

**Zarządzenie Nr 78/IX/2025**  
**Burmistrza Miasta Milanówka**  
**z dnia 7 kwietnia 2025 roku**

**w sprawie wprowadzenia w Urzędzie Miasta Milanówka wewnętrznej procedury dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych**

Na podstawie art. 24 ust. 1 ustawy z dnia 14 czerwca 2024 roku o ochronie sygnalistów (Dz.U. poz. 928) zarządza się, co następuje:

§1.

Wprowadza się w Urzędzie Miasta Milanówka wewnętrzną procedurę dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych, zwaną dalej procedurą, w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§2.

Nadzór nad wdrożeniem i stosowaniem zapisów procedury powierza się Sekretarzowi Miasta.

§3.

Zarządzenie wchodzi w życie z dniem podpisania i obowiązuje po upływie 7 dni od podania go do wiadomości pracowników Urzędu Miasta Milanówka.

§4.

Z dniem wejścia w życie niniejszego zarządzenia traci moc zarządzenie nr 102/IX/2024 z dnia 25 września 2024 roku w sprawie wprowadzenia w Urzędzie Miasta Milanówka wewnętrznej procedury dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych.

Burmistrz Miasta Milanówka

/-/

Artur Niedziński

Przygotowała: Katarzyna Stelmach

## **Procedura dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych w Urzędzie Miasta Milanówka**

### **I. Zakres przedmiotowy i podmiotowy Procedury**

1. Procedura dokonywania zgłoszeń naruszeń prawa i podejmowania działań następczych, zwana dalej *Procedurą*, reguluje zasady zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych. *Procedura* stanowi realizację przepisu art. 24 ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. poz. 928), zwanej dalej *Ustawą*, która wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305 z 26.11.2019, str. 17, Dz. Urz. UE L 347 z 20.10.2020, str. 1, Dz. Urz. UE L 265 z 12.10.2022, str. 1 oraz Dz. Urz. UE L 150 z 09.06.2023, str. 40)
2. Zakresem podmiotowym *Procedury* objęci są sygnaliści, czyli osoby fizyczne, zgłaszające lub ujawniające publicznie informację o naruszeniu prawa pozyskaną w kontekście związanym z pracą, świadczeniem usług lub pełnieniem funkcji na rzecz Urzędu na innej podstawie - o których mowa w art. 4 Ustawy.
3. Na podstawie niniejszej *Procedury oraz przepisów Ustawy* następuje zgłaszanie naruszeń prawa, czyli działań lub zaniechań niezgodnych z prawem lub mających na celu obejście prawa, dotyczących obszarów, o których mowa w art. 3 ust. 1 Ustawy.

### **II. Podstawowe pojęcia**

Ilekroć w niniejszej procedurze jest mowa o:

- 1) Administratorze – należy przez to rozumieć administratora danych osobowych w rozumieniu art. 4 pkt 7) RODO, tj. Urząd Miasta Milanówka;
- 2) Burmistrzu – należy przez to rozumieć Burmistrza Miasta Milanówka;
- 3) pracownikach – należy przez to rozumieć osoby zatrudnione w Urzędzie Miasta Milanówka oraz jednostkach organizacyjnych objętych niniejszą Procedurą, bez względu na podstawę nawiązania stosunku pracy, a także osoby świadczące pracę lub stałe usługi na rzecz Urzędu na innej podstawie prawnej;
- 4) rejestrze – należy przez to rozumieć rejestr zgłoszeń wewnętrznych, o którym mowa w art. 29 Ustawy;
- 5) RODO – należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. Nr 119, s. 1 ze zm.).

- 6) Urządzenie – należy przez to rozumieć Urząd Miasta Milanówka, a także jednostki organizacyjne objęte niniejszą procedurą.

### **III. Sposób dokonywania zgłoszeń**

1. Zgłoszenia naruszenia można dokonywać w formie pisemnej poprzez dedykowany poufny kanał zgłoszeń za pomocą poczty elektronicznej na adres: [sygnalistawewnetrzny@umm.milanowek.pl](mailto:sygnalistawewnetrzny@umm.milanowek.pl) w zaszyfrowanej wiadomości przesłanej zgodnie z instrukcją stanowiącą **załącznik nr 1**.
2. Zgłoszenie w szczególności powinno zawierać:
  - 1) dane osobowe zgłaszającego pozwalające na ustalenie jego tożsamości, tj.: imię/imiona, nazwisko, stanowisko, miejsce pracy;
  - 2) dane kontaktowe do celów informowania sygnalisty o etapach procedowania zgłoszenia i ewentualnych wyjaśnień lub uzupełnień;
  - 3) datę dokonania zgłoszenia i pozyskania informacji o naruszeniu;
  - 4) dane osobowe osoby lub osób, której zgłoszenie dotyczy, osób mających związek z naruszeniem i świadków;
  - 5) charakterystykę i możliwie szczegółowy opis naruszenia;
  - 6) określenie przepisów właściwych regulacji wewnętrznych, przepisów prawa lub standardów, do których odnosi się zgłoszenie;
  - 7) opis okoliczności, w których zgłaszający dowiedział się o naruszeniu;
  - 8) inne okoliczności mających znaczenie dla sprawy.
3. Zgłoszenia dokonane anonimowo nie są rozpatrywane w trybie przewidzianym niniejszą procedurą.

### **IV. Osoby wyznaczone do przyjmowania zgłoszeń**

1. Do przyjmowania zgłoszeń wyznacza się następujące osoby:
  - 1) Sekretarz Miasta
  - 2) Kierownik Referatu Kancelaryjno Organizacyjnego
2. Kierownik Referatu Kancelaryjno Organizacyjnego niezwłocznie informuje Sekretarza Miasta o otrzymanych zgłoszeniach celem podjęcia działań następczych oraz innych działań wynikających z Procedury oraz przepisów Ustawy.
3. Dostęp do zgłoszeń będą posiadać wyłącznie osoby uprawnione, w zakresie niezbędnym do wykonania powierzonych zadań.
4. Administrator upoważnia osoby wyznaczone do przyjmowania zgłoszeń, zgodnie z obowiązującymi wewnętrznymi regulacjami z zakresu polityki bezpieczeństwa i ochrony danych osobowych. Nadane upoważnienia określają szczegółowy zakres czynności, do wykonywania których będzie upoważniona wyznaczona osoba.
5. Osoby, o których mowa w ust. 1 zobowiązane są do:

- 1) przyjmowania i potwierdzania zgłoszeń; potwierdzenie zgłoszenia powinno nastąpić w terminie 7 dni od dnia jego otrzymania, chyba że sygnalista nie poda adresu do kontaktu, na który należy przekazać potwierdzenie;
  - 2) wstępnej oceny zgłoszenia;
  - 3) kontaktowania się z sygnalistą w przypadku wątpliwości co do właściwej oceny przedmiotu naruszenia, w celu uzupełniania przekazanych informacji;
  - 4) przekazania sygnaliście treści informacji o zasadach przetwarzania danych osobowych;
  - 5) odebrania zgody na ujawnienie tożsamości sygnalisty, jeżeli sygnalista wyrazi taką zgodę i przekazanie informacji o konsekwencjach ujawnienia tożsamości;
6. Sekretarz Miasta zobowiązany jest do:
- 1) przekazania sygnaliście informacji zwrotnej, w terminie nie dłuższym niż 3 miesiące od dnia potwierdzania przyjęcia zgłoszenia wewnętrznego, lub – w przypadku nieprzekazania potwierdzenia, w terminie 3 miesięcy od upływu 7 dni od dnia dokonania zgłoszenia wewnętrznego, chyba że sygnalista nie poda adresu do kontaktu, na który należy przekazać informację zwrotną;
  - 2) pozostawania w kontakcie z sygnalistą i informowania go o etapach procedowania zgłoszenia;
  - 3) podjęcia działań następczych oraz informowania sygnalisty o podjętych działaniach następczych;
  - 4) terminowego i rzetelnego prowadzenia rejestru zgłoszeń.

#### **V. Rejestr zgłoszeń wewnętrznych**

1. Urząd prowadzi rejestr zgłoszeń wewnętrznych. Wpisów w rejestrze dokonuje osoba wyznaczona, wskazana w pkt IV.6 pkt 1.
2. Wpisy w rejestrze dokonywane są w sposób zapewniający poszanowanie zasad ochrony danych osobowych. Osoba dokonująca wpisów zapewnia przechowywanie rejestru w sposób zabezpieczający go przed dostępem osób nieuprawnionym oraz zniszczeniem.
3. Rejestr może być prowadzony w formie elektronicznej.

#### **VI. Rozpatrywanie zgłoszenia**

1. Jeśli wymaga tego charakter sprawy, w celu rozpatrzenia zgłoszenia wewnętrznego, Burmistrz na wniosek Sekretarza Miasta może powołać komisję do zbadania okoliczności opisanych w zgłoszeniu i oceny merytorycznej treści zgłoszenia.
2. Burmistrz powołuje skład Komisji, kierując się wymogiem włączenia w skład Komisji osób bezstronnych. Członkiem komisji nie może być:
  - 1) sygnalista,
  - 2) osoba, której dotyczy zgłoszenie,
  - 3) osoba wskazana w treści zgłoszenia,

- 4) osoby związane powiązaniami personalnymi lub służbowymi z sygnalistą, osobą, której dotyczy zgłoszenie lub osobą wskazaną w treści zgłoszenia,
  - 5) osoba uczestnicząca w ocenie lub udostępnianiu informacji związanej ze zgłoszeniem,
  - 6) osoba, której udział w rozpatrywaniu zgłoszenia mógłby wywołać wątpliwości co do jej bezstronności.
3. Komisja uprawniona jest do:
- 1) dostępu do dokumentów i informacji niezbędnych do przeprowadzenia postępowania wyjaśniającego,
  - 2) uzyskiwania wyjaśnień, pisemnych i ustnych od kierowników jednostek i komórek organizacyjnych, pracowników i szeroko rozumianego personelu Urzędu;
  - 3) dostępu do pomieszczeń i infrastruktury technicznej, w tym telefonów, komputerów i nośników informacji w zakresie niezbędnym do wyjaśnienia zgłoszenia oraz przy poszanowaniu zasad ochrony danych osobowych i ochrony tajemnicy korespondencji,
  - 4) przeprowadzenia przeszukania i zabezpieczenia dowodów, w zakresie związanym z treścią zgłoszenia;
  - 5) kontaktowania się z sygnalistą w celu uzyskania informacji wyjaśniających.
4. Komisja włącza inspektora ochrony danych w rozpoznawanie zgłoszenia, w szczególności, w zakresie dotyczącym ochrony danych osobowych, dopuszczalności ich pozyskania lub udostępnienia.
5. Po przeprowadzeniu postępowania wyjaśniającego, Komisja sporządza raport, który przekazuje Burmistrzowi. Raport zawiera informacje dotyczące zgłoszenia oraz propozycje działań następczych, w tym: zamknięcie procedury (w wypadku niepotwierdzenia się zgłoszenia), przeprowadzenie zmian w procedurach wewnętrznych, złożenie wniosku o charakterze organizacyjnym, złożenie wniosku o wszczęcie postępowania dyscyplinarnego, złożenie wniosku o wszczęcie postępowania w sprawie naruszenia dyscypliny finansów publicznych, złożenie zawiadomień do właściwych organów, zgłoszenie naruszenia ochrony danych do Prezesa Urzędu Ochrony Danych Osobowych.
6. Decyzję o podjęciu stosownych działań następczych podejmuje Burmistrz.

## **VII. Ochrona danych osobowych**

1. Administratorem danych osobowych w rozumieniu art. 4 pkt 7) RODO, jest Urząd Miasta Milanówka w związku z przyjmowaniem i rozpatrywaniem zgłoszeń wewnętrznych. Dane osobowe przetwarzane są wyłącznie z polecenia Administratora.
2. Dane osobowe sygnalisty przetwarzane są na podstawie art. 6 ust. 1 lit. c) RODO w związku z przepisami Ustawy. Dane osobowe mogą być przetwarzane także na podstawie art. 9 ust. 2 lit. g) RODO, jeżeli sygnalista poda w zgłoszeniu dane osobowe

należące do szczególnych kategorii danych osobowych, , art. 6 ust. 1 lit. a RODO w przypadku wyrażenia zgody na ujawnienie danych w zakresie imienia i nazwiska oraz art. 6 ust. 1 lit. f RODO w przypadku ustalenia i dochodzenia roszczeń lub obrony przed roszczeniami.

3. Osoby wyznaczone do obsługi zgłoszeń pozyskują wyłącznie dane niezbędne. Dane osobowe niemające znaczenia dla zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania, są usuwane bez zbędnej zwłoki, nie dłużej niż do upływu 14 dni od momentu ustalenia, że nie mają znaczenia dla sprawy.
4. Administrator realizuje obowiązek informacyjny, o którym mowa w art. 13-14 RODO, wobec: sygnalisty, osoby, której dotyczy zgłoszenie, osoby wskazanej w zgłoszeniu.
5. Obowiązki informacyjne dla sygnalisty, osoby której dane są przetwarzane w ramach zgłoszenia oraz osoby, przeciwko której toczy się postępowanie znajdują się w Polityce Prywatności na stronie internetowej: [www.milanowek.pl/bip](http://www.milanowek.pl/bip).
6. Administrator realizuje prawa osób, których dane dotyczą, wskazane w art. 15-22 RODO, z ograniczeniami w zakresie prawa dostępu do danych osobowych, wskazanych w Ustawie o ochronie sygnalistów. Administrator pozyskuje zgodę sygnalisty na ujawnienie jego tożsamości, jeżeli taka jest inicjatywa i wola sygnalisty. Administrator realizuje obowiązek informacyjny wobec sygnalisty w przypadku pozyskania takiej zgody.
7. Jeżeli zgłoszenie sygnalisty nosi znamiona naruszenia ochrony danych, Administrator zapewnia realizację obowiązków wynikających z art. 33-34 RODO.
8. Administrator przetwarza dane osobowe zgodnie z zasadami ochrony danych wskazanymi w art. 5 RODO. Administrator zapewnia bezpieczeństwo danych osobowych, zabezpieczając je przed nieuprawnionym dostępem, ujawnieniem i zniszczeniem.

### **VIII. Postanowienia końcowe**

1. Procedura obowiązuje od dnia podpisania i wchodzi w życie po upływie 7 dni od podania jej do wiadomości pracowników.
2. Postanowienia Procedury dotyczą wszystkich pracowników oraz osób świadczących pracę lub usługi lub pełniące funkcję w Urzędzie na podstawie innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług.
3. Osobie ubiegającej się o pracę na podstawie stosunku pracy lub innego stosunku prawnego stanowiącego podstawę świadczenia pracy lub usług lub pełnienia funkcji Urząd przekazuje informację o Procedurze zgłoszeń wewnętrznych wraz z rozpoczęciem rekrutacji lub negocjacji poprzedzających zawarcie umowy.

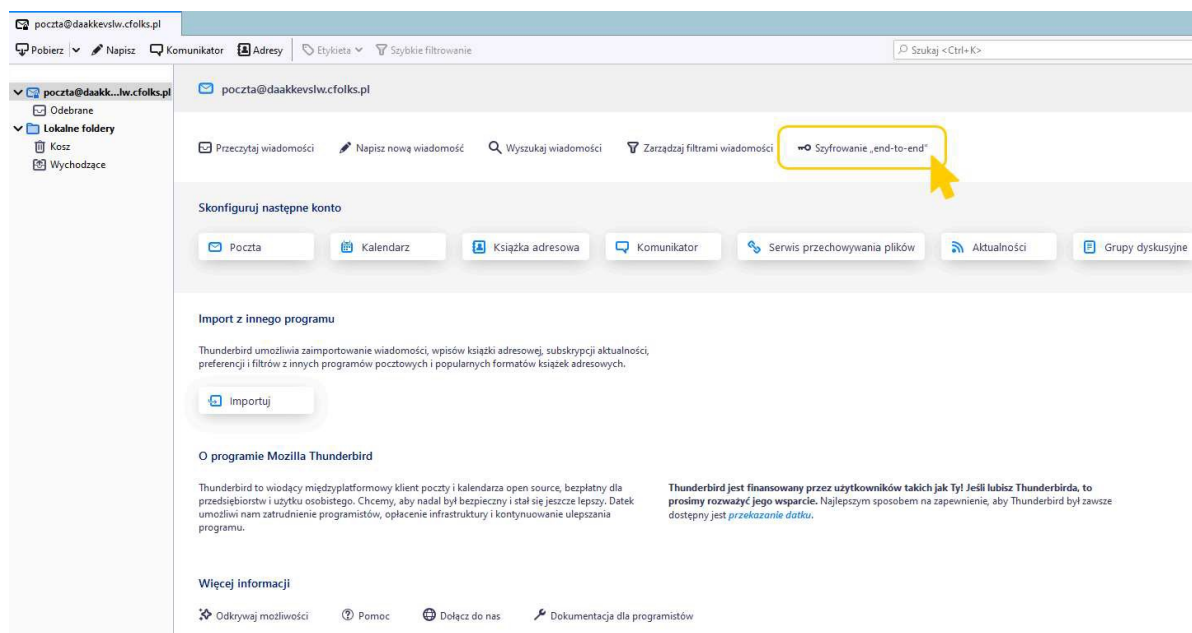
## Instrukcja przyjmowania zgłoszeń

### Mozilla Thunderbird – szyfrowanie wiadomości „end-to-end”

W tym artykule pokażemy Ci jak w prosty sposób szyfrować wiadomości mailowe korzystając z programu pocztowego Mozilla Thunderbird wersja(Thunderbird Setup 128.5.2esr) Najnowsze wydania Thunderbird’a posiadają już natywną obsługę OpenPGP, dzięki czemu nie musisz instalować żadnych dodatkowych aplikacji, czy też pluginów.

### Krok I – wygenerowanie klucza PGP

Otwórz program Mozilla Thunderbird i z głównej części aplikacji wybierz opcję „Szyfrowanie end-to-end”.



Następnie przy wybranym adresie mailowym dla którego chcesz mieć możliwość szyfrowania wiadomości skorzystaj z przycisku „Dodaj klucz”.

## Szyfrowanie „end-to-end”



Bez szyfrowania typu „end-to-end” treść wiadomości jest łatwo widoczna dla dostawcy poczty i inwigilacji rządowej.

Do wysyłania zaszyfrowanych lub cyfrowo podpisanych wiadomości wymagana jest konfiguracja technologii szyfrowania OpenPGP lub S/MIME.

Wybierz swój klucz osobisty, aby umożliwić korzystanie z OpenPGP, lub certyfikat osobisty, aby umożliwić korzystanie z S/MIME. Dla klucza lub certyfikatu osobistego posiadasz odpowiedni tajny klucz.

[Więcej informacji](#)


### OpenPGP

 Thunderbird odnalazł 1 klucz osobisty OpenPGP powiązany z tożsamością **myguelibez-warc@unimil.br** 

✓ Bieżąca konfiguracja wykorzystuje klucz o identyfikatorze **0x3E82CECA48F11D12**

[Więcej informacji](#)

**Żaden**  
Nie używaj OpenPGP dla tej tożsamości.

**0x3E82CECA48F11D12** 

Wygasa: 3.01.2027

Opublikowanie klucza publicznego na serwerze kluczy umożliwia innym jego wykrycie.


Użyj menedżera kluczy OpenPGP, aby przeglądać i zarządzać kluczami publicznymi swoich rozmówców oraz wszystkimi pozostałymi kluczami niewymienionymi tutaj.

### S/MIME

Certyfikat osobisty do podpisywania cyfrowego:

Certyfikat osobisty do szyfrowania:

W kolejnym oknie pozostaw zaznaczoną opcję „Utwórz nowy klucz OpenPGP” i zatwierdź wybór przyciskiem „Kontynuuj”.

 **Jeśli masz już klucz osobisty** dla tego adresu e-mail, zaimportuj go. W przeciwnym razie nie będziesz mieć dostępu do swoich archiwów zaszyfrowanych wiadomości, ani nie będziesz w stanie odczytać przychodzących zaszyfrowanych wiadomości e-mail od osób, które nadal używają Twojego istniejącego klucza. [Więcej informacji](#)

- Utwórz nowy klucz OpenPGP**
- Importuj istniejący klucz OpenPGP**



Zdefiniuj ustawienia generowanego klucza- okres ważności typ oraz wielkość. Zalecane przez nas ustawienia:

Data ważności: do 2 lat

Typ klucza: RSA

Wielkość: 4096

## Wygeneruj klucz OpenPGP

Tożsamość `Sygnalista <zenestrng> <sygnalista.zenstrng@ummmilan.wask.pl> - sygnalista.zenstrng`

### Ważność klucza

Określ czas wygaśnięcia nowo utworzonego klucza. Możesz później zmienić datę, aby w razie potrzeby przedłużyć ten czas.

Klucz wygasa za    

Klucz nie wygasa

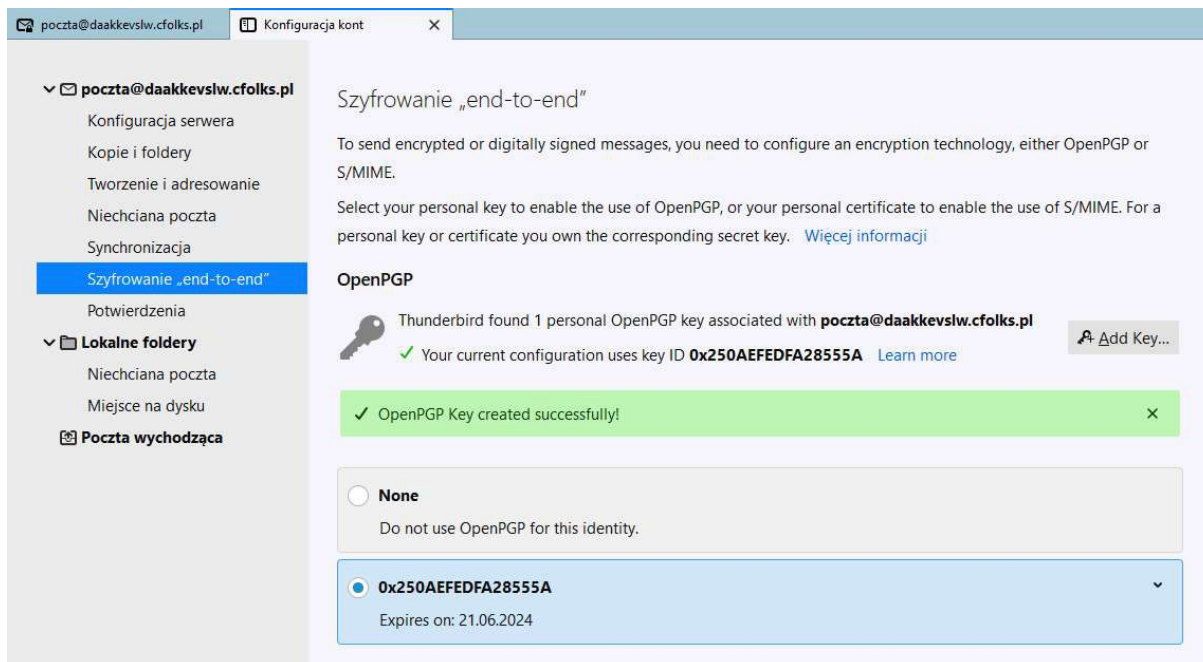
### Ustawienia zaawansowane

Zaawansowane ustawienia klucza OpenPGP.

Typ klucza:

Rozmiar klucza:

Po zdefiniowaniu ustawień w kolejnym oknie zatwierdź chęć wygenerowania klucza. Uwaga! Proces ten może potrwać nawet kilka minut- w tym czasie nie zamykaj programu pocztowego i nie wyłączaj komputera.

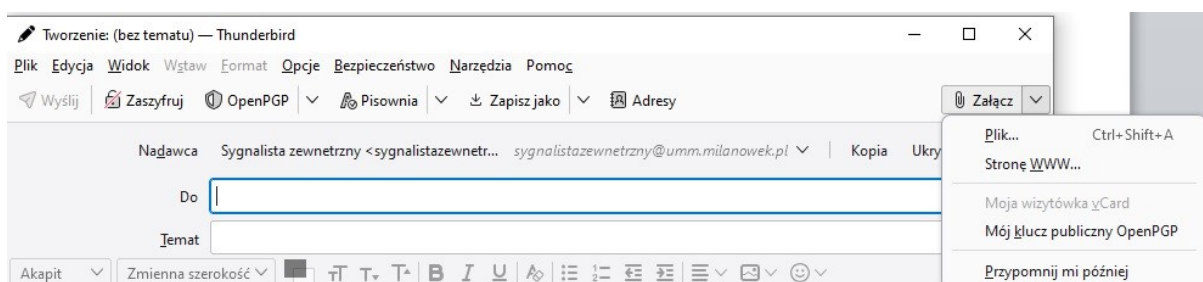


Brawo! Twój klucz jest już gotowy. W dalszej części poradnika dowiesz się, jak wymieniać się kluczami oraz szyfrować wiadomości.

## Krok II – wysyłka i import publicznych kluczy PGP

Szyfrowanie i odczyt zaszyfrowanych wiadomości możliwy jest wyłącznie po uprzedniej wymianie publicznych kluczy PGP przez nadawcę i odbiorcę.

Celem przesłania odbiorcy Twojego publicznego klucza PGP w oknie tworzenia standardowej wiadomości w sekcji „Załącz” wybierz opcję „mój klucz publiczny OpenPGP”, a następnie wyślij wiadomość. Uwaga! Na tym etapie nie zaznaczaj jeszcze opcji szyfrowania.



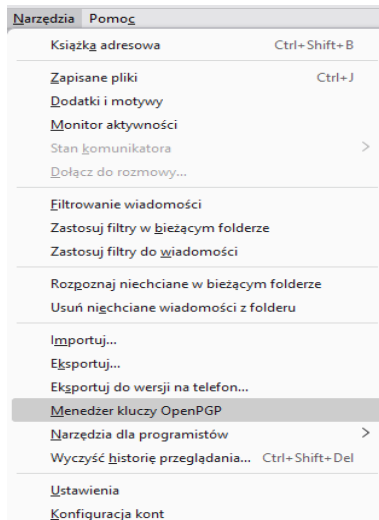
Klucz publiczny można odszukać z serwera kluczy w menadżerze kluczy OpenPGP.

## Import publicznego klucza PGP

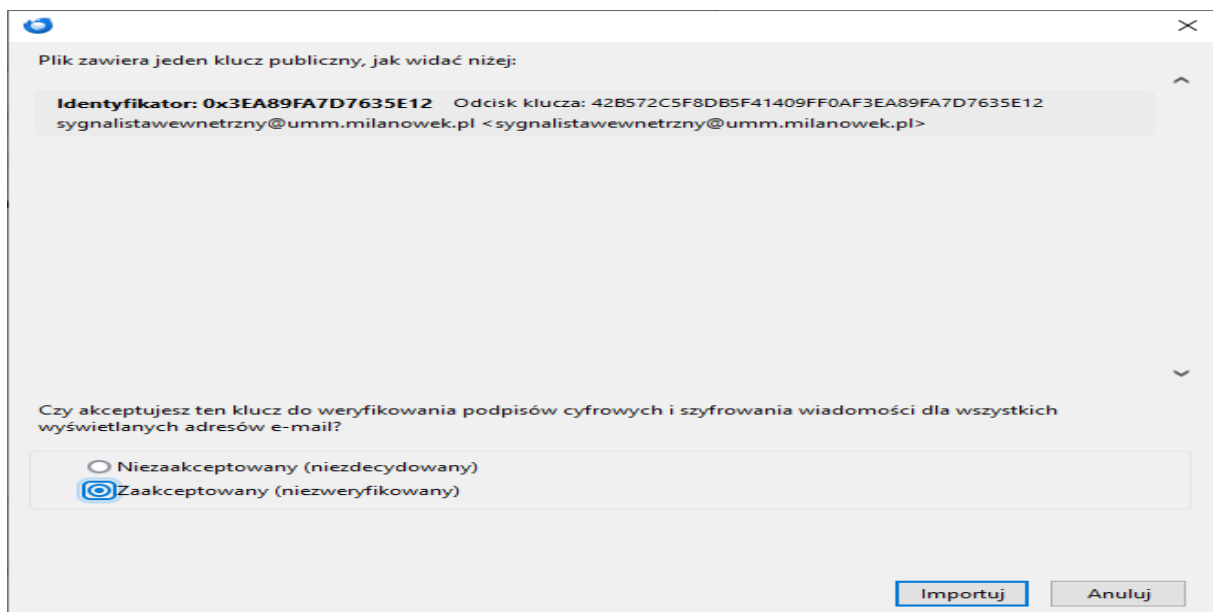
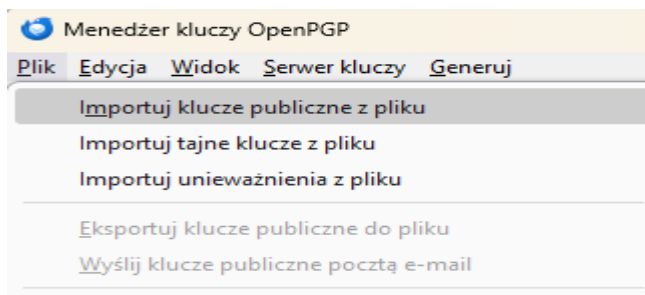
Klucz znajduje się pod adresem `bip.milanowek.pl` dołączony wraz z tą procedurą.

„klucz\_publiczny\_sygnalistawewnetrzny@umm.milanowek.pl-0x3EA89FA7D7635E12-pub.asc”

W przypadku chęci zaimportowania klucza kliknij paska menu narzędzia następnie „Menedżer kluczy OpenPGP”



W nowym oknie wybierz plik a następnie wybierz opcję „Importuj klucze publiczne OpenPGP”.



Gdy pojawi się okno sprawdzamy odcisk klucza czy jest to:

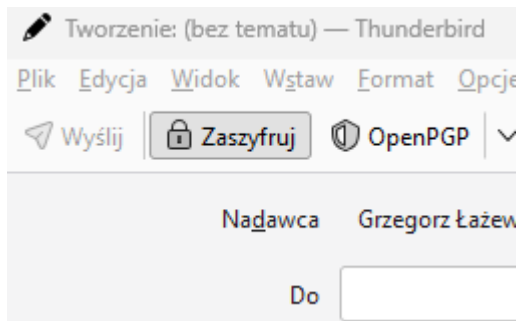
**42B5 72C5 F8DB 5F41 409F F0AF 3EA8 9FA7 D763 5E12**

Zaznaczamy opcję „Zaakceptowany”

W oknie zatwierdź otrzymany klucz nadawcy i wybieramy importuj.

Krok III – wysyłka zaszyfowanej wiadomości

Gdy, już wraz z odbiorcą wymieniliśmy się publicznymi kluczami PGP, nadszedł czas na wysyłkę pierwszej zaszyfowanej wiadomości. W tym celu wystarczy, że w oknie tworzenia wiadomości w sekcji „Zaszyfruj” zaznaczysz opcję.



Krok IV – odbiór zaszyfowanej wiadomości

Jeśli prawidłowo wymieniliśmy się z nadawcą kluczami PGP to przesłana przez niego wiadomość zostanie automatycznie odszyfowana. Informację o szyfrowaniu znajdziesz w prawym górnym rogu wiadomości.

