*Załącznik **nr 4***
do UCHWAŁY NR 6/2/2022 ZARZĄDU Związku Gmin
i Powiatów Kanału Elbląskiego i Pojezierza Iławskiego
z 17 października 2022 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator: **ZWIĄZEK GMIN I POWIATÓW KANAŁU ELBLĄSKIEGO I POJEZIERZA IŁAWSKIEGO z siedzibą w OSTRÓDZIE**

Adres: **ul. Adama Mickiewicza 24, 14-100 Ostróda**

Kontakt: **tel. (89) 642 94 00, e-mail: zwiazek@um.ostroda.pl**

ROZDZIAŁ I. POSTANOWIENIA OGÓLNE

§ 1. Celem *Instrukcji Zarządzania Systemem Informatycznym* Związku Gmin i Powiatów Kanału Elbląskiego i Pojezierza Iławskiego, zwanej dalej „Instrukcją" jest zapewnienie bezpieczeństwa przetwarzanych danych osobowych poprzez stosowanie zasad i trybu postępowania przy przetwarzaniu danych osobowych w systemie informatycznym zgodnych z przepisami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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.U. UE L 119 z 4.5.2016)*, zwanego ogólnym rozporządzeniem o ochronie danych osobowych (RODO) oraz *ustawy z 10 maja 2018 roku o ochronie danych osobowych* (t.j. Dz.U. z 2019 r. poz. 1781). Niniejsza Instrukcja zarządzania systemem informatycznym zawiera:

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

2. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego, w którym są przetwarzane dane osobowe.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

6. Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych.

7. Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

9. Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych.

ROZDZIAŁ II. UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

§ 2.1. Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych.

2. Upoważnienie nadaje i odwołuje Administrator Danych Osobowych.

3. Upoważnienie i jego odwołanie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie, drugi – dla Administratora Danych Osobowych.

4. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik **nr 6** do Polityki ochrony danych osobowych.

5. Upoważnienia nie sporządza się dla Administratora Danych Osobowych. Upoważnienia nadane przed dniem wprowadzenia Instrukcji pozostają w mocy.

6. Upoważnienia do przetwarzania danych osobowych wpisywane są do Ewidencji osób upoważnionych do przetwarzania danych osobowych. Wzór Ewidencji stanowi załącznik **nr 9** do Polityki ochrony danych osobowych. Ewidencję prowadzi Administrator Danych Osobowych.

ROZDZIAŁ III. ZARZĄDZANIE I UŻYTKOWANIE SYSTEMU INFORMATYCZNEGO

§ 3.1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem. Obowiązują następujące zasady tworzenia hasła:

1) hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów;
2) hasło musi składać się z co najmniej 6 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
3) hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury;
4) hasło nie może być jednakowe z identyfikatorem użytkownika;
5) hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

2. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.

3. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.

4. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora danych osobowych.

5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

ROZDZIAŁ IV. PROCEDURY ROZPOCZĘCIA, ZAWIESZANIA I ZAKOŃCZENIA PRACY

§ 4.1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić administratora danych osobowych.

2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania

jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

3. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

4. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyty CD, pendrive i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuje poprzez wylogowanie się z tego systemu.

ROZDZIAŁ V. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

§ 5.1. Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik systemu informatycznego służącego do przetwarzania danych osobowych.

2. Kopie awaryjne może tworzyć jedynie administrator danych.

3. Kopie zapasowe powinny być kontrolowane przez administratora danych osobowych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

4. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

5. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

ROZDZIAŁ VI. PRZECHOWYWANIE ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

§ 6.1. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w „Polityce ochrony danych osobowych”.

3. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce ochrony danych osobowych”, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

4. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

ROZDZIAŁ VII. ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

§ 7.1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.

2. Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.

3. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowane oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

ROZDZIAŁ VIII. UDOSTĘPNIANIE DANYCH OSOBOWYCH

§ 8.1. W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.

2. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, administrator danych odnotowuje je w rejestrze odbiorców danych osobowych.

3. W rejestrze odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Wzór rejestru stanowi załącznik **nr 11** do Polityki Ochrony Danych Osobowych.

ROZDZIAŁ IX. PRZEGLĄDY I KONSERWACJA SYSTEMÓW I NOŚNIKÓW INFORMACJI

§ 9.1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w „Polityce ochrony danych osobowych" przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

2. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych osobowych.

3. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

4. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni administrator danych. Administrator Danych Osobowych prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji.

5. Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika.

ROZDZIAŁ IX. POSTANOWIENIA KOŃCOWE

§ 10.1. Administrator danych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.

2. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.

Ostróda, 17 października 2022 roku