ZARZĄDZENIE NR 51.2021
BURMISTRZA OLESNA

z dnia 24 czerwca 2021 r.

w sprawie wprowadzenia Instrukcji zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713 z późn. zm.) w związku z art. 24 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) zarządza się, co następuje:

§ 1. Wprowadza się do stosowania „Instrukcję zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie", stanowiącą załącznik do zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Oleśnie do zapoznania się z treścią instrukcji, o której mowa w § 1, oraz właściwego wykonywania jej postanowień.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr inż. Sylwester Lewicki

INSPEKTOR OCHRONY DANYCH
dr Krzysztof Latocha
24-06-2021

GŁÓWNY SPECJALISTA
ds. administrowania siecią komputerową
mgr inż. Hubert Piątek

Waldemar Leśniewski
RADCA PRAWNY
nr upraw. OP-855/2008

Załącznik do zarządzenia nr 51.2021 Burmistrza Olesna
z dnia 24 czerwca 2021 r.

Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie

§ 1. 1. Instrukcja określa sposób zarządzania i funkcjonowania systemu teleinformatycznego, wykorzystywanego do przetwarzania danych osobowych w Urzędzie Miejskim w Oleśnie, zwanego dalej „systemem teleinformatycznym", w celu zabezpieczenia danych osobowych przed zagrożeniami, w szczególności przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Przepisów instrukcji nie stosuje się w przypadku, gdy system teleinformatyczny posiada odrębną dokumentację obowiązującą na podstawie odrębnych przepisów.

§ 2. 1. Dostęp do systemu teleinformatycznego może uzyskać wyłącznie osoba upoważniona przez administratora danych osobowych do przetwarzania danych osobowych i zarejestrowana w tym systemie przez administratora systemu jako użytkownik.

2. Rejestracja użytkownika, następuje na wniosek administratora danych osobowych i polega na przyporządkowaniu mu: identyfikatora, przydzieleniu hasła i nadaniu określonych we wniosku uprawnień oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§ 3. 1. Wyrejestrowania użytkownika z systemu teleinformatycznego dokonuje administrator systemu na wniosek administratora danych osobowych lub inspektora ochrony danych.

2. Wyrejestrowanie może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje przez:

1) zablokowanie konta użytkownika lub odebranie uprawnień do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);

2) usunięcie danych użytkownika z bazy użytkowników systemu lub odebranie uprawnień (wyrejestrowanie trwałe).

§ 4. Czasowe wyrejestrowanie użytkownika z systemu teleinformatycznego może nastąpić w razie: nieobecności dłuższej niż 30 dni kalendarzowych, zawieszenia w czynnościach służbowych lub wszczęcia postępowania dyscyplinarnego.

§ 5. Rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego użytkownik wykonywał swoje obowiązki oraz odebranie uprawnień stanowi podstawę do trwałego wyrejestrowania użytkownika z systemu teleinformatycznego.

§ 6. 1. Użytkownicy są uprawnieni do logowania się do systemu teleinformatycznego tylko na własne konto założone przez administratora systemu.

2. Dostęp jest indywidualnie zdefiniowany dla każdego użytkownika. Użytkownik ma dostęp jedynie do zasobów, które są mu niezbędne do wykonywania obowiązków służbowych.

3. Tożsamość użytkownika systemu jest jednoznacznie określona i sprawdzona przed rozpoczęciem pracy w systemie (uwierzytelnienie).

4. Uwierzytelnienie w systemie teleinformatycznym odbywa się z wykorzystaniem indywidualnych haseł oraz wymaga od użytkowników w szczególności:

1) nieujawniania haseł do kont w systemie teleinformatycznym;

2) natychmiastowej zmiany hasła w przypadku podejrzenia jego ujawnienia, o ile istnieje taka możliwość techniczna.

§ 7. 1. Aktualne hasła do kont administratora systemu przechowuje administrator systemu w zbiorze haseł awaryjnych.

2. Hasła, o których mowa w ust. 1, są przechowywane odrębnie dla każdego systemu i zabezpieczone przed dostępem osób nieuprawnionych.

3. Administrator systemu dokumentuje każdy dostęp i użycie hasła ze zbioru, o którym mowa w ust. 1.

§ 8. 1. Użytkownik jest odpowiedzialny za użycie zasobów teleinformatycznych przy wykorzystaniu jego identyfikatora i hasła, z zastrzeżeniem ust. 6.

2. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

3. Pierwsze hasło wymagane do uwierzytelnienia się w systemie teleinformatycznym przydzielane jest przez administratora systemu po pouczeniu osoby upoważnionej o obowiązku zachowania haseł w tajemnicy oraz po potwierdzeniu odbioru pierwszego hasła.

4. System teleinformatyczny automatycznie wymusza zmianę hasła przy pierwszym logowaniu oraz co 30 dni.

5. Inspektor ochrony danych może, w uzasadnionych przypadkach, polecić użytkownikowi dokonanie zmiany hasła.

6. Administrator systemu jest uprawniony do dokonania zmiany hasła dostępu do konta na wniosek użytkownika lub jego przełożonego.

7. Zablokowanie konta użytkownika w systemie, o ile istnieje taka możliwość techniczna, następuje po trzech nieudanych próbach wprowadzenia hasła.

§ 9. 1. Rozpoczęcie pracy na stacji roboczej w systemie teleinformatycznym następuje po wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora (logowanie).

2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w obecności użytkownika lub innej osoby upoważnionej do przebywania w tym pomieszczeniu.

§ 10. 1. Na stacjach roboczych w systemie teleinformatycznym należy stosować wygaszacze ekranu.

2. W przypadku czasowego opuszczenia stanowiska pracy użytkownik jest obowiązany zablokować stację roboczą.

3. Zakończenie pracy na stacji roboczej następuje po prawidłowym wylogowaniu się użytkownika.

§ 11. 1. Użytkownik powiadamia administratora systemu o braku możliwości zalogowania się na konto przez użytkownika lub stwierdzenia innych nieprawidłowości w pracy systemu.

2. W przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane w tym celu narzędzia programowe lub sprzętowe, użytkownik niezwłocznie powiadamia o tym fakcie administratora systemu oraz administratora danych osobowych i inspektora danych osobowych.

§ 12. 1. Użytkownicy nie są upoważnieni do kopiowania całych zbiorów danych osobowych.

2. Całe zbiory danych mogą być kopiowane tylko przez administratora systemu, administratora danych osobowych lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.

3. Jednostkowe dane osobowe mogą być kopiowane na nośniki pod warunkiem, że po ustaniu przydatności tych kopii należy trwale skasować dane lub fizycznie zniszczyć nośniki, na których są przechowywane.

§ 13. 1. Tworzenie kopii zapasowych zbiorów danych jest obligatoryjne.

2. Częstotliwość tworzenia kopii zapasowych musi uwzględniać charakter zbioru, częstotliwość jego modyfikacji oraz zmiany liczby danych oraz zasady jego funkcjonowania.

§ 14. Nośniki zawierające kopie zapasowe należy oznaczać jako „kopia zapasowa" wraz z podaniem daty sporządzenia i nazwy systemu teleinformatycznego, o ile istnieje taka możliwość.

§ 15. Szczegółowe procedury tworzenia i niszczenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania oraz zasady przechowywania i udostępniania tych kopii określa się odrębnie.

§ 16. 1. Elektroniczne nośniki informacji zawierające dane osobowe przechowuje się w sposób zapewniający ochronę przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

2. Dopuszcza się przechowywanie nośników, o których mowa w ust. 1, w zamykanych na klucz meblach biurowych, z wyłączeniem przypadków, gdy odrębne przepisy nakładają wyższe rygory bezpieczeństwa ich przechowywania.

3. Nośniki, o których mowa w ust. 1, podlegają obligatoryjnemu ewidencjonowaniu.

§ 17. Nośniki, o których mowa w § 16 ust. 1, nie mogą być pozostawiane bez nadzoru poza obszarem przetwarzania danych osobowych.

§ 18. Podstawowe zasady bezpieczeństwa przetwarzania danych osobowych, o których mowa w polityce bezpieczeństwa informacji stosuje się również do danych osobowych zgromadzonych na nośnikach, o których mowa w § 16 ust. 1.

§ 19. 1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, uszkodzone lub nienadające się do dalszej eksploatacji niszczy się w sposób uniemożliwiający ich odczytanie.

2. Naprawa urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe, jest przeprowadzana wyłącznie na obszarze przetwarzania danych osobowych.

3. Naprawa urządzeń przetwarzających dane osobowe może zostać przeprowadzona poza siedzibą administratora danych osobowych po wymontowaniu z nich i pozostawieniu w jego siedzibie dysków lub innych elektronicznych nośników informacji.

§ 20. Administrator systemu jest obowiązany do:

1) zainstalowania i aktualizowania oprogramowania antywirusowego oraz określenia częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie;

2) usuwania wszelkich nieprawidłowości w pracy systemu;

3) zapewnienia ciągłości pracy systemu i nadzoru nad jego prawidłowym funkcjonowaniem;

4) przeglądu i konserwacji systemu.

§ 21. Sposób zabezpieczenia systemu teleinformatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu oraz procedury wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych osobowych określa się odrębnie.

§ 22. 1. System teleinformatyczny posiadający połączenie z Internetem chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. Administrator systemu określa sposób zabezpieczenia systemu teleinformatycznego posiadającego połączenie z Internetem.

§ 23. Rodzaj, zakres i czas przechowywania informacji o zdarzeniach w systemie teleinformatycznym, gromadzonych dla potrzeb kontroli, określa się odrębnie.

§ 24. Do podstawowych zasad bezpiecznej eksploatacji systemów przeznaczonych do przetwarzania danych osobowych należy:

1) zakaz podłączania do gniazd dedykowanej sieci elektrycznej przeznaczonych dla sprzętu komputerowego innych urządzeń;

2) obowiązek dbania o prawidłową eksploatację sprzętu i oprogramowania zgodnie z instrukcjami, wytycznymi administratora systemu i inspektora ochrony danych oraz zaleceniami producenta.