Załącznik do Zarządzenia 7/2026

REGULAMIN BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH W MUZEUM CYPRIANA NORWIDA W DĘBINKACH

I. Wprowadzenie

1. Niniejszy regulamin określa zasady ochrony danych osobowych w Muzeum Cypriana Norwida w Dębinkach, ul. Pałacowa 7, 07-230 Dębinki, NIP: 7622013536, REGON: 520272368
2. (dalej jako: „Administrator") i jest wprowadzany w związku z przepisami rozporządzenia PEiR (UE) nr 2016/679 z 27.04.2016 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 (Dz.Urz. UE L z 2016 r, 119, s. 1 ze zm.) – dalej RODO.
3. W Regulaminie pod określeniem "pracownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych wymagające dostępu do zasobów sprzętowych i informacyjnych organizacji.

II. Zasady przetwarzania danych osobowych

1. Każdy pracownik Administratora przetwarza dane osobowe wyłącznie w związku z wykonywaniem swoich zadań służbowych. Pracownicy są zobowiązani do zachowania poufności danych osobowych i ich zabezpieczeń. Udostępnianie danych osobom trzecim jest zabronione.
2. W przypadku uzyskania przez pracownika dostępu do danych osobowych (papierowych lub elektronicznych) przekraczających zakres upoważnienia tego pracownika, udostępnione w ten sposób informacje należy zachować w poufności. Należy również poinformować pracownika odpowiedzialnego za udostępnione dokumenty o zaistniałej sytuacji, a także zawiadomić Inspektora Ochrony Danych o incydencie.
3. Pracownik jest obowiązany logować się do systemu za pomocą własnego loginu oraz hasła dostępu. Udzielanie informacji na temat loginu i hasła innym osobom jest zabronione.
4. Pracownik ma prawo korzystać z Internetu wyłącznie w celu wykonywania obowiązków służbowych, zabronione jest korzystanie z prywatnej poczty służbowej, prywatnych profili na social mediach, wykorzystywanie komercyjnych komunikatorów typu WhatsApp oraz korzystanie z ogólnie dostępnej wersji Chata GPT przy realizacji obowiązków służbowych.
5. Pracownicy zobowiązani są do przechowywania na biurku tylko tych dokumentów, które są im niezbędne w danym momencie do wykonania bieżących zadań.
6. Opuszczając czasowo stanowisko pracy pracownik ma obowiązek zablokować komputer poprzez wylogowanie się z programu oraz dokonać blokady systemu operacyjnego, za pomocą skrótu klawiszowego [Windows + L] lub [Cmd + Ctrl + Q] – w zależności od systemu operacyjnego komputera.
7. Kończąc pracę pracownik pozostaje przy stanowisku komputerowym do czasu całkowitego wyłączenia się komputera.

8. Po zakończonej pracy pracownik jest zobowiązany do wylogowania się z systemu. Na biurku może pozostać jedynie telefon oraz materiały biurowe, takie jak np. długopis i zszywacz – zasada czystego biurka.
9. Po pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy/szafki. Klucze do szaf należy umieścić w wyznaczonym do tego celu umówionym, bezpiecznym miejscu.
10. Obowiązuje zakaz trzymania na biurku wszelkich produktów spożywczych, których posiadanie grozi rozlaniem płynu.
11. Zabronione jest korzystanie z prywatnych nośników informacji (np. dysk zewnętrzny, pendrive).
12. Korzystając ze służbowych nośników pamięci (np. pendrive) bezwzględnie wymagane jest ich zaszyfrowania odpowiednim hasłem dostępu.
13. Bez potrzeby nie należy tworzyć plików komputerowych zawierających dane osobowe. Pliki z danymi po ustaniu przydatności należy trwale usunąć.
14. Wszelkie dokumenty zawierające dane osobowe należy niszczyć za pomocą niszczarek dokumentów- zasada czystego kosza.
15. Pliki z dany osobowymi (Word, Excel, PDF, 7zip,) przed wysłaniem za pośrednictwem komunikacji elektronicznej powinny być zaszyfrowane, a hasło powinno być wysłane oddzielnym kanałem komunikacji (np. sms)
16. Pracownicy zobowiązani są do tworzenia silnych haseł do plików, poczty i systemów zgodnie z polityką haseł przyjętą u Administratora.
17. Zabronione jest otwieranie załączników i klikanie w linki pochodzące od nieznanych nadawców bądź podejrzane, sugerujące próbę phishingową. Podejrzane e-maile należy zgłaszać niezwłocznie wyznaczonemu Inspektorowi Ochrony Danych.
18. Wysyłając e-mail do wielu odbiorców spoza organizacji, pamiętamy o użyciu funkcji UDW.
19. Każdy pracownik jest odpowiedzialny za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe i nie pozostawianie wydruków z danymi osobowymi na drukarce – zasad czystego druku.
20. Zabronione jest samodzielne instalowanie i pobieranie programów przez Pracowników.
21. Pracownicy zobowiązani są do przenoszenia dokumentów i sprzętu służbowego w sposób zapobiegający ich kradzieży, zagubieniu lub utracie, odpowiadając za ich zabezpieczenie.
22. Pracownicy są obowiązani do przekazywania Administratorowi nośników z danymi przeznaczonych do zniszczenia.
23. Pracownicy zobowiązani są do ustawienia wygaszaczy ekranu, uruchamiających blokadę systemu po 5 minutach bezczynności.
    Pracownicy zobowiązani są prowadzić swoją aktywności w prywatnych mediach społecznościowych przy zachowaniu dbałości o dobre imię pracodawcy, jego wizerunek czy ochronę tajemnicy przedsiębiorstwa w ramach przysługujących im praw i obowiązków pracowniczych, nie naruszając przepisów art. 212 §1 i § 2 KK.
24. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych.
    W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym

profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

ZGŁASZANIE INCYDENTÓW W ZAKRESIE DANYCH OSOBOWYCH

Pracownik zobowiązany jest do NIEZWŁOCZNEGO powiadomienia Inspektora Ochrony Danych – e-mail: iod@odokancelaria.pl, tel. 577-940-399 w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, np. ślady na drzwiach, oknach i szafach wskazują na próbę włamania; niszczenie dokumentacji bez użycia niszczarki; wysyłka maila z niezaszyfrowanym załącznikiem zawierającym dane osobowe, wysyłka maila na zewnątrz organizacji bez stosowania kopi UDW, omyłkowa wysyłka maila na inny adres, wynoszenie danych osobowych w wersji papierowej i elektronicznej poza siedzibę Administratora bez zgody przełożonego; otrzymanie maili zachęcających do ujawnienia identyfikatora i/lub hasła, udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej, korzystanie z niezaszyfrowanych dysków czy pendriv-ów.

DYREKTOR MUZEUM

Jacenty Matysiak