

Zarządzenie nr 4/IX/2025

Burmistrza Miasta Milanówka

z dnia 13 stycznia 2025 r.

w sprawie **wprowadzenia w Urzędzie Miasta Milanówka procedury przyjmowania zgłoszeń zewnętrznych sygnalistów oraz podejmowania działań następnych**

Na podstawie art. 33 ustawy z 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. 2024 r., poz. 928) zarządza się, co następuje:

§ 1

Wprowadza się w Urzędzie Miasta Milanówka procedurę przyjmowania zgłoszeń zewnętrznych sygnalistów oraz podejmowania działań następnych, 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 opublikowania na stronie podmiotowej Biuletynu Informacji Publicznej prowadzonej przez Urząd Miasta Milanówka.

Burmistrz Miasta Milanówka

/-/

Artur Niedziński

**Procedura przyjmowania zgłoszeń zewnętrznych sygnalistów
oraz podejmowania działań następczych
w Urzędzie Miasta Milanówka**

§1

1. Procedura przyjmowania zgłoszeń zewnętrznych, zwana dalej procedurą, reguluje zasady zgłaszania informacji o naruszeniach prawa i podejmowania działań następczych. Procedura stanowi realizację przepisu art. 8 ust. 1 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii, zwaną dalej dyrektywą, oraz art. 33 ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. z 2024, poz. 928), zwanej dalej ustawą.
2. Zakresem podmiotowym procedury objęci są sygnaliści, czyli osoby fizyczne, zgłaszające lub ujawniające publicznie informację o naruszeniu prawa pozyskaną w kontekście związanym z pracą, o których mowa w art. 4 ustawy.
3. Na podstawie niniejszej procedury następuje zgłaszanie naruszeń w ramach obszarów, o których mowa w art. 3 ust. 1 ustawy.
4. Niniejsza procedura nie ma zastosowania do zgłoszeń dokonanych anonimowo. Zgłoszenia dokonane anonimowo nie są przyjmowane.

§2

Ilekcroć w niniejszej procedurze jest mowa o:

- 1) administratorze – należy przez to rozumieć administratora danych osobowych w rozumieniu art. 4 pkt 7) RODO, tj. Burmistrza Miasta Milanówka;
- 2) Burmistrzu – należy przez to rozumieć Burmistrza Miasta Milanówka;
- 3) Koordynatorze - należy przez to rozumieć Sekretarza Miasta Milanówka;
- 4) rejestrze – należy przez to rozumieć rejestr zgłoszeń zewnętrznych, o którym mowa w art. 46 ust. 1 pkt 1 ustawy;
- 5) KPA - należy przez to rozumieć Kodeks Postępowania Administracyjnego;
- 6) 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.);
- 7) urzędzie – należy przez to rozumieć Urząd Miasta Milanówka;

- 8) ustawie - należy przez to rozumieć ustawę z 14 czerwca 2024 r. o ochronie sygnalistów (Dz.U. 2024 r., poz. 928).

§3

1. Za wdrożenie procedury i koordynację działań wynikających z jej zapisów odpowiada Koordynator.
2. Koordynator odpowiada za przyjmowanie zgłoszeń oraz podejmowanie działań następczych.
3. Koordynator działa na podstawie upoważnienia Burmistrza.
4. Koordynator prowadzi rejestr zgłoszeń zewnętrznych.

§4

1. Zgłoszenia naruszenia można dokonywać w formie pisemnej poprzez dedykowany poufny kanał zgłoszeń za pomocą poczty elektronicznej na adres: sygnalistazewnetrzny@umm.milanowek.pl w zaszyfrowanej wiadomości przesłanej zgodnie z instrukcją stanowiącą **załącznik nr 1**.
2. Przyjmowane są zgłoszenia podpisane przez sygnalistę. Zgłoszeń dokonanych anonimowo nie przyjmuje się. .
3. W przypadku gdy zgłoszenie wpłynie za pośrednictwem innego kanału komunikacji, właściwy pracownik przekazuje je niezwłocznie Koordynatorowi, bez wprowadzania zmian w zgłoszeniu.
4. Dostęp do zgłoszeń posiadać mogą wyłącznie osoby uprawnione, w zakresie niezbędnym do wykonania powierzonych zadań.

§5

1. Koordynator dokonuje wstępnej weryfikacji zgłoszenia.
2. Jeżeli wstępna weryfikacja zgłoszenia wykaże, że zgłoszenie podlega rozpatrzeniu, Koordynator przekazuje sygnaliście potwierdzenie przyjęcia zgłoszenia w terminie 7 dni od jego otrzymania, chyba że sygnalista wystąpił wyraźnie z odmiennym wnioskiem w tym zakresie lub Koordynator ma uzasadnione podstawy sądzić, że potwierdzenie przyjęcia zgłoszenia zagroziłoby ochronie poufności tożsamości sygnalisty..
3. Jeżeli wstępna weryfikacja wykaże, że dla rozpatrzenia zgłoszenia właściwy jest inny organ publiczny, Koordynator:
 - 1) przekazuje zgłoszenie do właściwego organu niezwłocznie, nie później jednak niż w terminie 14 dni od dnia dokonania zgłoszenia, a w uzasadnionych przypadkach – nie później niż w terminie 30 dni;
 - 2) informuje o tym sygnalistę, w terminie określonym w KPA, wskazując przynajmniej organ publiczny, do którego przekazano zgłoszenie, i datę przekazania, chyba że sygnalista nie przekazał adresu do kontaktu.

4. Jeżeli wstępna weryfikacja zgłoszenia wykaże, że zgłoszenie nie podlega rozpatrzeniu, Koordynator przekazuje zgłaszającemu informację w tym zakresie, w terminie określonym w KPA.

§6

1. Koordynator podejmuje działania następcze wobec każdego zgłoszenia zewnętrznego przyjętego do rozpatrzenia.
2. Działania następcze obejmują:
 - 1) wstępną ocenę zgłoszenia, w celu przygotowania postępowania wyjaśniającego;
 - 2) postępowanie wyjaśniające, którego celem jest ustalenie stanu faktycznego i ocena prawdziwości informacji zawartych w zgłoszeniu;
 - 3) dalsze działania następcze, które mają na celu przeciwdziałanie skutkom i przyczynom naruszenia prawa lub obniżenie ryzyka naruszenia prawa.
3. Jeżeli wstępna ocena zgłoszenia wykaże, że zawiera ono informacje, które na mocy odrębnych przepisów podlegają przekazaniu do właściwych instytucji, organów lub jednostek organizacyjnych Unii Europejskiej, to Koordynator realizuje obowiązek wskazany w art. 39 ust 4 ustawy.
4. Jeżeli wstępna ocena zgłoszenia wskaże na zasadność powierzenia postępowania wyjaśniającego innej jednostce, Koordynator działając w imieniu Burmistrza, może przekazać takie zgłoszenie:
 - 1) jednostce organizacyjnej podległej lub nadzorowanej;
 - 2) innej jednostce organizacyjnej, której powierzono zadania w drodze porozumienia z wyjątkiem jednostki organizacyjnej, której dotyczy zgłoszenie.
5. Po przeprowadzeniu postępowania wyjaśniającego jednostka, o której mowa w ust. 4, przekazuje Koordynatorowi protokół ustaleń lub odpowiedni dokument wynikający z przepisów odrębnych, w celu podjęcia dalszych działań następczych, z propozycjami takich działań.
6. W przypadku samodzielnego prowadzenia postępowania wyjaśniającego, Koordynator powierza jego przeprowadzenie zgodnie z właściwością wewnętrzną tj. osobom lub komórce organizacyjnej właściwej w badaniu naruszenia prawa będącego przedmiotem zgłoszenia.
7. W przypadku gdy zgłoszenie dotyczy naruszeń prawa pozostających we właściwości kilku stanowisk lub komórek organizacyjnych, Koordynator powołuje zespół zadaniowy złożony z ich przedstawicieli, w celu całościowego wyjaśnienia zgłoszenia.
8. Zespół może korzystać z pomocy wewnętrznych i zewnętrznych ekspertów.
9. Koordynator informuje sygnalistę o ostatecznym wyniku postępowań wyjaśniających wszczętych na skutek zgłoszenia zewnętrznego.

§7

1. Po zakończeniu postępowania wyjaśniającego sporządzany jest protokół ustaleń zawierający opis stanu faktycznego oraz wnioski w zakresie potwierdzenia naruszenia prawa. Do protokołu Koordynator dołącza propozycję dalszych działań następczych.
2. Jeżeli przepisy odrębne nie wymagają innego trybu, to:
 - 1) protokół jest przedkładany Burmistrzowi;
 - 2) Burmistrz może zwrócić protokół w celu przeprowadzenia dodatkowych czynności, nie może jednak samodzielnie ingerować w jego treść;
 - 3) Burmistrz zatwierdza protokół i określa dalsze działania następcze, jeżeli postępowanie wyjaśniające stwierdziło naruszenie prawa lub wskazało na ryzyko występowania naruszeń prawa.
3. Zatwierdzenie protokołu kończy postępowanie wyjaśniające.

§8

1. Burmistrz działający przy pomocy urzędu jest administratorem danych osobowych w rozumieniu art. 4 pkt 7) RODO, które przetwarza 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. 1 lit. g) RODO, jeżeli sygnalista poda w zgłoszeniu dane osobowe należące do szczególnych kategorii danych osobowych.
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. Klauzula informacyjna jest dostępna na Karcie zgłoszenia i wręczana będzie przy zgłoszeniu bezpośrednim. Pełna treść obowiązku informacyjnego stanowi załącznik nr 2 do niniejszej procedury.
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.

§9

1. Koordynator prowadzi działania informacyjne związane ze stosowaniem ustawy i procedury. W szczególności opracowuje informację na temat zgłoszeń zewnętrznych, o której mowa w art. 48 ustawy.
2. Koordynator przygotowuje projekty sprawozdań, o których mowa w art. 47 ustawy.
3. Koordynator dokonuje przeglądów procedur, o których mowa w art. 49 ustawy.

Załącznik nr 1
do Procedury przyjmowania zgłoszeń zewnętrznych sygnalistów
oraz podejmowania działań następnych
w Urzędzie Miasta Milanówka

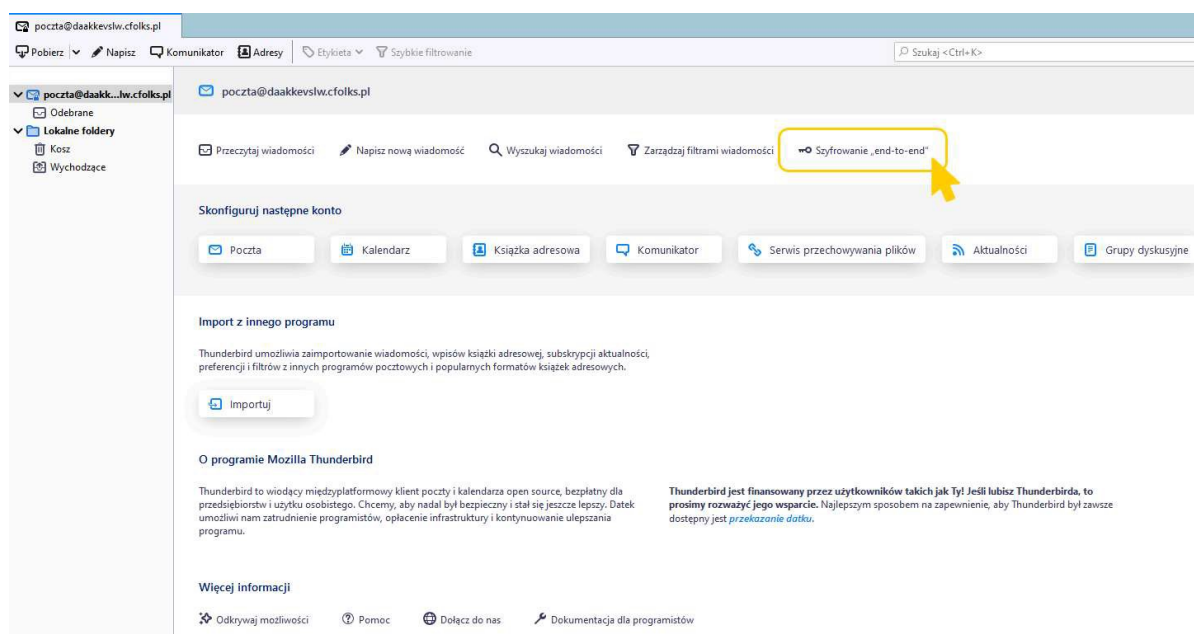
Instrukcja przesyłania zgłoszeń zewnętrznych

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 **mgr@liberemur.org@unimilano.edu.pl**

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

[Więcej informacji](#)

[Dodaj klucz...](#)

☐ Żaden

Nie używaj OpenPGP dla tej tożsamości.



0x3E82CECA48F11D12

Wygasa: 3.01.2027

Opublikowanie klucza publicznego na serwerze kluczy umożliwia innym jego wykrycie.

[Opublikuj](#)

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

[Menedżer kluczy OpenPGP](#)

S/MIME

Certyfikat osobisty do podpisywania cyfrowego:

[Wybierz...](#)

[Wyczyść](#)

Certyfikat osobisty do szyfrowania:

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

i **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

Kontynuuj

Anuluj



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: **Signalista z zewnątrz <signalista.zewnetrzny@umm.milanoosk.pl> - signalista z zewnątrz**

Ważność klucza

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

☒ Klucz wygasa za lat(a)

☐ Klucz nie wygasa

Ustawienia zaawansowane

Zaawansowane ustawienia klucza OpenPGP.

Typ klucza:

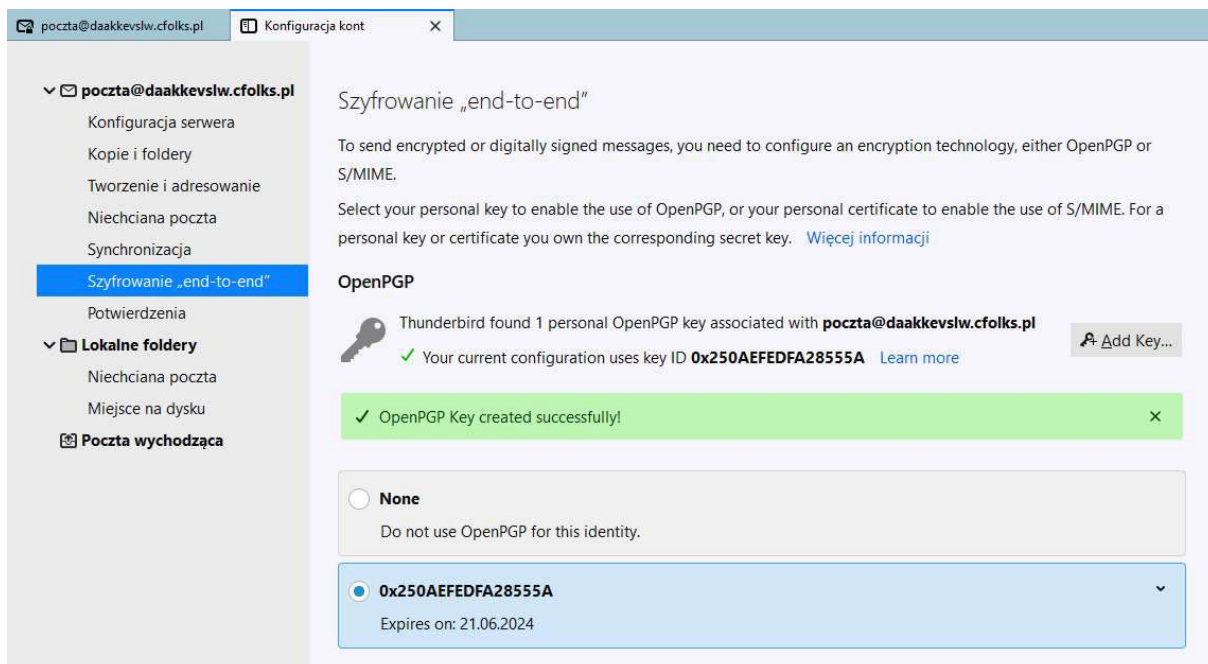
Rozmiar klucza:

Wygeneruj klucz

Wstecz

Anuluj

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.

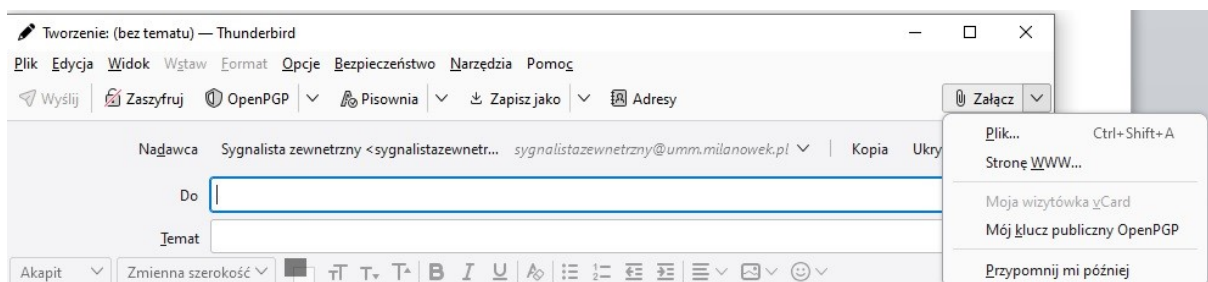


Brawo! Twój klucz jest już gotowy. W dalszej części poradnika dowiesz się, jak wymieniać się kluczami oraz szyfrować wiadomości.

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.

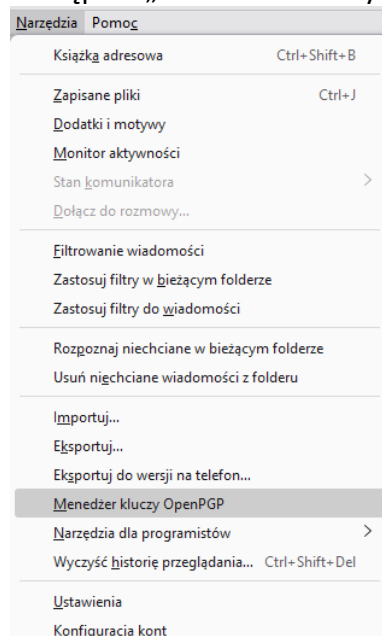


Klucz publiczny można odszukać z serwera kluczy w menadżerze kluczy OpenPGP.

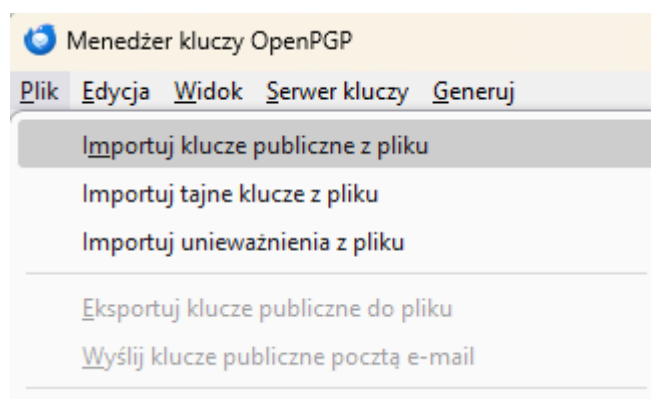
Import publicznego klucza PGP

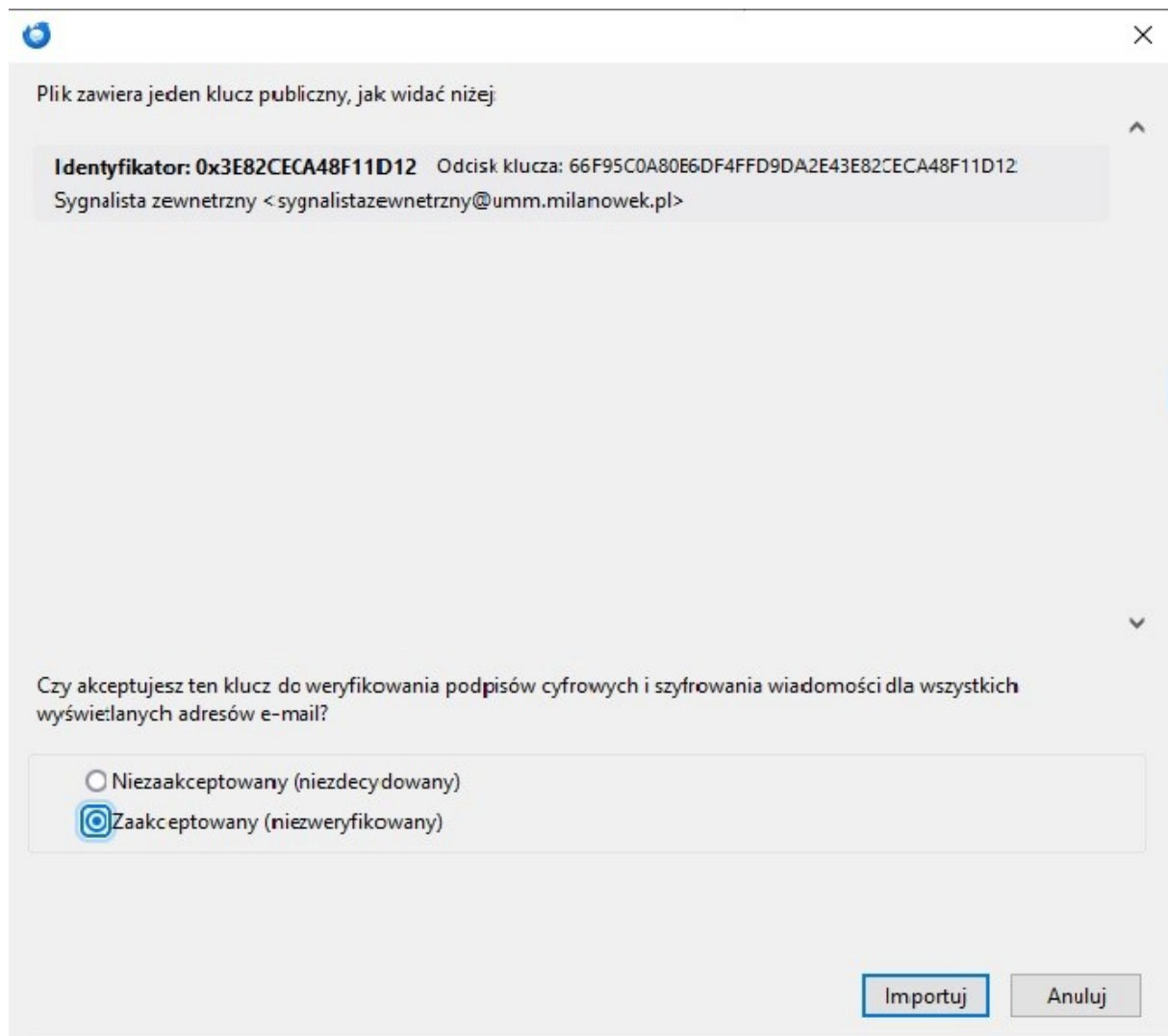
Klucz znajduje się pod adresem bip.milanowek.pl dołączony wraz z tą procedurą. „Sygnalista zewnętrzny sygnalistazewnetrzny@umm.milanowek.pl-(0x3E82CECA48F11D12)-public”

W przypadku chęci zaimportowania klucza prywatnego kliknij pasku 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 palca klucza czy jest to:

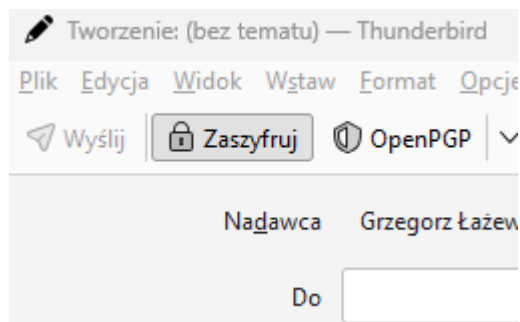
66F9 5C0A 80B6 DF4F FD9D A2E4 3E82 CECA 48F1 1D12

Zaznaczamy opcję „Zaakceptowany”

W oknie zatwierdź otrzymany klucz nadawcy i wybieramy importuj.

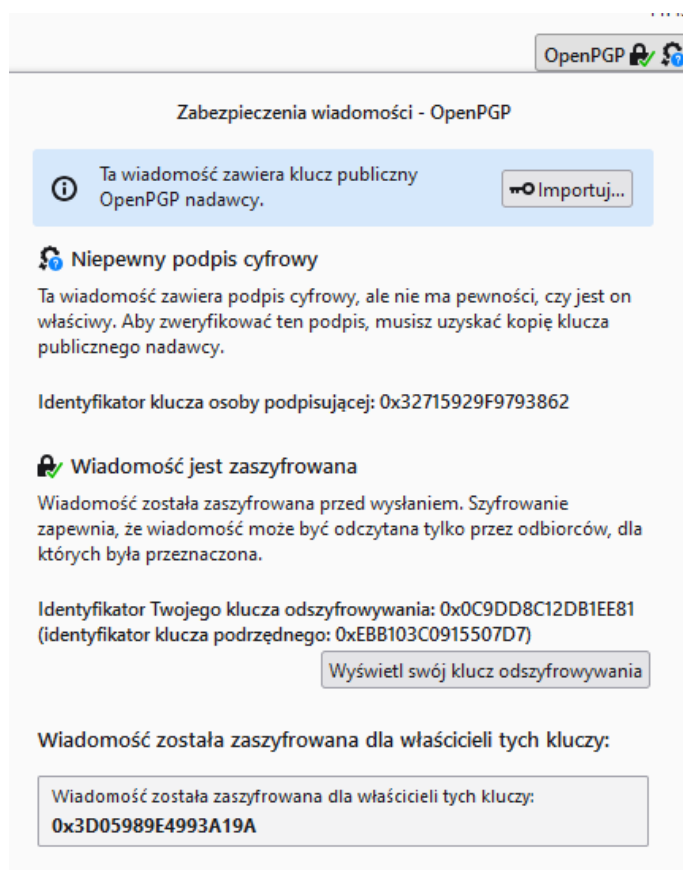
Krok III – wysyłka szyfrowanej wiadomości

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



Krok III – odbiór zaszyfrowanej wiadomości

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



Klauzula informacyjna RODO

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), zwane dalej RODO, informujemy, o tym, że:

1. Administrator danych osobowych:

Administratorem Pani/Pana danych osobowych jest Burmistrz Miasta Milanówka działający przy pomocy Urzędu Miasta Milanówka z siedzibą przy ul. Kościuszki 45, 05-822 Milanówek, 05-822 Milanówek, tel. 22 758 30 61, e-mail: miasto@milanowek.pl

2. Inspektor Ochrony Danych:

Administrator powołał Inspektora Ochrony Danych, z którym może się Pani/Pan skontaktować w przypadku jakichkolwiek pytań lub uwag dotyczących przetwarzania Pani/Pana danych osobowych i praw przysługujących Pani/Panu na mocy przepisów o ochronie danych osobowych. Dane kontaktowe IOD : tel. 22 350 01 40, e-mail: iod@milanowek.pl

3. Cel przetwarzania

Pani/Pana dane osobowe będą przetwarzane w celach związanych z sygnalizowaniem naruszenia, zgodnie z art. 6 ust. 1 lit. c RODO w zw. z ustawą o ochronie sygnalistów z dnia 14 czerwca 2024 roku (Dz. U. z 2024 r. poz. 928 ze zm.)

4. Prawa osób, których dane dotyczą

Posiada Pani/Pan prawo do żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do wniesienia skargi do organu nadzorczego (Prezes Urzędu Ochrony Danych Osobowych).

5. Okres przechowywania

1. Pani/Pana dane osobowe zwarte w rejestrze zgłoszeń wewnętrznych są przechowywane przez okres 3 lat po zakończeniu roku kalendarzowego, w którym zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.
2. dane osobowe przetwarzane w związku z przyjęciem zgłoszenia lub podjęciem działań następczych oraz dokumenty związane z tym zgłoszeniem są przechowywane przez podmiot prawny przez okres 3 lat po zakończeniu roku kalendarzowego, w którym przekazano zgłoszenie zewnętrzne do organu publicznego właściwego do podjęcia działań następczych lub zakończono działania następcze, lub po zakończeniu postępowań zainicjowanych tymi działaniami.

6. Odbiorcy danych

Co do zasady Pana/ Pani dane są zachowane w poufności. Pani/Pana dane osobowe mogą być ujawniane uprawnionym podmiotom, w związku z weryfikacją zgłoszenia za Pana/Pani wyraźnym przyzwoleniem, w trybie określonym przez bezwzględnie obowiązujące przepisy prawa.

7. Profilowanie

Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany.

8. Dobrowolność podania danych

Podanie danych osobowych jest dobrowolne, przy czym zgłoszenia dokonane anonimowo nie podlegają przyjęciu.