**ZARZĄDZENIE NR 87/2026**
**BURMISTRZA MIEROSZOWA**

z dnia 22 kwietnia 2026 r.

**w sprawie zmiany Zarządzenia Nr 274/2021 Burmistrza Mieroszowa z dnia 24 listopada 2021 r. w sprawie wdrożenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Mieroszowie**

Na podstawie art. 33 ust.1 i ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz.U z 2025 poz. 1153) oraz 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 dyrektywy 95/46/WE (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) – dalej jako RODO zarządzam, co następuje:

**§ 1.** W Zarządzeniu Nr 274/2021 Burmistrza Mieroszowa z dnia 24 listopada 2021 r. w sprawie wdrożenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Mieroszowie wprowadzam następujące zmiany:

1. W § 3 ust.2 otrzymuje brzmienie:

1) "2. W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa, określone na formularzu nr 21 - Procedura postępowania w sytuacji naruszenia ochrony danych osobowych."

2) Formularz nr 21- stanowi załącznik nr 1 do niniejszego zarządzenia.

2. W § 9 ust.1 tiret 25 otrzymuje brzmienie: " - IOD raz w roku do 31 grudnia przeprowadza na formularzu nr 20 audyt KRI. Wnioski z audytu KRI zawarte w rekomendacjach są podstawą do opracowania Sprawozdania rocznego z funkcjonowania ochrony danych osobowych w Urzędzie Miejskim w Mieroszowie."

3. W § 10 ust.1 lit. e otrzymuje brzmienie:

1) "e. Szkolenie pracowników. IOD na polecenie Administratora, osobiście lub przy wykorzystaniu podmiotu zewnętrznego przeprowadza szkolenia pracowników w zakresie przepisów prawa oraz uregulowań wewnętrznych zgodnie z przyjętym harmonogramem stanowiącym formularz nr 22. Szkolenia:

   - Pracownicy nowo zatrudnieni przed przystąpieniem do pracy podlegają szkoleniu przez IOD z zakresu ochrony danych osobowych.

   - Szkolenia okresowe odbywają się nie rzadziej niż raz w roku.

   - Ze szkoleń grupowych sporządza się listę obecności pracowników biorących udział wraz z programem szkolenia, które przechowuje IOD."

2) Formularz nr 22- stanowi załącznik nr 2 do niniejszego zarządzenia.

**§ 2.** Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych.

**§ 3.** Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Mieroszowa

**Andrzej Lipiński**

Załącznik nr 1 do zarządzenia nr 87/2026

Burmistrza Mieroszowa

z dnia 22 kwietnia 2026 r.

**Formularzu nr 21 - Procedura postępowania w sytuacji naruszenia ochrony danych osobowych**
**Procedura postępowania w sytuacji naruszenia ochrony danych osobowych**

**§ 1. Cel procedury**

Celem procedury jest zapewnienie szybkiej i skutecznej reakcji na naruszenie ochrony danych osobowych, w tym spełnienie obowiązków wynikających z art. 33 i 34 RODO oraz wytycznych UODO.

**§ 2. Definicje**

1. **Naruszenie ochrony danych osobowych** – zgodnie z art. 4 pkt 12 RODO oznacza naruszenie bezpieczeństwa prowadzące do:

1.1. zniszczenia;

1.2. utracenia;

1.3. zmodyfikowania;

1.4. nieuprawnionego ujawnienia;

1.5. nieuprawnionego dostępu.

2. **Administratorem danych osobowych** jest, zgodnie z artykułem 4 punkt 7 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), osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

3. Jeśli w postanowieniach zarządzenia nie zostanie wskazane inaczej, Administratorem Danych Osobowych jest Burmistrz Mieroszowa.

**§ 3. Klasyfikacja naruszeń ochrony danych osobowych**

1. **Naruszenia poufności danych** rozumie się jako każde zdarzenie prowadzące do:

1.1. nieuprawnionego ujawnienia danych osobowych osobom nieupoważnionym,

1.2. nieautoryzowanego dostępu do danych objętych obowiązkiem ochrony,

1.3. utraty kontroli nad danymi w wyniku działania osób trzecich lub niewłaściwych zabezpieczeń.

4. **Naruszenia integralności danych** oznaczają zdarzenia skutkujące:

4.1. nieautoryzowaną lub przypadkową modyfikacją danych osobowych,

4.2. nieprawidłowym przetworzeniem prowadzącym do zmiany treści danych,

4.3. uszkodzeniem danych uniemożliwiającym ustalenie ich pierwotnej wersji.

5. **Naruszenia dostępności danych** obejmują sytuacje, w których:

5.1. dane osobowe stają się niedostępne dla uprawnionych podmiotów w wymaganym czasie,

5.2. dochodzi do trwałej utraty danych w wyniku zdarzeń losowych lub celowych działań,

5.3. systemy przetwarzania uniemożliwiają realizację praw osób, których dane dotyczą.

**§ 4. Stwierdzenie naruszenia**

1. Wystąpienie naruszenia ochrony danych osobowych nie oznacza, że administrator lub podmiot przetwarzający dopuścił się naruszenia przepisów RODO.

2. Naruszenie przepisów RODO wynika z postępowania niezgodnego z określonymi wymogami przewidzianymi w tym akcie prawnym.

**§ 5. Obowiązki administratora**

1. W przypadku „stwierdzenia" naruszenia ochrony danych osobowych administrator musi zrealizować następujące obowiązki. Należą do nich:

1.1.zaradzenie naruszeniu ochrony danych osobowych oraz jego ewentualnym negatywnym skutkom;

1.2.ocenienie ryzyka naruszenia praw lub wolności osób fizycznych, jakie może wynikać z naruszenia ochrony danych osobowych;

1.3.zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu (w przypadku ryzyka naruszenia praw lub wolności osób fizycznych);

1.4.zawiadamianie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych (w przypadku wysokiego ryzyka naruszenia praw lub wolności tych osób);

1.5.dokumentowanie naruszenia ochrony danych osobowych. Każde takie zdarzenie stanowi okazję do poprawy zabezpieczeń i minimalizowania ryzyka występowania podobnych incydentów w przyszłości.

**§ 6. Działania IOD**

1. Działania IOD w sprawie naruszeń ochrony danych osobowych obejmują w szczególności:

1) pomoc w zapobieganiu naruszeniom, w szczególności poprzez promowanie w organizacji wiedzy o ochronie danych osobowych, organizowanie szkoleń oraz formułowanie zaleceń dotyczących bezpieczeństwa przetwarzania danych;

2) udzielanie wskazówek dotyczących odpowiedniego reagowania na naruszenia ochrony danych osobowych, w tym zaradzania im;

3) zawiadamianie osób, których dane dotyczą;

4) doradztwo w zakresie dokumentowania naruszeń i zarządzania dokumentacją;

5) przekazywanie dodatkowych informacji o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą.

2. IOD nie powinien:

a) zgłaszać naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń;

b) zawiadamiać w imieniu administratorów osób, których dane dotyczą, o naruszeniach ochrony danych osobowych;

c) dokumentować naruszeń ochrony danych osobowych w imieniu administratorów (w szczególności jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określeniem działań zaradczych);

d) podejmować zobowiązań dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających;

e) działać na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych.

**§ 7. Odpowiedzialność administratorów w zakresie ochrony danych osobowych**

1. Administrator danych osobowych ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych, zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO.

2. Zasada rozliczalności oznacza obowiązek wykazania, że działania podejmowane przez administratora są zgodne z przepisami RODO.

3. Administrator jest zobowiązany do dokumentowania swoich działań w zakresie ochrony danych osobowych oraz do przechowywania dowodów potwierdzających zgodność tych działań z obowiązującymi przepisami, w szczególności na potrzeby kontroli lub postępowania przed organem nadzorczym.

4. Dokumentacja potwierdzająca zgodność z RODO obejmuje w szczególności:

4.1.dokumenty tradycyjne, takie jak notatki służbowe, instrukcje, procedury, decyzje wewnętrzne, korespondencję e-mailową;

4.2.wyciągi i raporty z systemów informatycznych;

4.3.raporty z audytów, testów bezpieczeństwa lub przeglądów zgodności.

5. Brak możliwości wykazania zgodności z RODO może zostać uznany za naruszenie przepisów o ochronie danych osobowych, niezależnie od rzeczywistego przebiegu zdarzeń.

**§ 8. Obowiązek zgłaszania incydentów ochrony danych osobowych**

1. Każdy pracownik, który poweźmie podejrzenie lub stwierdzi naruszenie ochrony danych osobowych (tzw. incydent), jest zobowiązany niezwłocznie poinformować o tym swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych.

2. Zgłoszenie powinno nastąpić niezwłocznie, nie później niż w ciągu 24 godzin od momentu powzięcia informacji o incydencie, w formie ustnej (do wiadomości przełożonego) oraz pisemnej (e-mail, notatka służbowa).

3. Niedopełnienie obowiązku zgłoszenia może zostać potraktowane jako naruszenie obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

**§ 9. Moment rozpoczęcia biegu terminu zgłoszenia naruszenia ochrony danych osobowych**

1. Administrator danych osobowych stwierdza naruszenie ochrony danych osobowych w momencie, gdy uzyskuje wiedzę, że wykryte zdarzenie:

1.1.stanowi incydent bezpieczeństwa informacji;

1.2.dotyczy przetwarzanych danych osobowych;

1.3.może skutkować przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub dostępem do tych danych.

2. Stwierdzenie naruszenia przez Administratora stanowi moment początkowy dla biegu terminu 72 godzin na dokonanie ewentualnego zgłoszenia do organu nadzorczego, zgodnie z art. 33 ust. 1 RODO.

3. Za moment uzyskania uzasadnionych podstaw uznaje się także sytuację, w której Inspektor Ochrony Danych, działając z upoważnienia Burmistrza, poinformuje go o potwierdzonym naruszeniu ochrony danych osobowych.

4. W przypadku wątpliwości co do charakteru zdarzenia, Burmistrz podejmuje niezwłoczne działania w celu ustalenia, czy wystąpiło naruszenie wymagające zgłoszenia do organu nadzorczego.

5. Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania wiąże się ryzyko lub wysokie ryzyko.

**§ 10. Zasady zgłaszania incydentów w ramach współpracy z podmiotami przetwarzającymi**

1. Ze względu na fakt, że incydenty ochrony danych osobowych mogą występować zarówno po stronie administratora, jak i podmiotów przetwarzających, strony zobowiązane są do uzgodnienia jednoznacznych zasad wymiany informacji na temat potencjalnych lub potwierdzonych naruszeń ochrony danych osobowych.

2. W umowie powierzenia przetwarzania danych osobowych należy określić:

2.1.kto jest odpowiedzialny za zgłoszenie naruszenia organowi nadzorczemu i osobom, których dane dotyczą;

2.2.sposób i formę powiadamiania pozostałych stron o incydencie (np. e-mail, telefon, dedykowany formularz);

2.3.maksymalny termin na zgłoszenie incydentu drugiej stronie (np. nie później niż w ciągu 12 godzin od wykrycia);

2.4.zakres przekazywanych informacji, w tym co najmniej: opis naruszenia, kategorie danych i osób, potencjalne skutki oraz podjęte lub planowane środki zaradcze.

3. Celem powyższych ustaleń jest umożliwienie administratorowi niezwłocznego podjęcia działań zaradczych oraz realizacja obowiązków wynikających z RODO, w szczególności w zakresie zgłaszania naruszeń organowi nadzorczemu w terminie 72 godzin.

4. Brak współpracy lub opóźnienie w przekazaniu informacji przez podmiot przetwarzający może zostać uznane za naruszenie postanowień umowy i skutkować odpowiedzialnością kontraktową.

**§ 11. Zasady oceny ryzyka naruszenia ochrony danych osobowych**

1. Administrator danych osobowych jest zobowiązany do dokonania niezwłocznej oceny ryzyka naruszenia ochrony danych osobowych w przypadku zaistnienia incydentu bezpieczeństwa.

2. Aby prawidłowo ocenić ryzyko, należy oszacować:

2.1. wagę potencjalnych konsekwencji dla osób, których dane dotyczą;

2.2. prawdopodobieństwo wystąpienia tych konsekwencji.

3. Ocena ryzyka powinna uwzględniać w szczególności następujące okoliczności danego zdarzenia:

3.1. rodzaj naruszenia ochrony danych osobowych (np. utrata, ujawnienie, dostęp nieuprawniony);

3.2. charakter, wrażliwość i zakres danych osobowych objętych naruszeniem;

3.3. łatwość identyfikacji osób, których dane dotyczą;

3.4. dotkliwość możliwych konsekwencji dla osób, których dane dotyczą (np. utrata reputacji, szkoda majątkowa, dyskryminacja);

3.5. cechy szczególne osób, których dane dotyczą (np. dzieci, osoby starsze, osoby w trudnej sytuacji życiowej);

3.6. cechy szczególne administratora (np. skala przetwarzania danych, profil działalności publicznej);

3.7. liczbę osób, których dane dotyczą.

4. Ocena ryzyka powinna być odpowiednio udokumentowana i przechowywana na wypadek kontroli organu nadzorczego.

5. Administrator musi ustalić, czy naruszenie ochrony danych osobowych może wiązać się z:

5.1. brakiem ryzyka;

5.2. ryzykiem, co wymaga zgłoszenia go Prezesowi UODO;

5.3. wysokim ryzykiem, co oznacza obowiązek zgłoszenia go Prezesowi UODO oraz zawiadomienia osób, których dane dotyczą.

**§ 12. Przypadki niewystępowania ryzyka naruszenia praw i wolności**

1. Administrator, dokonując oceny ryzyka związanego z incydentem ochrony danych osobowych, może uznać, że ryzyko naruszenia praw lub wolności osób fizycznych nie występuje, jeżeli spełnione są określone przesłanki.

2. Do typowych przypadków, w których brak jest ryzyka naruszenia, należą w szczególności:

2.1. ujawnienie danych, które są już publicznie dostępne, a ich ponowne rozpowszechnienie nie powoduje dodatkowego zagrożenia dla osób, których dane dotyczą;

2.2. ujawnienie lub utrata danych osobowych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych – pod warunkiem, że:

2.2.1. dane są zabezpieczone silnym mechanizmem kryptograficznym,

2.2.2. klucz szyfrujący nie został naruszony,

2.2.3. administrator posiada dostęp do integralnej kopii zapasowej danych;

2.3. incydenty, którym administrator skutecznie i definitywnie zaradził przed powstaniem realnego zagrożenia dla osób, których dane dotyczą (np. przywrócenie kontroli nad kontem zanim doszło do odczytu danych przez osobę nieuprawnioną).

3. W przypadkach takich incydentów nie zachodzi obowiązek zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, ani zawiadamiania osób, których dane dotyczą – pod warunkiem, że administrator posiada dokumentację potwierdzającą brak ryzyka.

4. Każdy incydent związany z naruszeniem ochrony danych osobowych wymaga indywidualnej analizy z uwzględnieniem charakteru zdarzenia oraz jego potencjalnych skutków dla osób, których dane dotyczą.

**§ 13. Okoliczności świadczące o wysokim ryzyku naruszenia praw lub wolności osób fizycznych**

1. Administrator danych osobowych, powinien w szczególności zwrócić uwagę na następujące okoliczności, które mogą świadczyć o wysokim ryzyku naruszenia praw lub wolności osób fizycznych. Powyższe dotyczy w szczególności objęcie incydentem szczególnych kategorii danych osobowych, takich jak:

1.1.informacje ujawniające pochodzenie rasowe lub etniczne,

1.2.poglądy polityczne,

1.3.przekonania religijne lub światopoglądowe,

1.4.przynależność do związków zawodowych,

1.5.dane genetyczne i biometryczne,

1.6.dane dotyczące zdrowia, seksualności i orientacji seksualnej,

1.7.informacje o wyrokach skazujących oraz czynach zabronionych,

1.8.dane finansowe oraz dane powszechnie wykorzystywane do potwierdzania tożsamości lub zawierania umów (takie jak numer PESEL, seria i numer dowodu osobistego);

2. szeroki zakres danych osobowych objętych incydentem – im większy zakres, tym większe ryzyko;

3. szczególna dotkliwość potencjalnych skutków incydentu, w tym:

3.1.kradzież tożsamości,

3.2.oszustwa finansowe,

3.3.poważne straty finansowe,

3.4.problemy zawodowe,

3.5.uszczerbek na zdrowiu psychicznym lub fizycznym,

3.6.silny stres, lęk lub obniżone poczucie bezpieczeństwa;

4. szczególny charakter osób objętych incydentem – np. dzieci, osoby starsze, osoby z niepełnosprawnością lub znajdujące się w trudnej sytuacji życiowej;

5. duża liczba osób objętych incydentem – im większa skala naruszenia, tym wyższe prawdopodobieństwo wystąpienia szkód. W przypadku wystąpienia jednej lub kilku z wyżej wymienionych okoliczności, administrator powinien rozważyć konieczność niezwłocznego poinformowania osób, których dane dotyczą, zgodnie z art. 34 RODO.

**§ 14. Zaufany odbiorca danych osobowych**

1. Zaufanym odbiorcą może zostać uznany taki podmiot, który przypadkowo otrzymał dane osobowe, lecz z uwagi na dotychczasową, pozytywną współpracę z administratorem danych osobowych można uznać go za godnego zaufania, a więc takiego, który prawidłowo zareaguje na zaistniały incydent i przyczyni się do ograniczenia ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

2. Aby możliwe było uznanie nieuprawnionego odbiorcy danych osobowych za „zaufanego”, muszą zostać spełnione łącznie następujące warunki:

2.1.podmiot ten pozostaje z administratorem w stałych relacjach organizacyjnych lub współpracy biznesowej, np. jako:

2.1.1.inny dział w strukturze urzędu,

2.1.2.długoletni, sprawdzony dostawca usług,

2.1.3.podmiot przetwarzający działający na podstawie umowy powierzenia, który wykazuje się wysokim poziomem profesjonalizmu i rzetelności;

2.2.administrator danych osobowych zna istotne szczegóły dotyczące tego podmiotu, w szczególności:

2.2.1.jego procedury bezpieczeństwa,

2.2.2.historię współpracy, w tym wcześniejsze, prawidłowe reakcje na incydenty lub sytuacje wymagające podjęcia działań ochronnych.

3. Uznanie danego odbiorcy za „zaufanego" następuje w ramach indywidualnej oceny ryzyka związanego z danym naruszeniem poufności danych osobowych. Oznacza to, że:

3.1.decyzja o nadaniu statusu „zaufanego odbiorcy" nie ma charakteru stałego;

3.2.każdorazowo należy przeprowadzić ocenę ryzyka naruszenia praw lub wolności osób fizycznych;

3.3.status ten należy monitorować i okresowo weryfikować, w tym również w kontekście nowych okoliczności lub incydentów.

4. Jeżeli zmiana okoliczności (np. zmiana praktyk odbiorcy, incydent po jego stronie, naruszenie warunków umowy) prowadzi do utraty zaufania, administrator powinien ponownie ocenić ryzyko i ewentualnie uznać, że dany podmiot nie spełnia już kryteriów „zaufanego odbiorcy".

**§ 15. Obowiązek dokumentowania naruszeń ochrony danych osobowych**

1. Administrator danych osobowych ma obowiązek dokumentować wszystkie stwierdzone naruszenia ochrony danych osobowych.

2. W ramach zasady rozliczalności administrator powinien również dokumentować przypadki incydentów bezpieczeństwa, które zostały zaklasyfikowane jako niebędące naruszeniami danych osobowych, ze szczególnym uwzględnieniem przyczyn takiej decyzji.

3. Dokumentacja może być prowadzona w formie wewnętrznego rejestru naruszeń ochrony danych osobowych. Prowadzenie odrębnej ewidencji nie jest obowiązkowe, jednak wszelkie informacje muszą być:

3.1.wyraźnie oznaczone,

3.2.dostępne do wglądu na żądanie.

4. Dokumentacja naruszeń powinna obejmować co najmniej następujące elementy:

a) okoliczności naruszenia ochrony danych osobowych, w tym:

4.1.data i czas wystąpienia naruszenia,

4.2.moment stwierdzenia naruszenia oraz jego zakończenia,

4.3.sposób wykrycia naruszenia,

4.4.przyczyny naruszenia,

4.5.rodzaj i przebieg naruszenia,

4.6.rodzaj i zakres danych osobowych objętych naruszeniem,

4.7.liczba i kategorie osób, których dane dotyczą;

b) skutki naruszenia, jeśli wystąpiły, oraz możliwe konsekwencje dla osób, których dane dotyczą;

c) uzasadnienie oceny ryzyka związanego z naruszeniem;

d) podjęte działania:

4.8.zaradcze, mające na celu powstrzymanie i ograniczenie skutków naruszenia,

4.9.zapobiegawcze, mające na celu minimalizowanie ryzyka wystąpienia podobnych naruszeń w przyszłości;

e) szczegóły dotyczące zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych (UODO), w tym:

4.10.data zgłoszenia,

4.11.ewentualne przyczyny opóźnienia w zgłoszeniu,

4.12.inne istotne informacje zawarte w zgłoszeniu;

4.13.lub w przypadku braku zgłoszenia – uzasadnienie decyzji o niezgłoszeniu naruszenia Prezesowi UODO;

f) szczegóły dotyczące zawiadomienia osób, których dane dotyczą, o naruszeniu, w tym:

4.14.data zawiadomienia,

4.15.treść zawiadomienia,

4.16.metoda powiadomienia,

4.17.liczba osób powiadomionych;

4.18.lub – w razie braku zawiadomienia – uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą.

5. Dokumentacja naruszeń ochrony danych osobowych powinna być regularnie aktualizowana. Każda nowa informacja dotycząca incydentu, jego skutków lub podjętych działań może wpływać na ocenę ryzyka i wymagać korekty rejestru.

**§ 16. Techniczna realizacja obowiązku zgłaszania naruszeń ochrony danych osobowych na podstawie art. 33 RODO**

1. Techniczna realizacja obowiązku zgłaszania naruszeń ochrony danych osobowych na podstawie art. 33 RODO odbywa się za pośrednictwem kanałów komunikacji wskazanych przez Prezesa Urzędu Ochrony Danych Osobowych (UODO).

2. W ramach realizacji obowiązku zgłaszania naruszeń ochrony danych osobowych wyróżnia się trzy rodzaje zgłoszeń:

2.1.zgłoszenia wstępne – pozwalają na przekazanie podstawowych informacji o incydencie w wymaganym terminie (72 godziny od stwierdzenia naruszenia), z jednoczesnym obowiązkiem późniejszego uzupełnienia danych;

2.2.zgłoszenia uzupełniające – umożliwiają aktualizowanie oraz rozszerzanie informacji o naruszeniu w miarę pozyskiwania nowych danych i szczegółów dotyczących incydentu;

2.3.zgłoszenia kompletne – zawierają wszystkie wymagane informacje już przy pierwszym zgłoszeniu, co pozwala na pełne i wyczerpujące przedstawienie sytuacji bez konieczności późniejszych uzupełnień.

3. Zgłoszenie powinno zawierać:

3.1.podstawowe informacje o administratorze oraz innych podmiotach powiązanych z incydentem, takich jak współadministratorzy, podmioty przetwarzające lub podmioty trzecie;

3.2.okoliczności naruszenia ochrony danych osobowych, w tym m.in. datę i czas wystąpienia naruszenia, moment jego stwierdzenia i zakończenia, sposób wykrycia, przyczyny, rodzaj i przebieg naruszenia oraz rodzaj i zakres danych objętych naruszeniem, a także liczbę i kategorie osób, których dane dotyczą;

3.3.skutki naruszenia lub możliwe skutki dla osób, których dane dotyczą;

3.4.uzasadnienie oceny ryzyka związanego z naruszeniem;

3.5.podjęte działania zaradcze, jeśli zostały wdrożone, lub zaplanowane działania wraz z deklarowaną datą ich realizacji, gdy nie zostały jeszcze podjęte;

3.6.wdrożone środki bezpieczeństwa zapobiegające podobnym incydentom w przyszłości lub zaplanowane środki z deklaracją terminu ich wdrożenia;

3.7.szczegóły dotyczące zawiadomienia osób, których dane dotyczą o naruszeniu – w tym datę, treść, metodę oraz liczbę zawiadomionych osób, albo, jeśli osoby te nie zostały zawiadomione, uzasadnienie takiej decyzji zgodnie z art. 34 ust. 3 RODO;

3.8.imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych (IOD) lub informacji o innym wyznaczonym w organizacji punkcie kontaktowym.

**§ 17. Zawiadamianie osób, których dane dotyczą**

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Administrator nie jest zobowiązany do zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych, nawet jeśli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności tych osób, jeżeli zachodzą przynajmniej jedno z następujących warunków:

2.1.przed wystąpieniem naruszenia zastosowano odpowiednie środki ochrony, które całkowicie eliminują wysokie ryzyko – przykładem może być sytuacja ujawnienia lub utraty danych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych, pod warunkiem że klucz szyfrujący nie został naruszony, a administrator dysponuje kopią zapasową tych danych;

2.2.po wystąpieniu naruszenia administrator natychmiast podjął działania ochronne, które skutecznie wyeliminowały wysokie ryzyko naruszenia praw lub wolności osób, czyli incydent został definitywnie opanowany i zarządzony;

2.3.zawiadomienie osób wymagałoby niewspółmiernie dużego wysiłku, jednakże ten wyjątek obowiązuje tylko wtedy, gdy administrator wyda publiczny komunikat lub w inny, równie skuteczny sposób poinformuje osoby fizyczne o naruszeniu – w takim przypadku zwolnienie dotyczy wyłącznie indywidualnego zawiadomienia.

Załącznik nr 2 do zarządzenia nr 87/2026

Burmistrza Mieroszowa

z dnia 22 kwietnia 2026 r.

**Formularz 22 - Harmonogram szkoleń pracowników Urzędu Miejskiego w Mieroszowie**

| l.p | Szkolenie | | | Zakres |
|---|---|---|---|---|
| 1. | Pierwsze | w związku z rozpoczęciem zatrudnienia | Wszyscy pracownicy | - przepisy powszechnie obowiązujące,<br>- przepis wewnętrzne jednostki,<br>- przepisy w zakresie dotyczącym zajmowanego stanowiska. |
| 2. | Okresowe | min. 1 raz w roku | Wszyscy pracownicy | - zmiany przepisów wewnętrznych jednostki<br>- zmiany przepisów prawnych dotyczących RODO,<br>- zmiany przepisów branżowych, |
| 3. | Incydentalne | w przypadku wystąpienia naruszenia przepisów RODO | Wszyscy pracownicy | - przepisy powszechnie obowiązujące,<br>- przepis wewnętrzne jednostki,<br>- przepisy w zakresie dotyczącym zajmowanego stanowiska |