PODPIS ZAUFANY
MATEUSZ PIOTR
ZARYCHTA
23.11.2023 10:54:38 [GMT+1]
Dokument podpisany elektronicznie
podpisem zaufanym

Raport zgodności z RODO

Muzeum Historyczno-Etnograficzne w Chojnicach

ul. Podmurna 15,

89-600 Chojnice

Data sporządzenia raportu		23.11.2023 r.
Data przeprowadzenia audytu		30.10.2023 r.
Osoba Audytowana	**Pracownik sekretariatu**	Barbara Jażdżewska
Audytor	**IOD:**	Mateusz Zarychta

Spis treści

WNIOSKI Z AUDYTU:

Celem audytu było określenie poziomu zgodności przetwarzania danych osobowych w Muzeum Historyczno-Etnograficzne w Chojnicach.

W dniu 30.10.2023 r. przeprowadzono audyt RODO w zakresie zgodności stosowanych przepisów z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, zgodności z przepisami europejskiego rozporządzenia o ochronie danych osobowych (RODO) oraz zgodności z par. 20 rozporządzenia Krajowych Ram Interoperacyjności.

W wyniku przeprowadzonego audytu RODO w dniu 30.10.2023 r. nie stwierdzono rażących nieprawidłowości. W Muzeum realizowane są zasady bezpieczeństwa gromadzenia i przetwarzania danych osobowych zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych. Należy jednak zwrócić uwagę na wskazane w rekomendacjach obszary i dostosować je do obowiązujących w placówce dokumentów i przepisów.

Wskazany powyżej cel audytu został zrealizowany. Na podstawie przeprowadzonego audytu ustalono, że Muzeum Historyczno-Etnograficzne w Chojnicach jest zgodne w 85% z postanowieniami RODO.

OBSZARY AUDYTOWANE:

1) Bezpieczeństwo osobowe
2) Bezpieczeństwo sieci
3) Bezpieczeństwo sprzętu komputerowego
4) Bezpieczeństwo systemów i aplikacji

Na podstawie przeprowadzonych działań zidentyfikowano:

25 - zgodności z wymogiem

5 - nie dotyczy, pytanie wyłączone z badania

4 - niezgodności z wymogiem, które wymagają dostosowania do obowiązujących przepisów

WYNIK	
Suma ocen negatywnych * za ocenę negatywną uważa się oceny NIE oraz BRAK WIEDZY	4
Procent ocen negatywnych w stosunku do innych ocen *nie bierze się pod uwagę oceny NIE DOTYCZY	15%
Suma ocen pozytywnych * za ocenę pozytywną uważa się ocenę TAK	25
Procent ocen pozytywnych w stosunku do innych ocen *nie bierze się pod uwagę oceny NIE DOTYCZY	**85%**

DEFINICJE:

Użyte w niniejszym raporcie określenia należy rozumieć w następujący sposób:

1) **Administrator danych osobowych (ADO)** - osoba fizyczna lub prawna, organ publiczny, jednostka 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 (art. 4 pkt 7 RODO);

2) **Administrator Systemów Informatycznych (ASI)** - osoba wyznaczona przez administratora danych, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane przepisami o ochronie danych osobowych w przypadku nieskorzystania przez administratora danych z możliwości powołania administratora systemu informatycznego, pod wskazanym pojęciem rozumie się jednostkę organizacyjną właściwą w sprawach IT lub zewnętrzny podmiot zapewniający obsługę w zakresie funkcjonowania infrastruktury IT lub bezpośrednio administratora danych, w zakresie spraw związanych ze sprawnym funkcjonowaniem infrastruktury IT;
3) **Inspektor Ochrony Danych (IOD)** - osoba fizyczna wspierająca administratora danych w realizacji obowiązków dotyczących ochrony danych osobowych.
4) **Audyt** - „systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu" (PN-EN ISO 27000, pkt 2.5);
5) **Audytor -** osoba, która przeprowadza audyt;
6) **Audytowany** - organizacja, która jest audytowana;
7) **Bezpieczeństwo danych osobowych** - zachowanie poufności, integralności i dostępności danych osobowych (art. 32 ust. 1 RODO);
8) **Dane osobowe** - 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 (art. 4 pkt 11 RODO);
9) **Dowód z audytu** - zapisy, stwierdzenia faktu lub inne informacje, które są istotne ze względu na kryteria audytu i możliwe do zweryfikowania (PN-EN ISO 19011);
10) **Działanie korygujące** - działanie w celu wyeliminowania przyczyny niezgodności i zapobieżeniu powtórzeniu;
11) **RODO** - 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 (ogólne rozporządzenie o ochronie danych);
12) **KRI** - Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. W sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
13) **Przetwarzanie -** operacja 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;
14) **Osoba nieuprawniona** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, której dane nie dotyczą, nieposiadająca upoważnienia administratora do przetwarzania danych osobowych.

Cele, Zakres, Kryteria, Podstawa Audytu

Audyt został wykonany przez Inspektora Danych Osobowych placówki. Miał on charakter audytu planowego, wykonywanego w placówce raz w roku. Przeprowadzone działania miały za zadanie w sposób obiektywny sformułować opinię dotyczącą funkcjonującego systemu ochrony danych osobowych w kontekście spełnienia wymagań RODO.
Audyt został przeprowadzony z uwzględnieniem zasad określonych w normie PN-EN ISO 19011 Wytyczne dotyczące audytowania systemów zarządzania.

Cel Audytu

Celem audytu było określenie poziomu zgodności przetwarzania danych osobowych przez administratora danych z przepisami europejskiego rozporządzenia o ochronie danych osobowych (RODO) i zgodności z KRI.

Kryteria Audytu

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 1. 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);

2) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. W sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych w szczególności § 20. [System zarządzania bezpieczeństwem informacji]

3) Norma PN-ISO/IEC 27002 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady bezpieczeństwa informacji (wybrane zagadnienia wskazane w treści raportu);

4) Norma PN-EN ISO 19011 Wytyczne dotyczące audytowania systemów zarządzania.

Zakres Audytu

Zakres audytu wyznaczył funkcjonujący system ochrony danych osobowych.
W ramach audytu poddano weryfikacji następujące elementy:

1) analiza wypełniania obowiązków administratora danych wynikających z RODO,
2) analiza procesów przetwarzania danych osobowych, w stosunku do których organizacja jest administratorem danych, w zakresie zgodności z:
    a) zasadami przetwarzania danych osobowych,
    b) przetwarzania z prawem,
    c) obowiązkiem przejrzystego informowania i przejrzystej komunikacji oraz tryb wykonywania praw przez osobę,
    d) realizacji obowiązku informacyjnego,
    e) realizacji prawa umożliwienia dostępu do danych osobowych osobie, której dane dotyczą,
    f) dopełnieniem względem osób, których dane dotyczą obowiązku informacyjnego,
    g) uregulowaniem powierzania danych do przetwarzania,
    h) zasadami dotyczącymi zabezpieczenia danych osobowych (w tym m.in. realizowanie przez Zleceniodawcę obowiązku regularnego testowania, ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania),
    i) zasadami przekazywania danych do państw trzecich lub organizacji międzynarodowych,

j) uwzględniania ochrony danych w fazie projektowania oraz ich domyślnej ochrony,
k) rejestrowania czynności przetwarzania,
l) przetwarzania danych z upoważnienia administratora danych,

3) analiza procesów przetwarzania danych osobowych, w stosunku do których organizacja jest podmiotem przetwarzającym (procesorem danych),
4) analiza stosowanych przez organizację technicznych i organizacyjnych środków ochrony danych osobowych, w zakresie:
   a) adekwatności stosowanych zabezpieczeń,
   b) szyfrowania danych osobowych,
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
   e) zdolności do zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania

Opis Metodyki Audytu

Przeprowadzony audyt stanowił systematyczny, niezależny i udokumentowany proces mający na celu uzyskanie dowodów z audytu i dokonania ich obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu.

Główną metodą gromadzenia dowodów audytowych był wywiad osobowy połączony z weryfikacją powziętych informacji podczas przeprowadzonej wizji lokalnej wybranych pomieszczeń tworzących obszar przetwarzania danych osobowych.

Dodatkowymi metodami badawczymi były:

- analiza przekazanej dokumentacji,
- analiza stron internetowych oraz oficjalnych profili na portalach społecznościowych należących do administratora danych,
- weryfikacja funkcjonalności systemów informatycznych służących do przetwarzania danych osobowych wykorzystywanych przez administratora danych.

Wyniki przeprowadzonego audytu:

Muzeum Historyczno-Etnograficzne w Chojnicach jest placówką, w której dane osobowe są pozyskiwane min. w procesie rekrutacji pracowników i rejestracji zbiorów muzealnych. Są przez nią przetwarzane (m.in. poprzez przechowywanie, archiwizowanie, opracowywanie, zmienianie, usuwanie) oraz przekazywane na zewnątrz organizacji (np. uprawnionym organom Państwa, ubezpieczycielom, urzędom skarbowym, podmiotom służby zdrowia).
Analizie poddano zidentyfikowane procesy pozyskiwania danych osobowych (ustalenie podstaw prawnych przetwarzania, dopełnienie obowiązku informacyjnego), przetwarzania danych osobowych w ramach organizacji (adekwatność stosowanych technicznych i organizacyjnych środków ochrony danych) oraz przekazywania ich poza organizację (powierzenie przetwarzania, przekazywanie danych do państwa trzeciego).

Podczas kontroli zwrócono szczególną uwagę na analizę ryzyk i skutki ich wystąpienia jakie mogą one ze sobą nieść. Jednocześnie zostały wskazane metody przeciwdziałania danemu ryzyku uzyskując tym samym ocenę jego skuteczności.

USTALENIA AUDYTOWE:

lp.	Pytanie	Komentarz	Ocena	Rekomendacja
	Bezpieczeństwo osobowe			
1.	Czy pracownicy mają nadane upoważnienie określające zakres ich obowiązków związanych z przetwarzaniem danych osobowych?	Zostały zbadane dwie ostatnio zatrudnione osoby. Pracownicy mają nadane upoważnienie określające zakres obowiązków związanych z przetwarzaniem danych osobowych.	**zgodność**	Należy zaktualizować załącznik nr 4 (oświadczenie o spełnieniu przez ADO obowiązku informacyjnego) poprzez wykreślenie pobierania numeru PESEL przy tym oświadczeniu. Ponadto w załączniku nr 7 (upoważnienie) wskazać zbiory do których pracownik ma mieć dostęp, zgodnie z rejestrem czynności przetwarzania danych (zasada minimalizacji danych). Rekomenduje się, aby upoważnienia i oświadczenia przechowywać w teczkach osobowych pracowników.
2.	Czy pracownicy odbyli szkolenie z zasad przetwarzania i ochrony danych osobowych, w szczególności czy szkolenie odnosiło się do zagadnień związanych z pracą zdalną?	Pracownicy placówki zostali przeszkoleni z zasad przetwarzania i ochrony danych osobowych. Pracodawca zgodnie z zasadą rozliczalności powinien móc okazać dowód z przebytego przez pracownika szkolenia RODO.	**zgodność**	Rekomenduje się, aby kopię dowodu z przebytego szkolenia RODO przechowywać w teczce pracownika. (zasada rozliczalności)
3.	Czy pracownicy złożyli oświadczenie o zachowaniu w poufności danych osobowych, do których mają dostęp oraz środków ich ochrony?	Zostały zbadane dwie ostatnio zatrudnione osoby. Pracownicy złożyli oświadczenia o zachowaniu poufności danych osobowych.	**zgodność**	Rekomenduje się, aby oświadczenia przechowywać w teczkach osobowych pracowników. (zasada rozliczalności)
4.	Czy pracownicy znają i deklarują stosowanie polityk czystego ekranu i czystego biurka?	W placówce wprowadzona została polityka czystego ekranu i czystego biurka i jest ona przestrzegana.	**zgodność**	Brak rekomendacji.
5.	Czy w placówce znajdują się dokumenty dotyczące bezpieczeństwa przetwarzania danych osobowych? Czy pracownicy zapoznali się z powyższymi dokumentami?	W muzeum znajdują się dokumenty dotyczące bezpieczeństwa przetwarzania danych osobowych: Polityka Bezpieczeństwa Informacji, Instrukcja Zarządzania Systemem Informatycznym. Są one ogólnodostępne.	**zgodność**	Brak rekomendacji.

6.	Czy w placówce prowadzone są okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji, o których mowa w par. 20 ust. 2 pkt 3 rozporządzenia KRI?	W szkole znajduje się aktualna analiza ryzyka. Dokument znajduje się w segregatorze RODO.	**zgodność**	W przypadku wystąpienia któregokolwiek z ryzyk, należy zgłosić do IODO i uaktualnić dokument.
7.	Czy prowadzony jest Rejestr Czynności Przetwarzania danych osobowych zgodnie z art. 30 ust. 1 RODO?	W placówce prowadzony jest Rejestr Czynności Przetwarzania danych i jest on aktualny. Dokument znajduje się w segregatorze RODO.	**zgodność**	W przypadku zmian lub wystąpienia nowych czynności, należy zgłosić do IODO i uaktualnić dokument.
8.	Czy istnieje dokument określający zasady obowiązujące przy nadawaniu, modyfikowaniu i odbieraniu użytkownikom uprawnień? Jaki?	W placówce obowiązuje Instrukcja Zarzadzania Systemem Informatycznym w której opisane są zasady nadawania i odbierania uprawnień użytkownikom.	**zgodność**	Rekomenduje się uaktualnianie Załącznika nr 8 do Polityki bezpieczeństwa - Ewidencji osób upoważnionych do przetwarzania danych osobowych poprzez wpisanie daty odebrania uprawnień.
9.	Kto jest upoważniony i wg jakiego dokumentu do wstępu do pomieszczenia w którym przechowywane są serwery?	W muzeum nie ma serwerowni. Placówka ma podpisaną umowę na obsługę informatyczną z firmą zewnętrzną.	**zgodność**	Brak rekomendacji.
10.	Czy w umowach zawartych z podmiotami zew zewnętrznymi, zawarto zapisy mówiące o zobowiązaniu wykonawcy do zachowania w tajemnicy informacji do jakich może mieć dostęp w związku z realizacją przedmiotu umowy, zgodnie z par. 20 ust. 2 pkt 10 rozporządzenia KRI?	Podczas rozmowy zostały wskazane podmioty z którymi zostały zawarte umowy powierzenia danych osobowych min. w kategorii obsługi sieci informatycznej, BHP, Pomerania.	**zgodność**	Brak rekomendacji.
11.	Czy w jednostce komputery zabezpieczone są programem antywirusowym? Jaki?	W jednostce komputery zabezpieczone są programem antywirusowym ESET. Ważność do 22 listopada 2023 r.	**zgodność**	Brak rekomendacji.
12.	Proszę o wskazanie osób, które zakończyły zatrudnienie w Firmie w ostatnim czasie. Czy uprawnienia do dostępu do systemów informatycznych zostały im odebrane, zgodnie z	Podczas rozmowy została wskazana jedna osoba, która pracowała na stanowisku księgowej i potwierdzono odebranie uprawnień.	**zgodność**	Rekomenduje się uaktualnianie Załącznika nr 8 do Polityki bezpieczeństwa - Ewidencji osób upoważnionych do przetwarzania danych osobowych.

	par. 20 ust. 2 pkt 5 rozporządzenia KRI?			
	Bezpieczeństwo sieci			
13.	W jaki sposób pracownicy łączą się z siecią Internet?	W placówce Internet jest dostarczony przez pracodawcę. Sieć jest zabezpieczona.	**zgodność**	Brak rekomendacji.
14.	Jaka jest długość oraz złożoność hasła do Wifi?	12 znaków: małe i duże litery, znaki specjalne i cyfry	**zgodność**	Brak rekomendacji.
15.	Czy sieć Wi-Fi jest szyfrowana za pomocą protokołu WPA2/WPA3?	Podczas kontroli sprawdzono szyfrowanie protokołu.	**zgodność**	Brak rekomendacji.
16.	Czy sieć jest tak skonfigurowana aby funkcja WPS była wyłączona?	Obsługę sieci prowadzi firma zewnętrzna.	**nie dotyczy**	Brak rekomendacji.
17.	W jaki sposób zabezpieczony jest dostęp do panelu konfiguracyjnego urządzenia sieciowego?	Obsługę sieci prowadzi firma zewnętrzna.	**nie dotyczy**	Brak rekomendacji.
18.	Czy istnieje możliwość konfiguracji sprzętu sieciowego z urządzeń spoza sieci LAN?	Podczas kontroli sprawdzono możliwość konfiguracji sprzętu sieciowego z urządzeń spoza sieci LAN i stwierdzono, że dostęp zewnętrzny do panelu administracyjnego został wyłączony.	**zgodność**	Brak rekomendacji.
	Bezpieczeństwo sprzętu komputerowego			
19	Na jakim sprzęcie komputerowym pracują pracownicy, prywatnym czy udostępnionym przez pracodawcę? Jeżeli pracownicy pracują na sprzęcie prywatnym to czy posiadają dedykowane konto (o uprawnieniach użytkownika)?	W placówce pracownicy pracują na sprzęcie udostępnionym przez pracodawcę. Sprzęt nie jest zabierany do domu.	**zgodność**	Brak rekomendacji.
20	Jeżeli praca odbywa się na sprzęcie prywatnym, to czy weryfikowane jest spełnienie przez ten sprzęt zasad bezpieczeństwa?	W placówce laptopy nie są zabierane do domu przez pracowników.	**nie dotyczy**	Brak rekomendacji.

21	W jaki sposób zabezpieczona jest kontrola dostępu do sprzętu komputerowego? Jeżeli dostęp jest ograniczony hasłem to w jaki sposób wygląda długość i złożoność zmiany hasła?	Dostęp do sprzętu komputerowego zabezpieczony jest hasłem. Hasło składa się z minimum 8 znaków, dużych i małych liter, cyfr i znaku specjalnego. Brak wymuszenia zmiany hasła co 30 dni.	**zgodność**	Brak rekomendacji.
22	Czy sprzęt komputerowy, z którego korzystają pracownicy ma zaszyfrowany dysk twardy?	Podczas kontroli sprawdzony został komputer stacjonarny na którym zainstalowany jest system operacyjny Windows Home oraz laptop, na którym zainstalowany został system Windows Professional z automatyczną funkcją szyfrowania dysku.	**niezgodność**	Rekomenduje się zmianę systemu operacyjnego z Windows Home na Proffesional w celu lepszego zabezpieczenia dysku.
	Bezpieczeństwo systemów i aplikacji			
23	Jaka wersja systemu operacyjnego jest zainstalowana na komputerach, z których korzystają pracownicy? Czy systemy są skonfigurowane, aby aktualizowały się automatycznie?	Podczas kontroli sprawdzony został komputer stacjonarny na którym zainstalowany jest system operacyjny Windows Home oraz laptop, na którym zainstalowany został system Windows Professional z automatyczną funkcją szyfrowania dysku.	**niezgodność**	Rekomenduje się zmianę systemu operacyjnego z Windows Home na Proffesional.
24	Jakie uprawnienia posiadają pracownicy (użytkownik czy administrator)?	Podczas kontroli sprawdzony został komputer stacjonarny oraz laptop, na obydwu stanowiskach pracownicy posiadali konta administratora.	**niezgodność**	W celu zwiększenia bezpieczeństwa sieci i danych rekomenduje się zmianę ustawień kont pracowników z administratora na użytkownika.
25	W przypadku sprzętu prywatnego - czy użytkownicy do codziennego użytkowania korzystają z kont użytkownika, a nie administratora?	Pracownicy nie korzystają ze sprzętu prywatnego	**nie dotyczy**	
26	Z jakich systemów i aplikacji korzystają pracownicy?	Symfonia, Musnet, Pakiet Office	**zgodność**	Brak rekomendacji.
27	Czy w związku z wykorzystywanymi systemami i aplikacjami dochodzi do przekazywania danych do	Placówka nie przekazuje danych do państw trzecich.	**zgodność**	Brak rekomendacji.

	państw trzecich? Jeżeli tak, na jakiej podstawie?			
28	Czy do służbowej poczty pracownicy wykorzystują prywatną pocztę e-mail?	W placówce wszyscy pracownicy korzystają ze skrzynek mailowych założonych w domenie muzeum. Poczta e-mail byłej księgowej jest nadal w pełni aktywna i przekierowana na konto obecnie zatrudnionej p. księgowej.	**zgodność**	Rekomenduje się jednak aby konto pocztowe byłego pracownika, było zablokowane, a jedynie przekierowane.
29	Czy systemy i aplikacje są aktualizowane automatycznie?	Wszystkie systemy i aplikacje zainstalowane na komputerach są aktualizowane automatycznie.	**zgodność**	Brak rekomendacji.
30	Czy na komputerach, z których korzystają pracownicy została zainstalowana zapora sieciowa (firewall)?	Na komputerach wbudowana jest standardowa zapora sieciowa systemu operacyjnego	**zgodność**	Brak rekomendacji.
31	Czy prowadzona jest w ewidencja osób upoważnionych do przetwarzania danych osobowych? Czy jest ona uaktualniana?	W placówce prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych zgodnie z załącznikiem nr 8 do Polityki Bezpieczeństwa Informacji. Podczas kontroli została sprawdzona aktualność danych ewidencji osób upoważnionych do przetwarzania danych osobowych. Stwierdzono w niektórych przypadkach brak uzupełnienia daty odebrania uprawnień.	**zgodność**	Rekomenduje się uaktualnianie Załącznika nr 8 do Polityki bezpieczeństwa - Ewidencji osób upoważnionych do przetwarzania danych osobowych poprzez wpisanie daty odebrania uprawnień. Dokument może być prowadzony w postaci elektronicznej.
32	Czy osoby techniczne (nie związane bezpośrednio z przetwarzaniem danych osobowych) mają podpisane upoważnienie do przebywania w pomieszczeniach w których są przetwarzane dane osobowe?	Podczas kontroli stwierdzono brak takich osób	**nie dotyczy**	

33	Czy w placówce prowadzony jest dziennik ASI?	Podczas kontroli stwierdzono brak dziennika ASI będącego załącznikiem do Instrukcji Zarządzania Systemem Informatycznym. Brak jest tym samym historii najważniejszych przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.	**niezgodność**	Rekomenduje się stosowanie do Procedur Instrukcji Zarządzania Systemem Informatycznym i prowadzenie dziennika ASI w wersji elektronicznej.
34	Czy na stronie internetowej placówki znajduje się aktualna polityka bezpieczeństwa? Czy dane kontaktowe IOD zostały opublikowane na stronie internetowej lub jeśli nie prowadzi strony, w sposób ogólnie dostępny w miejscu prowadzenia swojej działalności? *jeśli tak, proszę wskazać gdzie zostały opublikowane dane oraz w jakim zakresie	Na stronie internetowej znajduje się zakładka "RODO". Znajdują się tam wymagane klauzule i informacje za wyjątkiem danych IOD zgodnie z art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych	**zgodność**	Rekomenduje się uzupełnienie treści znajdującej się na stronie internetowej o wymagane zgodnie z ustawą RODO dane IOD. Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, (...wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora...) niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Po dokonaniu całkowitej analizy stwierdza się że w Muzeum Historyczno-Etnograficzne w Chojnicach ryzyko jest na poziomie nieznacznym, co jest w pełni akceptowalnym ryzykiem.

Stosując się do zaleceń opisanych powyżej, prawdopodobieństwo wystąpienia ryzyka ocenia się na znikome. Oznacza to, że zdarzenie może zaistnieć jedyne w wyjątkowych okolicznościach.