	
Lokalizacja:	
Opis zdarzenia, okoliczności, ilość danych osobowych których dotyczy naruszenie:	
Naruszone przepisy organizacyjne, prawne:	
Zgłoszono do organu nadzorczego data/ godzina/ forma zgłoszenia:	
Czy wymagane jest poinformowanie osób których dane osobowe naruszono Jeżeli tak, informacja o realizacji obowiązku:	TAK / NIE
Postępowanie wyjaśniające:	
Osoby odpowiedzialne za działania zapobiegawcze:	
Planowane działania zapobiegawcze/ termin realizacji:	
Osoby odpowiedzialne za likwidację skutków:	
Działania zaakceptował ADO (podpis):	
Uwagi:	
Ocena skuteczności (podpis):	