AGENCJA ROZWOJU DYDAKTYCZNEGO

EDU ODO

MUZEUM W GOSTYNIU
Znak sprawy MG-153-15/18
Data wpływu 17.08.2018
Referent

Regulamin Ochrony Danych Osobowych

Nazwa podmiotu wprowadzającego	Muzeum w Gostyniu
Data wprowadzenia	17 sierpnia 2018 r.
Numer zarządzenia wprowadzającego	3/2018 z dn. 17.08.2018
Podpis ADO	DYREKTOR mgr Robert Czub
Podpis IOD	

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad dotyczących ochrony danych osobowych dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z wymienionych osób jest zobowiązana do zapoznania się z poniższym regulaminem oraz oświadczenia o stosowaniu zasad w nim zawartych własnoręcznym podpisem.

1. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW, NOŚNIKÓW ZEWNĘTRZNYCH

1. Jeśli użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony, dyski, pendrive, itp.,
2. Użytkownik ma obowiązek natychmiastowo zgłosić zagubienie, utratę, awarię lub zniszczenie powierzonego mu sprzętu IT,
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci), samowolne instalowanie oprogramowania bez wiedzy administratora lub podłączanie jakichkolwiek niezatwierdzonych przez administratora urządzeń (typu smartfon lub pendrive) do systemu informatycznego jest zabronione,
4. Użytkownik nie może umożliwiać osobom nieupoważnionym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych przez:
    a) Odwrócenie monitora w taki sposób, aby nie był możliwy wgląd,
    b) Niedopuszczenie osób niepowołanych do stanowiska,
    c) Korzystanie z filtra prywatyzującego, jeśli niemożliwe jest zrealizowanie pkt 4.a),
5. Przed odejściem od stanowiska pracy, użytkownik musi wywołać wygaszacz ekranu blokowanym hasłem (skrót klawiszowy: WINDOWS + L) oraz wylogować się z programów, w których przetwarza dane osobowe,
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    - Wylogować się z systemu informatycznego (jeśli to wymagane) następnie wyłączyć sprzęt komputerowy,
    - Zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki, na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów),
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem),

2. ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik posiadający dostęp do danych osobowych w systemie informatycznym (np. na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się. Wyjątek stanowi konto użytkownika w systemie Windows,
2. Osoba odpowiedzialna za nadawanie uprawnień do dostępu do danych w systemie informatycznym nadany login oraz pierwsze hasło podaje w formie ustnej,
3. Użytkownik zobowiązany jest do niezwłocznej zmiany hasła po jego otrzymaniu,

4. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji tylko na wyraźne polecenie administratora i przy realizacji administratorów systemu,
5. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora w systemie, tworzenia kont gościa, itd.
6. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym użytkownikom pracy na koncie i przekazywania danych dostępowych takich jak login i hasło innemu użytkownikowi,

3. POLITYKA HASEŁ

1. Hasło dostępowe użytkownika składa się z minimum 8 znaków,
2. Hasło dostępowe użytkownika składa się z dużych liter + małych liter + minimum 1 cyfry (lub znaku specjalnego),
3. Hasło nie może być łatwe do odgadnięcia. Nie można stosować powszechnie używanych słów,
4. W szczególności zabrania się wykorzystywania, jako haseł: dat (narodzin, ślubu, czy innych ważnych wydarzeń), imion i nazwisk osób bliskich, imion zwierząt, popularnych słów, typowych zestawów: 123456, qwerty itp.,
5. Hasła nie mogą być ujawnianie innym osobom. Zabrania się zapisywania haseł na kartkach i w notesach (również prywatnych), naklejania ich na komputerze, trzymania pod klawiaturą, w szufladzie lub na tablicy korkowej. Hasło zapisane musi być przechowywane w zamkniętej kopercie w sejfie,
6. W przypadku ujawnienia hasła – należy natychmiast je zmienić,
7. Hasła muszą być zmieniane nie rzadziej, niż co 30 dni
8. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła,
9. Jeżeli system umożliwia, administrator jest zobowiązany ustawić wymuszanie zmiany hasła.

4. ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ ZAWIERAJĄCEJ DANE OSOBOWE

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. polityki czystego biurka i czystej drukarki. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy,
2. Pomieszczenia, w których przetwarzane są dane osobowe muszą być każdorazowo zamykane na klucz po wyjściu ostatniej osoby,
3. Klucze do drzwi nie mogą pozostawać w zamku (zarówno od wewnątrz jak i od zewnątrz),
4. Klucze do szaf i biurek po godzinach pracy lub podczas nieobecności pracownika w trakcie godzin pracy nie mogą pozostawać w zamkach. Muszą one być schowane w miejsce niedostępne dla osób nieuprawnionych. Za takie miejsce nie uznaje się pierwszej otwartej szuflady w biurku, czy szufladek na dokumenty,

5. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków po ustaniu ich przydatności w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji,
6. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych, na tablicach korkowych, biurkach itd.,
7. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.
8. Zabrania się zabierania dokumentów do domu w celu utylizacji ich w prywatnym systemie grzewczym (np. w piecu, kominku).

5. ZASADY WYNOSZENIA NOŚNIKÓW DANYCH ORAZ DOKUMENTÓW POZA JEDNOSTKĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez pisemnej zgody administratora. Do takich nośników zalicza się m. in.: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash i inne dokumenty papierowe,
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, hasłowane pliki). Punkt nie dotyczy dokumentów papierowych,
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach,
4. Należy korzystać tylko ze sprawdzonych firm kurierskich,
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem, kradzieżą, zniszczeniem itd.,

6. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych,
2. Zabrania się zgrywania na dysk twardy komputera, instalowania oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania systemem informatycznym i tylko w uzasadnionych przypadkach,
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu,
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem),
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł,
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego

się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Użytkownicy mogą także korzystać z Internetu dla celów prywatnych, ale wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.
9. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego administratora.
10. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
11. W zakresie dozwolonym przepisami prawa, administrator zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad.
12. Ponadto, w uzasadnionym zakresie, administrator zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.
13. Administrator może również blokować dostęp do niektórych treści dostępnych przez Internet.

7. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem skrzynki e-mailowej poza jednostkę może odbywać się tylko przez osoby do tego upoważnione,
2. W przypadku przesyłania danych osobowych poza jednostkę lub w jej strukturach należy wykorzystywać mechanizmy kryptograficzne (minimum przy użyciu programu ZIP),
3. W przypadku zabezpieczenia plików hasłem, obowiązuje system minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, a hasło należy przesłać inną metodą, np. telefonicznie lub SMS-em. Zabrania się przesyłania hasła na ten sam adres mailowy, na który zostały wysłane pliki z danymi,
4. Użytkownicy zobowiązani są zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu, aby uniknąć przesłania plików do osób nieuprawnionych,
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata. W zastępstwie można użyć opcji automatycznego potwierdzenia otrzymania wiadomości w programie pocztowym,
6. Zabrania się otwierania załączników (plików) nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile mogą zawierać załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy,

7. Bez weryfikacji wiarygodności nadawcy, zabrania się „klikania" w hiperłącza w mailach, gdyż mogą to być odnośniki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki link bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy,
8. Każdy przypadek wykrycia podejrzanych wiadomości należy zgłaszać administratorowi,
9. Użytkownicy nie mogą rozsyłać maili niezwiązanych z pracą w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 200 osób,
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!,
11. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze. Jest to możliwe tylko w wyjątkowych sytuacjach, takich jak konieczność realizacji obowiązków służbowych,
12. Użytkownicy powinni minimum raz w miesiącu kasować niepotrzebne maile,
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych,
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników,
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i za wyraźną zgodą administratora,
16. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych,
17. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego,
18. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania,
19. Użytkownik bez zgody administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

8. OCHRONA ANTYWIRUSOWA

1. Administrator systemu zobowiązany jest do instalacji oprogramowania antywirusowego na każdym komputerze,
2. Użytkownicy zobowiązani są do skanowania plików i wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada,
3. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe,
4. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, Wykryto zagrożenie!", użytkownik obowiązany jest

poinformować niezwłocznie o tym fakcie administratora, inspektora ochrony danych lub administratora systemu.

9. *SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH DLA UŻYTKOWNIKA*

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do niezwłocznego powiadomienia administratora lub inspektora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych,
2. Do sytuacji wymagających powiadomienia, należą:
    a) Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b) Niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c) Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
    a) Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b) Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c) Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:
    a) Ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
    b) Dokumentacja jest niszczona bez użycia niszczarki,
    c) Fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    d) Otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    e) Ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
    f) Wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia administratora,
    g) Udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
    h) Telefoniczne próby wyłudzenia danych osobowych,
    i) Kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
    j) Maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    k) Pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,

l) Hasła do systemów przyklejone są w pobliżu komputera.

5. Powiadomienie administratora lub inspektora ochrony danych jest konieczne w sytuacji, gdy zachodzi podejrzenie utraty danych osobowych lub utraty ich bezpieczeństwa.

10. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) Przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez administratora zadaniach,
   b) Zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez administratora,
   c) Niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez administratora,
   d) Zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e) Ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem,
2. Każda osoba dopuszczona do przetwarzania jest zaznajamiana z zasadami ochrony danych osobowych przed rozpoczęciem ich przetwarzania. Zaznajomienia dokonuje wyznaczony inspektor ochrony danych lub administrator,
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są do podpisania upoważnienia do przetwarzania danych,
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego,
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

11. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Administrator zobowiązany jest do prowadzenia rejestru udostępnień danych osobowych,
2. Wnioski o udostępnienie danych osobowych mogą być przyjmowane przez każdą osobę upoważnioną. Wymaga się żądania wniosku w formie pisemnej dla celów dowodowych,
3. Każdy otrzymany wniosek o udostępnienie danych osobowych należy przekazać na ręce administratora lub inspektora ochrony danych
4. Udostępnienia danych dokonać może tylko administrator, każdorazowo uwzględniając takie udostępnienie w rejestrze udostępnień danych osobowych

12. DOKUMENTY DODATKOWE

1. Jako załącznik do regulaminu zostaną wprowadzone dokumenty określające:

a) Wykaz miejsc przetwarzania danych osobowych,
b) Wykaz danych przetwarzanych przez administratora,
c) Wykaz zabezpieczeń stosowanych przez administratora.

13. ZAPISY KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy,
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez administratora lub inspektora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.
3. Z naruszenia obowiązków wynikających z niniejszego dokumentu lub z postępowania sprzecznego mogą zostać wyciągnięte konsekwencje dyscyplinarne w postaci pisemnego upomnienia, nagany lub kary finansowej. Do wyciągania konsekwencji prawo ma administrator oraz inspektor ochrony danych.

DYREKTOR
mgr Robert Czub

Inspektor Ochrony Danych

Administrator Danych Osobowych