ZARZĄDZENIE NR 21/2023
BURMISTRZA MIASTA SEJNY

z dnia 20 lutego 2023 r.

w sprawie wprowadzenia instrukcji bezpiecznego przesyłania danych osobowych za pomocą poczty elektronicznej w Urzędzie Miasta Sejny

Na podstawie art. 33 ust.1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2023 r., poz. 40 z późń. zm.) w związku z art. 32 Rozporządzenia 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 - Dz. U. UE L 2016.119.1) zarządzam, co następuje:

§ 1. Wprowadza się instrukcję bezpiecznego przesyłania danych osobowych za pomocą poczty elektronicznej w Urzędzie Miasta Sejny, stanowiącą Załącznik do niniejszego zarządzenia.

§ 2. Nadzór nad wprowadzeniem instrukcji powierza się Sekretarzowi Miasta i Inspektorowi Ochrony Danych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta Sejny

Arkadiusz Adam Nowalski

Załącznik do zarządzenia Nr 21/2023

Burmistrza Miasta Sejny

z dnia 20 lutego 2023 r.

Instrukcja bezpiecznego przesyłania danych osobowych za pomocą poczty elektronicznej w Urzędzie Miasta Sejny

1. W Urzędzie Miasta Sejny przetwarza się na dużą skalę dane osobowe, w tym dane szczególnych kategorii. Jedną z czynności przetwarzania danych osobowych jest ich przesyłanie za pomocą poczty elektronicznej. Najczęściej występującym naruszeniem ochrony danych osobowych przy korzystaniu z poczty elektronicznej jest wysłanie wiadomości na niewłaściwy adres e-mail. Skutkiem naruszenia może być ujawnienie danych osobowych, w tym danych szczególnych kategorii, nieuprawnionym odbiorcom. Takie naruszenie w większości wypadków wymaga zgłoszenia do Urzędu Ochrony Danych Osobowych, który może uruchomić procedury sprawdzające z kontrolą włącznie. Również osoby, których dane ujawniono, mogą wystąpić na drogę prawną przeciwko administratorowi danych. W celu uniknięcia tego rodzaju naruszeń lub znacznego ograniczenia ich skutków wprowadza się niniejszą instrukcję.

2. Należy zachować dużą ostrożność przy wpisywaniu adresu e-mail i upewnić się, że adres jest poprawny. Szczególnej ostrożności wymaga korzystanie z automatycznych podpowiedzi, które pojawiają się po wpisaniu początkowych liter adresu e-mail w polu „Do" programu poczty elektronicznej. Korzystanie z tej możliwości, zwłaszcza w pośpiechu, zwiększa ryzyko wysłania wiadomości na niewłaściwy adres e-mail.

3. Najprostszym sposobem zapewnienia bezpieczeństwa danych osobowych w wiadomościach e-mail jest przesyłanie ich w postaci zaszyfrowanych załączników w programach MS Office i 7-Zip. Szyfrowanie zapewnia poufność przesyłanych informacji, dlatego zaleca się szyfrowanie załączników wiadomości mailowych przed ich wysłaniem. Należy unikać umieszczania danych osobowych w treści samej wiadomości, która nie będzie szyfrowana.

4. Szyfrowanie w programie Word: W menu na górze ekranu z lewej strony otworzyć: *1.* ***Plik*** > *2.* ***Informacje*** > *3.* ***Chroń dokument*** > *4.* ***Szyfruj przy użyciu hasła.***

5. Szyfrowanie w programie Excel: W menu na górze ekranu z lewej strony otworzyć: *1.* ***Plik*** > *2.* ***Informacje*** > *3.* ***Chroń skoroszyt*** > *4.* ***Szyfruj przy użyciu hasła.***

6. Szyfrowanie w programie 7-Zip. Jest to darmowy program do kompresji plików wyposażony w opcję zabezpieczania archiwum hasłem. Można nim szyfrować np. pliki PDF. Program można pobrać ze strony https://www.7-zip.org lub https://www.7-zip.org.pl

7. Po zainstalowaniu programu 7-Zip, możemy szyfrować pliki za jego pomocą w następujący sposób:

a) w odpowiednim katalogu wybieramy plik, który chcemy zaszyfrować,

b) klikamy na nim prawym przyciskiem myszy,

c) w rozwiniętym menu wybieramy opcję **7-Zip > Dodaj do archiwum,**

d) w menu **Dodaj do archiwum** pojawi się możliwość dodania hasła,

e) po wprowadzeniu hasła, jego powtórzeniu i zatwierdzeniu OK otrzymamy spakowany plik, zabezpieczony hasłem przed odczytaniem. Nazwa pliku nie może zawierać chronionych danych, ponieważ nazwy plików są widoczne, mimo zabezpieczenia hasłem ich treści.

f) zaszyfrowany plik pojawi się w tym samym katalogu, co plik wybrany do zaszyfrowania,

g) zaszyfrowany plik można bezpiecznie przesłać pocztą elektroniczną jako załącznik.

8. Hasło zabezpieczające zaszyfrowany plik powinno składać się z co najmniej 10 znaków, z wykorzystaniem małych i wielkich liter oraz cyfr lub znaków specjalnych.

9. Hasło, umożliwiające odczytanie zaszyfrowanych danych, należy przesłać adresatowi wiadomości e-mail bezpiecznym kanałem komunikacji, innym niż poczta elektroniczna, np. za pomocą wiadomości SMS lub telefonicznie. Nie wolno wysyłać hasła na adres, na który wysłano zaszyfrowaną wiadomość. Zaszyfrowana wiadomość i hasło trafiłyby do niewłaściwego odbiorcy, gdyby adres okazał się błędny.

10. W razie pytań lub trudności w procesie szyfrowania wiadomości należy zwrócić się do informatyka lub Inspektora Ochrony Danych.

11. Zanonimizowane kopie dokumentów, z których usunięto dane osobowe, można przesyłać pocztą elektroniczną bez konieczności ich szyfrowania.