ZARZĄDZENIE NR 13/2022
p.o. Dyrektora Instytutu Dziedzictwa i Dialogu
– Łaźnia Moszczenica w Jastrzębiu-Zdroju
z dnia 29 lipca 2022 roku
w sprawie ustalenia Regulaminu dla osób przetwarzających dane osobowe
w Instytucie Dziedzictwa i Dialogu- Łaźnia Moszczenica w Jastrzębiu-Zdroju

Na podstawie:

1) Ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej,
2) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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

1. Wprowadzam Regulamin dla osób przetwarzających dane osobowe w Instytucie Dziedzictwa i Dialogu-Łaźnia Moszczenica w Jastrzębiu-Zdroju, stanowiącą załącznik Nr 1 do niniejszego Zarządzenia.
2. Pracownicy Instytutu Dziedzictwa i Dialogu – Łaźnia Moszczenica są zobowiązani do zapoznania się z treścią Regulaminu oraz jego przestrzegania.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 1 sierpnia 2022r

p.o. Dyrektora
Izabela Grela
.....
(podpis i pieczątka imienna dyrektora)

Przemysław Czech
Radca Prawny
WT 3122

Załącznik Nr 1
Do Zarządzenia Nr 13/2022
Dyrektora
Instytutu Dziedzictwa i Dialogu
– Łaźnia Moszczenica
w Jastrzębiu-Zdroju
z dnia 29 lipca 2022 roku

Regulamin dla osób przetwarzających dane osobowe w Instytucie Dziedzictwa i Dialogu– Łaźnia Moszczenica w Jastrzębiu-Zdroju

§ 1
DEFINICJE

1. Rozporządzenie - rozumie się przez to 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) obowiązujące od 25 maja 2018 r.;
2. Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, 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;
3. Administrator – (Instytut Dziedzictwa i Dialogu - Łaźnia Moszczenica w Jastrzębiu-Zdroju, mającym swoją siedzibę w 44-335 Jastrzębie-Zdrój, ul 1 Maja 45, NIP: 6332245278, Regon: 520605172, dalej jako 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 ;
4. Osoba przetwarzająca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
5. Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
6. Obszar przetwarzania – miejsce gdzie przetwarzane są dane osobowe biura, pomieszczenia na terenie siedziby Administratora lub poza nią.
7. Inspektor Ochrony danych – osoba sprawująca nadzór nad przetwarzaniem danych osobowych na podstawie Art. 39 RODO

§ 2
ZAKRES STOSOWANIA

1. Każda osoba przetwarzająca dane osobowe i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie Administratora. Przetwarzanie takie rozumiemy jako niezbędne i wynikające z określonego zakresu czynności, wynikające z zajmowanego stanowiska zgodnie z zakresem czynności lub na inne wyraźnie polecenie Administratora lub przełożonego.
2. Dane osobowe należy chronić niezależnie od ich formy zarówno w formie tradycyjnej jak i danych przetwarzanych w systemach informatycznych.
3. Do ochrony danych osobowych zobowiązane są wszelkie osoby je przetwarzające w jakikolwiek sposób taki jak:
   - Wprowadzanie, modyfikowanie i usuwanie danych w systemach informatycznych do tego przeznaczonych
   - Tworzenie, modyfikowanie, przenoszenia, kopiowanie, skanowanie inne powielanie, przechowywanie, przeglądanie i usuwanie.
   - Udostępnianie, przesyłanie lub przekazywane danych w sposób werbalny.

§ 3
ZABEZPIECZENIA FIZYCZNE

1. Osoba przetwarzająca zobowiązuje się do:
   - niepozostawiania obszarów przetwarzania danych bez nadzoru, pozostawiania w nim osób postronnych bez osób upoważnionych;
   - nieprzenoszenia jakiejkolwiek dokumentacji do pomieszczeń do tego nie przeznaczonych;
   - w przerwie pomiędzy sesjami (np. po godzinach pracy) pracy w pomieszczeniach lub na biurkach pozostawiania dokumentów zawierających informacje chronione;
   - nieużywania powtórnie jednostronnie zadrukowanych dokumentów informacjami chronionymi;
   - strzeżenia akt, teczek, przenośnych nośników pamięci i urządzeń;
   - niepozostawiania dokumentów i urządzeń w samochodach i miejscach publicznych;
   - ustawiania ekranów komputerowych w sposób uniemożliwiający podgląd zawartości osobom niepowołanym;
   - niezapisywania haseł na papierze bądź innym nośniku;
   - niepodłączania do listew podtrzymujących napięcie urządzeń mogących spowodować zakłócenia w pracy bez zgody obsługi technicznej;
   - dbania o techniczne warunki pracy sprzętu informatycznego (unikanie zalania, zabrudzenia klawiatury);
   - chowania do szaf lub szuflad zamykanych na klucz wszystkich druków zawierających dane osobowe, z których nie korzysta się w danej chwili ;
   - przestrzegania ustalonej polityki dostępu do pomieszczeń;
   - zamykania okien w przypadku opuszczania pomieszczenia po pracy;
   - ochrony dokumentów i urządzeń przed zniszczeniem, zalaniem, zabrudzeniem;
   - niszczenia niepotrzebnych dokumentów za pomocą niszczarek.

§ 4
ZABEZPIECZENIA INFORMACJI W POSTACI ELEKTRONICZNEJ

1. Osoba przetwarzająca zobowiązuje się do:
   - nieudostępniania identyfikatora do sytemu informatycznego i hasła inne osobie oraz niewykorzystywania identyfikatora innej osoby ;
   - niezapisywania danych (np. Umów z kontrahentami) w zasobach lokalnych komputerów i na mobilnych nośnikach informacji (CD, DVD, PenDrive, itp.) bez zgody Administratora, a w przypadku koniecznego użycia trwałego usuwania danych zapisanych na elektronicznych nośnikach przenośnych po ich użyciu a zapisywania wyłącznie w określonych przez Administratora miejscach np. folderach/udziałach sieciowych w celu przechowywania skanów dokumentów w przypadku udostępnionej takiej możliwości pracy ;
   - powstrzymania się i osób niepowołanych od samodzielnej ingerencji w oprogramowanie i konfigurację sprzętu;
   - przestrzegania swoich uprawnień w systemie;
   - zgłaszanie nadmiernych uprawnień;
   - przesyłania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej (lub zabezpieczonej hasłem) i tylko zgodnie z zatwierdzonymi zasadami;
   - usuwania zbędnych wiadomości z programów pocztowych;
   - nie wynoszenia danych poza siedzibę Administratora z wyłączeniem komputerów przenośnych przeznaczonych do tego celu;
   - wykonywania kopii roboczych wyłącznie w zakresie procedur i na polecenie;
   - przestrzegania obowiązujących procedur i instrukcji;
   - przestrzegania polityki „czystego biurka i ekranu" tj.: w przerwie pomiędzy sesjami pracy pracownika komputer jest wyłączony lub zablokowany, a monitor komputera pozbawiony jest jakichkolwiek nośników niosących informacje. Przerwa pomiędzy sesjami pracy to dłuższy czas, w którym nie przebywa się przy swoim komputerze.

§ 5
ZAMIESZCZANIE TREŚCI NA STRONACH INTERNETOWYCH, PROFILACH SPOŁECZNOŚCIOWYCH, W ZWIĄZKU Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

1. Postanowienia regulaminu dotyczą zarówno redaktorów odpowiedzialnych za zamieszczanie treści, jak i osób, które te treści przygotowują do publikacji [autorzy treści].
2. Każda treść, tzn. tekst, grafika, zdjęcie, film lub inne multimedium, musi zostać przygotowane z poszanowaniem praw autorskich - autor treści jest odpowiedzialny za zagwarantowanie spełnienia tego warunku.
3. Każda treść, tzn. tekst, grafika, zdjęcie, film lub inne multimedium, musi zostać przygotowane z poszanowaniem dóbr osobistych oraz prawa do prywatności osób, których dane są zawarte w treści - autor treści jest odpowiedzialny za zagwarantowanie spełnienia tego warunku.
4. Treści publikowane na stronie nie mogą: naruszać powszechnie obowiązujących przepisów prawa, być wulgarne, namawiać do nienawiści, być niezgodne z polityką i wizerunkiem firmy. Autor treści jest odpowiedzialny za zagwarantowanie spełnienia tego warunku.
5. Na stronie internetowej mogą być publikowane dane osobowe pracowników i współpracowników w zakresie ich danych służbowych, jeżeli jest to niezbędne do

zapewnienia klientom kontaktu z nimi. Przez dane służbowe rozumie się: imię, nazwisko, stanowisko, miejsce pracy, wydział, służbowy adres e-mail, służbowy numer telefonu.

6. Publikowanie na stronie internetowej innych danych osobowych pracowników lub współpracowników, w tym ich wizerunków, dozwolone jest pod warunkiem uzyskania od nich uprzedniej, udokumentowanej zgody. Autor treści jest odpowiedzialny za zagwarantowanie spełnienia tego warunku.
7. Publikowanie na stronie internetowej danych osobowych klientów, gości, uczestników wydarzeń lub innych osób, dozwolone jest pod warunkiem uzyskania od nich uprzedniej, udokumentowanej zgody. Autor treści jest odpowiedzialny za zagwarantowanie spełnienia tego warunku.
8. Publikowanie na stronie internetowej wizerunków osób fizycznych w oparciu o zwolnienia z konieczności uzyskania zgody na publikację, wskazane w przepisach prawa autorskiego, wymaga weryfikacji każdej treści przez osobę odpowiedzialną za jej przygotowanie. W tym wypadku autor treści jest odpowiedzialny za wykazanie, że warunki zwalniające z obowiązku uzyskania zgody zostały spełnione.
9. Jeżeli treść zawiera wypowiedź innej osoby, autor treści przed jej przekazaniem do publikacji przekazuje ją do autoryzacji autorowi wypowiedzi. Zabronione jest publikowanie treści bez uprzedniej autoryzacji.
10. Autor treści przekazując redaktorowi tę treść do publikacji, informuje o planowanym terminie usunięcia/ ustania publikacji.
11. Jeżeli CMS strony umożliwia takie działanie, podczas publikacji redaktor ustawia czas ustania publikacji treści.
12. Redaktor strony jest odpowiedzialny za dokonywanie przeglądu treści zawartych na stronie co ..... w celu usuwania treści, których przydatność już ustała.

§ 6
KOMUNIKACJA Z PODMIOTAMI ZEWNĘTRZNYMI

1. Jako podmioty zewnętrzne rozumiemy innych Administratorów niż:
    - Urzędy państwowe lub samorządowe
    - Ubezpieczyciele;
    - Banki
    - Inne podmioty, w tym upoważnione na podstawie przepisów prawa (np. ZUS, US, PFRON itp.)

    W celu prawidłowej komunikacji i przesyłania danych zgodnie z prawem stosujemy się wyłączenie do wytycznych tych podmiotów oraz korzystamy z narzędzi przez nich udostępnionych np. udostępnione portale internetowe. Za prawidłowe przetwarzanie danych od momentu uzyskania od osoby której dotyczą do momentu przekazania do podmiotu zewnętrznego odpowiada Administrator a osoba przetwarzająca za odpowiada przetwarzanie zgodnie z wykonywaną pracą lub na jego polecenie.
2. Przesyłanie załączników na portal podmiotu zewnętrznego:

    Dane zebrane od osoby przechowujemy w bezpiecznym miejscu i określonym przez Administratora/ Administratora systemu informatycznego.

Po zebraniu danych od osoby i umieszczeniu ich na udostępnionym portalu podmiotu zewnętrznego należy przechowywać dane wyłączenie przez czas konieczny do realizacji operacji przetwarzania. Po ukończeniu operacji przetwarzania dane należy usunąć jeśli nie wymaga tego przepis prawa lub Administrator, dotyczy to również usuwania poczty elektronicznej.

3. Korzystanie z poczty elektronicznej

   Dane zebrane od osoby przechowujemy w bezpiecznym miejscu i określonym przez Administratora a przesyłane jako załączniki pocztą elektroniczną podlegają szyfrowaniu:

   - Pliki typu MS Office lub Open Office konwertujemy do formatu PDF lub zabezpieczamy hasłem dostępowym a hasło udostępniamy innym kanałem informacyjnym np. telefonicznie.
   - Pliki typu PDF możemy zabezpieczyć hasłem zabezpieczamy programem np.: PDFMate Free PDF Merger, hasłem dostępowym do otwarcia pliku hasło udostępniamy innym kanałem informacyjnym np. telefonicznie.
   - Zaleca się jednak pliki zawierające dane, w szczególności zbiory plików spakować z hasłem np. programem **7zip** lub innym programem szyfrującym.
   - Dane osobowe można przesłać osobie, której dane dotyczą w postaci nieszyfrowanej wyłącznie za jej potwierdzoną zgodą.

4. Urządzenia mobilne , smartfony.
   Do przechowywania danych osobowych, zdjęć dokumentów zawierających dane, danych adresowych nie używa się telefonów z wyłączeniem danych kontaktowych w zakresie: imię, nazwisko, firma, numer telefonu. Na urządzeniach mobilnych zainstalowany jest system antywirusowy.

5. Chmury obliczeniowe.
   Do przechowywania danych osobowych w postaci nieszyfrowanej nie korzysta się z chmur obliczeniowych (np. Google drive / Dropbox/ ICloud / Onedrive itp.) .

§ 7
ZGŁASZANIE INCYDENTÓW

1. Użytkownik stwierdzający naruszenie bezpieczeństwa danych osobowych jest zobowiązany zawiadomić natychmiast Administratora o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa, a w szczególności o:
   - naruszeniu hasła lub identyfikatora (problemy z zalogowaniem);
   - całkowitym lub częściowym braku danych albo dostępie szerszym niż wynikającym z uprawnień;
   - braku dostępu do aplikacji lub zasobu;
   - wykryciu wirusa komputerowego;
   - zauważeniu śladów włamania komputerowego;
   - znaczącym spowolnieniu pracy systemu;
   - innych dziwnych objawach nienaturalnej pracy komputera (np. samoczynne przesuwanie się kursora);
   - podejrzeniu kradzieży sprzętu lub dokumentów;
   - zauważeniu śladów usiłowania włamania do pomieszczeń lub szaf
   - w przypadku naruszenia należy natychmiast skontaktować się skutecznie z inspektorem ochrony danych pod numerem 664 309 439.

§ 8
ZABEZPIECZENIA ORGANIZACYJNE

1. We wszystkich sytuacjach nieopisanych w procedurach lub niejasnych, podejrzanych sytuacjach należy niezwłocznie inspektora ochrony danych lub bezpośrednio przełożonego.

§ 9
DOMYŚLNA OCHRONA DANYCH

1. Wszelkie zmiany w procesach przetwarzania danych wymagają stosowania domyślnej ochrony danych tj. zapewnienia ich ochrony już w fazie projektowania. Zapewnia się to poprzez konsultacje z Inspektorem ochrony danych bezpośrednio lub za pośrednictwem przełożonego.

§ 10
UDOSTĘPNIANIE DANYCH I REALIZACJA PRAW

1. Każda zidentyfikowana osoba (Np. pracownik, klient, potencjalny klient) ma prawo dostępu do swoich danych i ich poprawiania. Dane osobowe udostępniane są innym podmiotom przez Administratora w porozumieniu z Inspektorem Ochrony Danych. Inne prawa jak usuwanie, sprzeciw, przenoszenie realizowane są na wniosek osoby której dane dotyczą.