Załącznik nr 3
do zarządzenia nr 22.2024
Dyrektora Miejskiego Ośrodka Pomocy Społecznej
w Ełku z dnia 17 września 2024 .
w sprawie ustalenia wewnętrznej procedury
dokonywania zgłoszeń naruszeń prawa
i podejmowania działań następczych,
z uwzględnieniem ochrony osób dokonujących tych
zgłoszeń

OCHRONA DANYCH OSOBOWYCH SYGNALISTY

ZASADY ZWIĄZANE Z REALIZACJĄ PROCEDURY ZGŁASZANIA NARUSZEŃ PRAWA

Definicje

§ 1.

1) **Organizacja lub ADO**– /Miejski Ośrodek Pomocy Społecznej/, będący Administratorem danych osobowych sygnalistów i innych osób, których dane są przetwarzane w związku z przyjmowaniem zgłoszeń wewnętrznych;
2) **ustawa o ochronie sygnalistów** – ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. 2024 r. poz. 928) wdrażającej dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii;
3) **RODO** - Rozporządzenie 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);
4) **procedura** - /Procedura zgłoszeń wewnętrznych w Miejskim Ośrodku Pomocy Społecznej/
5) **upoważniony** – osoba upoważniona na podstawie Procedury do realizacji zadań wynikających z ustawy o ochronie sygnalistów;
6) **sygnalista** – osoba, która zgłasza lub ujawnia publicznie informację o naruszeniu prawa uzyskaną w kontekście związanym z pracą, zgodnie z Procedurą;
7) **osoba pomagająca w dokonaniu zgłoszenia** – osoba fizyczna, która pomaga sygnaliście w zgłoszeniu lub ujawnieniu publicznym;
8) **osoba powiązana z sygnalistą** – osoba fizyczna, która może doświadczyć działań odwetowych w związku ze zgłoszeniem dokonanym przez sygnalistę. To może obejmować współpracowników, członków rodziny sygnalisty, lub innych, którzy mogą być narażeni na negatywne konsekwencje z powodu ich związku z sygnalistą;
9) **osoba której dotyczy zgłoszenie** - oznacza osobę fizyczną lub prawną, która jest wskazana w zgłoszeniu lub ujawnieniu publicznym jako osoba, która dopuściła się naruszenia lub z którą osoba ta jest powiązana;
10) **dane osobowe** – zgodnie z art. 4 ust. 1 RODO informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
11) **inspektor ochrony danych (IOD)** – osoba wyznaczona przez Administratora, do pełnienia zadań, o których mowa w art. 39 RODO;

Przetwarzanie danych osobowych

§ 2.

1. Organizacja w związku z przyjmowaniem zgłoszeń od sygnalistów zapewnia:
   1) aby przetwarzanie danych osobowych odbywało się w sposób uniemożliwiający nieupoważnionym osobom uzyskanie dostępu do informacji objętych zgłoszeniem;
   2) ochronę poufności tożsamości sygnalisty, innych osób wskazanych w zgłoszeniu lub powiązanych z sygnalistą;
   3) aby dane osobowe wskazane w zgłoszeniu wykorzystywane były wyłącznie na potrzeby weryfikacji zgłoszenia i podejmowania działań następczych;
   4) aby dostęp do danych osobowych miały wyłącznie osoby upoważnione do realizacji poszczególnych obowiązków związanych z przyjmowaniem zgłoszeń, ich rozpatrywaniem i realizowaniem działań następczych. ***Wzór upoważnienia i oświadczenia o zachowaniu poufności stanowi załącznik nr 1 do niniejszych zasad***;
   5) aby do dokumentów zawierających dane osobowe sygnalisty lub innych osób wskazanych w zgłoszeniu i podlegających ochronie nie miało dostępu ani kierownictwo organizacji, ani przełożeni sygnalisty.

§ 3.

1. Na potrzeby realizacji obowiązków Organizacji wynikających z ustawy o ochronie sygnalistów mogą być przetwarzane dane osobowe dotyczące:
   1) sygnalisty (podane w zgłoszeniu o naruszeniu prawa);
   2) osób wskazanych przez sygnalistę w zgłoszeniu, w szczególności:
      a) osób pomagających sygnaliście w dokonaniu zgłoszenia,
      b) osób powiązanych z sygnalistą,
      c) osób, których dotyczy zgłoszenie,
      d) ewentualnych świadków;
   3) innych osób, które mogą mieć istotne informacje na temat naruszenia prawa, które zgłasza sygnalista.
2. W związku z przyjmowaniem i rozpatrywaniem zgłoszeń mogą być przetwarzane dane zwykłe, ale też dane szczególnej kategorii, o których mowa w art. 9 ust. 1 lub art. 10 RODO (np. dotyczących stanu zdrowia, orientacji seksualnej, poglądów politycznych, przekonań religijnych lub światopoglądowych oraz wyroków i naruszeń prawa – jeśli takie informacje zostaną ujawnione przez sygnalistę).

§ 4.

1. Wobec sygnalistów oraz osób pomagających w zgłoszeniu realizuje się obowiązek informacyjny wynikający z art. 13 RODO poprzez umieszczenie informacji przy formularzu zgłoszeń znajdującego się: www.sygnalista.miasto.elk.pl
2. ***Wzór klauzuli informacyjnej dla sygnalistów oraz osób pomagających w zgłoszeniu stanowi załącznik nr 2 do niniejszych zasad***.

3. Wobec osób, których dotyczy zgłoszenie obowiązek informacyjny realizuje się:
   1) z uwzględnieniem art. 14 RODO, przy czym przekazanie klauzuli informacyjnej powinno nastąpić najpóźniej:
      a) w ciągu miesiąca od pozyskania danych (chyba że, istnieje uzasadnione podejrzenie, że osoba, która ma zostać poinformowana o przetwarzaniu jej danych w związku z wyjaśnianiem zgłoszonego naruszenia może dopuścić się zacierania śladów naruszenia),
      b) przy pierwszym ujawnieniu danych innemu odbiorcy;
   2) z pominięciem informacji o źródle danych, chyba że sygnalista:
      a) nie spełnia warunku art. 6 ustawy o ochronie sygnalistów (czyli nie miał uzasadnionej podstawy by sądzić, że informacja będąca przedmiotem zgłoszenia jest prawdziwa w momencie dokonywania zgłoszenia i że stanowi informację o naruszeniu prawa), lub
      b) wyraził wyraźną zgodę na ujawnienie swojej tożsamości.
4. ***Wzór klauzuli informacyjnej dla osób, których dotyczy zgłoszenie stanowi załącznik nr 3 do niniejszych zasad***.
5. W przypadku, gdy pracownik upoważniony do realizacji działań następczych prowadzi przesłuchania pracowników lub innych osób mających lub mogących mieć związek z przedmiotem postępowania, wobec tych osób również zostaje spełniony obowiązek informacyjny. ***Wzór klauzuli informacyjnej dla osób przesłuchiwanych w związku ze zgłoszeniem stanowi załącznik nr 4 do niniejszych zasad.***
6. Obowiązek informacyjny może zostać niespełniony wyłącznie w przypadku gdy przekazanie klauzuli informacyjnej wpłynie na realizację obowiązków związanych ze zgłoszonym naruszeniem (uniemożliwi lub poważnie utrudni realizację celów przetwarzania).
7. Dla wykazania spełniania zasady rozliczalności każda decyzja o rezygnacji z realizacji obowiązku informacyjnego jest odnotowywana z podaniem uzasadnienia decyzji.
8. Na stronie internetowej oraz w siedzibie Organizacji, w widocznym miejscu umieszcza się ogólną klauzulę informacyjną dla osób, których dane są przetwarzane w związku z przyjmowaniem i rozpatrywaniem zgłoszeń. Upoważniony pracownik w każdym momencie może odesłać osobę zainteresowaną poznaniem zasad przetwarzania danych osobowych na stronę www lub w odpowiednie miejsce w siedzibie.
9. ***Wzór ogólnej klauzuli informacyjnej na stronę internetową oraz do placówek stanowi załącznik nr 5 do niniejszych zasad.***

§ 5.

1. Nie ujawnia się osobom nieupoważnionym danych osobowych sygnalisty, pozwalających na ustalenie jego tożsamości.
2. Zapisów ust. 1 nie stosuje się w przypadku gdy sygnalista **wyraził wyraźną zgodę na ujawnienie jego danych.**
3. Przed dokonaniem ujawnienia osoba upoważniona powiadamia o tym sygnalistę, przesyłając w postaci papierowej lub elektronicznej wyjaśnienie powodów ujawnienia jego

danych osobowych, chyba że takie powiadomienie zagrozi postępowaniu wyjaśniającemu lub postępowaniu przygotowawczemu, lub sądowemu.

4. Dane osobowe wskazane w zgłoszeniu sygnalisty mogą zostać ujawnione organom publicznym właściwym do podjęcia działań następczych, np.: Policja, prokuratura, Państwowa Inspekcja Pracy. W przypadku przekazywania informacji tym instytucjom, konieczna jest bezwzględna ochrona tożsamości sygnalisty i innych osób narażonych na działania odwetowe.

§ 6.

1. Nie są zbierane dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia. W razie przypadkowego zebrania dane osobowe są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy.
2. Dane osobowe przetwarzane w związku z przyjęciem zgłoszenia lub podjęciem działań następczych oraz dokumenty związane z tym zgłoszeniem są przechowywane przez Organizację 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.
3. Dane osobowe oraz pozostałe informacje zawarte w prowadzonym w Organizacji 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.
4. Upoważniony pracownik co najmniej raz w roku dokonuje przeglądu danych osobowych w celu ustalenia niezbędności dalszego ich przechowywania.
5. Usuwane są dane osobowe, których dalsze przechowywanie jest zbędne do realizacji celów, dla których zostały zebrane z zachowaniem terminów wskazanych w ust. 1 - 3
6. Z czynności, o których mowa w ust. 4-5 sporządza się protokół przeglądu/usunięcia danych osobowych przetwarzanych w związku z przyjęciem zgłoszenia sygnalisty lub podjęciem działań następczych. ***Wzór protokołu stanowi załącznik nr 6 do niniejszych zasad.***
7. Dane osobowe powinny zostać usunięte w sposób uniemożliwiający ich ponowne odczytanie i w sposób zapewniający zachowanie poufności tych informacji. W szczególności dane zapisane na nośnikach papierowych (dokumenty), powinny zostać zniszczone w niszczarce.
8. Usunięcie danych osobowych obejmuje wszelkie kanały, systemy i nośniki, na których zgromadzono dane osobowe, w tym pocztę e-mail.

Obowiązki Organizacji

§ 7.

1. Organizacja wprowadza wszelkie niezbędne środki techniczne i organizacyjne, które mają gwarantować bezpieczeństwo danych osobowych sygnalistów i innych osób, których dane przetwarzane są w związku ze zgłoszeniem.
2. Organizacja przeprowadza analizę ryzyka zgodnie z procedurami przyjętymi w Polityce Ochrony Danych.
3. W celu ograniczenia ryzyka związanego z utratą dostępności, integralności oraz poufności przetwarzanych danych osobowych Organizacja:
    1) zobowiązuje się do uniemożliwienia dostępu do danych osobowych sygnalisty osobom z kierownictwa lub bezpośrednim przełożonym;
    2) zapewnia upoważnionym odpowiednio zabezpieczony sprzęt służbowy (laptopy, komputery) z dostępem do bezpiecznej sieci Internet;
    3) w prowadza zabezpieczenia skrzynki mailowej przeznaczonej do przyjmowania zgłoszeń inne niż standardowe, w tym: uniemożliwienie dostępu do skrzynki oraz kopii wiadomości osobom innym niż upoważniony;
    4) wprowadza zakaz kopiowania danych osobowych sygnalistów i innych osób na zewnętrzne nośniki danych (pendrive, dyski, itp.) oraz robienia dodatkowych wydruków;
    5) ogranicza dostęp do poszczególnych kategorii informacji uzależniając go od obowiązków powierzonych upoważnionemu,
    6) zapewnia szkolenia dla pracowników z procedury obsługi zgłoszeń sygnalistów;
    7) zapewnia szkolenia dla osób upoważnionych z zakresu ochrony danych osobowych;
    8) zapewnia aby wydawane upoważnienia do przetwarzania danych osobowych były dopasowane do zakresu obowiązków związanych z obsługą zgłoszeń;
    9) zapewnia upoważnionemu pracownikowi wydzielone odrębne szafki, szuflady z możliwością zamykania na klucz do przechowywania dokumentów/nośników danych związanych ze zgłaszaniem naruszeń;
    10) przeprowadza dokładne mapowanie przepływu informacji i ustalenie do jakich narzędzi (lub systemów) związanych z obsługą zgłoszeń mają dostęp pracownicy (np.: monitoring wizyjny, linia telefoniczna, itp.)

§ 8.

1. W każdym przypadku gdy realizacja działań związanych z przyjmowaniem zgłoszeń lub ich weryfikacją czy innych działań jest zlecana podmiotowi zewnętrznemu Organizacja realizuje obowiązki związane z powierzaniem przetwarzania danych osobowych zgodnie z procedurą przyjętą w Polityce Ochrony Danych, a w szczególności poprzez:
    1) dokonanie weryfikacji podmiotu przetwarzającego pod kątem spełniania wymogów RODO;
    2) zawarcie umowy powierzenia przetwarzania danych osobowych, zgodnie art. 28 ust. 3 RODO.

Obowiązki upoważnionego

§ 9.

1. W związku z przetwarzaniem danych osobowych sygnalisty i innych osób upoważniony pracownik jest zobowiązany do:
   1) przestrzegania zasad przyjętych w Polityce Ochrony Danych (w szczególności załącznika nr 5.3.1 do POD) oraz innych wewnętrznych procedurach;
   2) wykorzystywania danych osobowych zawartych w dokumentach dotyczących zgłoszenia tylko przez okres niezbędny do wykonania powierzonych zadań;
   3) wykorzystywania pozyskanych danych wyłącznie w celu realizacji swoich służbowych obowiązków;
   4) utrzymywania danych w tajemnicy, zarówno podczas łączącego go z Organizacją stosunku pracy jak i po jego zakończeniu;
   5) nie udostępniania osobom nieupoważnionym jakichkolwiek informacji i dokumentów zawierających dane osobowe,
   6) dbania podczas rozmów z innymi osobami by nie zasugerować kim jest sygnalista;
   7) przestrzegania określonych zasad korzystania z dokumentów papierowych:
      a) zabronione jest zabieranie dokumentów zawierających dane osobowe poza siedzibę Organizacji,
      b) zabronione jest wykonywanie kopii dokumentów zawierających dane osobowe,
      c) zabronione jest pozostawianie bez nadzoru osób trzecich w pomieszczeniu gdzie znajdują się dokumenty zawierające dane osobowe,
      d) należy stosować zasadę „białej kartki" w czasie bieżącej pracy - w celu uniemożliwienia osobie postronnej zapoznania się z danymi zawartymi na dokumencie,
      e) należy stosować zasadę „czystego biurka" - zabezpieczenie po pracy dokumentów w zamykanych szafach, do których nie ma dostępu żadna z osób nieupoważnionych,
      f) należy niezwłocznie odbierać wydruki zawierające dane osobowe z drukarki;
   8) przestrzegania zasady ograniczonego przechowywania, poprzez:
      a) pilnowania terminów usuwania danych po okresie ich przydatności,
      b) nie wyrzucania dokumentów zawierających dane osobowe do kosza,
      c) po okresie przechowywania danych określonym niszczy dane za pomocą niszczarki lub poprzez skuteczne zanonimizowanie danych – po upływie okresów przechowywania danych osobowych określonych w §6;
   9) zgłaszania bezpośredniemu przełożonemu lub IOD wszelkich incydentów dotyczących naruszenia bezpieczeństwa danych prowadzących do:
      a) przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania – np. kradzież, zgubienie, zniszczenie dokumentów, nośnika danych (pendrive, dysk przenośny, komputer itp.),

b) przypadkowego lub niezgodnego z prawem zmodyfikowania – np. zaszyfrowanie danych, lub przypadkowa zmiana ich treści powodująca, że danych nie można odtworzyć,

c) nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – np. ujawnienie treści dokumentu, przesłanie maila z danymi osobowymi na niewłaściwy adres, niestosowanie opcji UDW: wysyłając maila do wielu osób, jeżeli ujawnienie ich adresów kontaktowych nie jest zamierzone, a nawet ujawnienie danych członkom rodziny.

2. Za naruszenia bezpieczeństwa danych uważa się w szczególności:
   1) ujawnienie treści danych osobie nieupoważnionej;
   2) dopuszczenie osób nieuprawnionych do przetwarzania danych sygnalistów i innych osób wskazanych w zgłoszeniu;
   3) pozostawienie dokumentów bez nadzoru w miejscu dostępnym dla osób nieuprawnionych;
   4) nieuprawniony dostęp do danych;
   5) kradzież lub zagubienie dokumentów z danymi osobowymi;
   6) dopuszczenie osób nieuprawnionych do dostępu do wydruków z danymi osobowymi;
   7) przypadkowe zniszczenie danych;
   8) dopuszczenie osoby nieuprawnionej do systemu informatycznego;
   9) stwierdzenie prób włamania do systemu informatycznego;
   10) nieprawidłowe zniszczenie danych (np. wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie, niewłaściwa anonimizacja);
   11) przechowywanie danych po okresie wskazanym w przepisach;
   12) nieuzasadnione sporządzenie kopii danych na nośniku papierowym lub elektronicznym;
   13) utrata danych w wyniku działania żywiołów (pożar, zalanie, itp.).

§ 10.

1. W związku z przetwarzaniem danych osobowych z wykorzystaniem komputera/laptopa upoważniony pracownik zobowiązany jest do:
   1) stosowania procedur korzystania ze sprzętu służbowego;
   2) stosowania silnych i bezpiecznych haseł do wykorzystywanych systemów informatycznych, zmiany wykorzystywanych haseł co 90 dni;
   3) zachowania używanych haseł w poufności, nieprzechowywania zapisanych identyfikatorów i haseł w obszarze stanowiska pracy;
   4) nieudzielania dostępu lub zdalnego dostępu do systemu informatycznego osobom nieuprawnionym;
   5) korzystania wyłącznie z oprogramowania udostępnionego przez Organizację do celów związanych z obsługą zgłoszeń;
   6) zastosowania wszelkich możliwych sposobów ograniczających dostęp do urządzeń osobom postronnym, w tym do:

a) zabezpieczenia sprzętu hasłem,
b) każdorazowego blokowania dostępu do systemu przed odejściem od stanowiska pracy;

7) korzystania z udostępnionego przez Organizację bezpiecznego połączenia internetowego;
8) zadbania o to, aby przechowywane dane były bezpiecznie zarchiwizowane;
9) dbania o bezpieczeństwo danych osobowych podczas korzystania z poczty elektronicznej, poprzez:
   a) uniemożliwienie dostępu do poczty osobom nieuprawnionym,
   b) zaszyfrowaniu i zabezpieczeniu hasłem przesyłanych dokumentów zawierających dane osobowe (hasło powinno zostać wysłane innym źródłem komunikacji),
   c) używaniu funkcji UDW przy wysyłaniu wiadomości zawierających dane osobowe do większej ilości odbiorców,
   d) sprawdzeniu, czy jest wiadomość zawierająca dane osobowe skierowana została do odpowiedniego odbiorcy (sprawdzenie adresu e-mail).

Postanowienia końcowe

§ 11.

1. Upoważniony pracownik zobowiązany jest do zapoznania się i zastosowania reguł i procedur określonych w niniejszych zasadach.
2. Niedostosowanie się do niniejszych postanowień może stanowić naruszenie obowiązków pracowniczych.
3. Organizacja monitoruje przestrzeganie niniejszych zasad. Przy czym kontrola ich stosowania nie uprawnia Organizacji do dostępu do danych osobowych sygnalistów.
4. W razie zmiany obowiązujących przepisów prawa lub opublikowania nowych wytycznych powodujących niezgodność niniejszego dokumentu z nimi, niniejsze zasady zostaną dostosowane do obowiązujących przepisów i wytycznych.

Wykaz załączników, które stanowią integralną część do niniejszych zasad:

1. ***Wzór upoważnienia i oświadczenia o zachowaniu poufności - załącznik nr 1.***
2. ***Wzór klauzuli informacyjnej dla sygnalistów oraz osób pomagających w zgłoszeniu - załącznik nr 2.***
3. ***Wzór klauzuli informacyjnej dla osób, których dotyczy zgłoszenie - załącznik nr 3.***
4. ***Wzór klauzuli informacyjnej dla osób przesłuchiwanych w związku ze zgłoszeniem - załącznik nr 4.***
5. ***Wzór ogólnej klauzuli informacyjnej na stronę internetową oraz do placówek - załącznik nr 5.***
6. ***Wzór protokołu - załącznik nr 6 do niniejszych zasad.***

wz. DYREKTORA
Miejskiego Ośrodka Pomocy Społecznej w [illegible]
mgr Grażyna Chilińska
ZASTĘPCA DYREKTORA