ZARZĄDZENIE NR 73/19

Wójta Gminy Mrągowo

z dnia 2 kwietnia 2019r.

w sprawie wprowadzenia Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo

Na podstawie *art. 33 i 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 osobowych) (Dz. Urz. UE. L 11 z 4.5.2016);*

Zarządzam, co następuje:

§ 1.

Wprowadza się do stosowania „Procedurę postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo", w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2.

Zobowiązuje się wszystkich pracowników, współpracowników, stażystów oraz praktykantów Urzędu Gminy Mrągowo upoważnionych do przetwarzania danych osobowych do zapoznania się oraz przestrzegania Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

MM

WÓJT

mgr Piotr [illegible]

.....

(data i podpis Administratora Danych Osobowych)

Załącznik do Zarządzenia Nr 73/19 Wójta Gminy Mrągowo z dnia 02.04.2019r. w sprawie wprowadzenia Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo

PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY MRĄGOWO

§ 1.

Ilekroć w niniejszej procedurze użyto określeń:

1) **Administrator Danych Osobowych** – należy przez to rozumieć Urząd Gminy Mrągowo reprezentowany przez Wójta Gminy Mrągowo;

2) **Organ nadzorczy** – należy przez to rozumieć Urząd Ochrony Danych Osobowych;

3) **Jednostce** – należy przez to rozumieć Urząd Gminy Mrągowo;

4) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczcgólnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

5) **Osoba fizyczna** – osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6) **Incydent bezpieczeństwa danych osobowych** – należy przez to rozumieć zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie ochrony danych osobowych;

7) **Naruszenie ochrony danych osobowych** – należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego działania na danych osobowych, do których zaliczają się:

a) Zniszczenie,

b) Utrata,

c) Zmiana,

d) Nieuprawnione ujawnienie,

e) Nieuprawniony dostęp

do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

8) **Poufność** – należy przez to rozumieć zapewnienie, że dane osobowe nie są udostępniane ani ujawniane podmiotom do tego nieuprawnionym;

9) **Integralność** – zapewnienie, że dane osobowe nie zostały zmienione lub zniszczone przez podmioty do tego nieuprawnione.

10) **Rozliczalność** – zapewnienie, że dane osobowe są przetwarzane w sposób zgodny z prawem oraz wykazanie przestrzegania.

§ 2.
Cel procedury

Celem procedury jest określenie sposobu postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych.

§ 3.
Odpowiedzialność

Odpowiedzialność za określenie wielkości ryzyka naruszenia praw i wolności podmiotów, których naruszenie dotyczy oraz podjęcie działań korygujących spoczywa na podmiocie wyznaczonym przez Administratora Danych Osobowych.

§ 4.
Postępowanie w przypadku naruszenia ochrony danych osobowych

W momencie uzyskania informacji o wystąpieniu naruszenia ochrony danych osobowych, podmiot wyznaczony przez Administratora Danych Osobowych ocenia zastałą sytuacje oraz podejmuje działania mające na celu zminimalizowanie wpływu naruszenia na dane osobowe.

§ 5.

1. Do czasu przybycia Inspektora Ochrony Danych Osobowych zgłaszający:

1) zgłasza przełożonemu zaistniały incydent wskazując: datę, godzinę, osobę powiadamiającą o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe), lokalizację zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.), rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu;

2) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie lub naruszenie śladów bądź innych dowodów;

3) zabezpiecza elementy sprzętu komputerowego lub dokumentacji, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;

4) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 6.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Inspektor Ochrony Danych Osobowych po przybyciu na miejsce:

1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu;

2) wysłuchuje relacji osoby, która dokonała powiadomienia;

3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 7.

Inspektor Ochrony Danych Osobowych sporządza z przebiegu zdarzenia sprawozdanie, w którym znajdują się w szczególności informacje o:

1) dacie i godzinie powiadomienia;

2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane;

3) sytuacji, jaką zastał;

4) podjętych działaniach i ich uzasadnieniu;

5) decyzji IOD o tym, czy dany incydent powinien został zgłoszony do UODO czy też nie.

Sporządzone sprawozdanie IOD przekazuje Administratorowi, który po przeanalizowaniu zdarzenia podejmuje ostateczną decyzję o zgłoszeniu, bądź nie do UODO. W przypadku, gdy Administrator ma inne stanowisko niż IOD, przedstawia co do swojej decyzji odpowiednie argumenty.

§ 8.

1. Inspektor Ochrony Danych Osobowych podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:

1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu;

2) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy Inspektor Ochrony Danych Osobowych przekazuje stosowne informacje do Administratora Danych Osobowych, który podejmuje stosowne działania wobec osób, które dopuściły się tego uchybienia.

§ 9.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Inspektora Ochrony Danych Osobowych.

§ 10.

Naruszenie praw i wolności osób, których dane osobowe są przetwarzane

1. Administrator Danych Osobowych dokonuje oceny ryzyka czy wystąpienie naruszenia wiąże się z ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku stwierdzenia naruszenia praw lub wolności osób fizycznych Administrator w stosowny sposób informuje osobę, której dane osobowe są przetwarzane o zaistniałym naruszeniu ochrony danych.
2. Naruszeniem praw i wolności osób, których dane dotyczą będzie m. in.:
1) powstanie uszczerbku fizycznego;
2) powstanie szkód majątkowych lub niemajątkowych u osób fizycznych takich jak:
a) utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw,
b) dyskryminacja,
c) kradzież lub sfałszowanie tożsamości,
d) strata finansowa,
e) nieuprawnione odwrócenie pseudonimizacji,
f) naruszenie dobrego imienia,
g) naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
h) wszelkie inne znaczne szkody gospodarcze lub społeczne.

§ 11.

Ocena ryzyka

1. Podmiot wyznaczony przez Administratora Danych Osobowych dokonuje oceny ryzyka wpływu naruszenia na prawa i wolności osób, których dane dotyczą.
2. Główne kryteria brane pod uwagę przy ocenie stopnia nasilenia naruszenia danych osobowych:
1) **Kontekst Przetwarzania Danych (K)** – okoliczności w jakich Administrator Danych Osobowych przetwarza dane;
2) **Łatwość Identyfikacji (I)** – jak łatwo zidentyfikować daną osobę za pomocą naruszonych danych;
3) **Okoliczności Naruszenia (O)** – w jakich okolicznościach nastąpiło naruszenie danych osobowych.

§ 12.

Kontekst Przetwarzania Danych (K)

Aby określić wynik dla Kontekstu Przetwarzania Danych, osoba wyznaczona przez Administratora Danych Osobowych postępuje zgodnie z następującymi krokami:

1) **Krok 1** – Zdefiniowanie i klasyfikacja rodzajów danych osobowych

2) **Krok 2** – Dostosowanie czynników kontekstowych związanych z przetwarzaniem danych (ocena okoliczności występowania pewnych czynników, które mogłyby zwiększyć lub zmniejszyć punktację podstawową).

§ 13.

Identyfikacja i klasyfikacja rodzajów danych osobowych

1. Podmiot wyznaczony przez Administratora Danych osobowych zidentyfikował i sklasyfikował następujące kategorie danych osobowych i odpowiadające im punkty kontekstowe:

1) **Dane proste** (dane kontaktowe, imię, nazwisko, dane dotyczące edukacji, życia rodzinnego, doświadczenia zawodowego, dane biograficzne itp.)

Okoliczność	Punkty
Wstępny wynik podstawowy: kiedy naruszenie obejmuje dane proste, a Administrator nie jest świadomy żadnych czynników obciążających	**1**
Wynik zostaje zwiększony o 1, np. gdy objętość „prostych danych" i / lub cechy pozwalają na profilowanie poszczególnych osób, lub można uzyskać założenia dotyczące statusu społeczno-finansowego.	2
Wynik zostaje zwiększony o 2, gdy „dane proste" pozwalają na uzyskanie założenia stanu zdrowia, preferencje seksualne, przekonania polityczne lub religijne.	3
Wynik zostaje zwiększony o 3, gdy pewne cechy charakterystyczne osoby (np. grupy wrażliwe, małoletni) mogą	4

być kluczowe dla ich osobistego bezpieczeństwa lub warunków fizycznych / psychologicznych.	

2) **Dane behawioralne** (lokalizacja, dane o ruchu, personalne preferencje, nawyki itp.)

Okoliczność	Punkty
Wstępny wynik podstawowy: jeśli naruszenie obejmuje dane behawioralne, a Administrator nie jest świadomy żadnych czynników obciążających	**2**
Wynik zostaje zmniejszony o 1, gdy natura zbioru danych nie dostarcza istotnych informacji o zachowaniu użytkownika, a dane mogą być zbierane łatwo (niezależnie od naruszenia) za pośrednictwem publicznie dostępnych źródeł (np. połączenie informacji z wyszukiwarek internetowych dotyczące osoby, której dane zostały naruszone)	1
Wynik zostaje zwiększony o 1, jeżeli objętość danych behawioralnych i / lub cech przetwarzanych przez Administratora pozwalają na stworzenie profilu osoby, ujawniając szczególne informacje o swoim życiu codziennym i nawykach	3
Wynik zostaje zwiększony o 2, jeżeli może zostać utworzony profil zawierający dane wrażliwe	4

3) **Dane finansowe** (np. dochody, transakcje finansowe, wyciągi bankowe, faktury itp.)

Okoliczność	Punkty
Wstępny wynik podstawowy: jeśli naruszenie obejmuje dane finansowe, a Administrator nie jest świadomy żadnych czynników obciążających	**3**
Wynik zostaje zmniejszony o 2, jeżeli natura zbioru nie dostarcza istotnych informacji finansowych danej osoby (np. fakt, że dana osoba jest klientem danego	1

banku)	
Wynik zostaje zmniejszony o 1, np. gdy konkretny zestaw danych zawiera pewne informacje finansowe, ale nadal nie dostarcza istotnych informacji na temat sytuacji finansowej / życiowej (np. numery kont bankowych bez dodatkowej informacji)	2
Wynik zostaje zwiększony o 1, gdy ze względu na charakter i / lub objętość określonego zbioru danych, umożliwia stworzenie szczegółowego profilu społeczno-finansowego osoby, której dane dotyczą	4

4) **Dane szczególnej kategorii** (dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, zdrowia, seksualności lub orientacji seksualnej, wyroków skazujących)

Okoliczność	Punkty
Wstępny wynik podstawowy: jeśli naruszenie obejmuje dane wrażliwe, a Administrator nie jest świadomy żadnych czynników obciążających	**4**
Wynik może zostać zmniejszony o 3, np. gdy natura zbioru nie dostarcza istotnych informacji o zachowaniu osób, których dane zostały naruszone, a dane mogą zostać łatwo zebrane (niezależnie od naruszenia) za pośrednictwem publicznie dostępnych źródeł (np. połączenie informacji z wyszukiwarek internetowych)	1
Wynik może zostać zmniejszony o 2, np. gdy charakter danych może prowadzić wyłącznie do ogólnych założeń	2
Wynik może zostać zmniejszony o 1, np. gdy natura danych może prowadzić wyłącznie do założeń dotyczących poufnych informacji	3

2. W momencie, kiedy naruszeniu ulegają dane wielu kategorii, jako wynik Kontekstu Przetwarzania Danych (K) wykorzystujemy najwyższy wynik.

§ 14.
Łatwość Identyfikacji (I)

1. Łatwość Identyfikacji jest definiowana na jednym z czterech poziomów:

1) **I = 0,25** (poziom nieistotny), np. w przypadku: imienia i nazwiska, które występują znacznie w skali całego kraju; numeru paszportu nie powiązanego z żadnymi dodatkowymi informacjami umożliwiającymi wykorzystanie danej w kontekście; adresu poczty elektronicznej, którego nazwa nie zdradza żadnych dodatkowych danych o osobie, której dane dotyczą; nieostre zdjęcie.

2) **I = 0,5** (poziom ograniczony), np. w przypadku: imienia i nazwiska, które występują rzadko w skali całego kraju; numeru telefonu, gdzie identyfikacja jest możliwa poprzez bezpośrednią komunikację; zdjęcia, które jest nieostre ale umożliwia identyfikację miejsca w którym zostało zrobione.

3) **I = 0,75** (poziom znaczący), np. w przypadku: imienia i nazwiska, które występują rzadko w skali danego miasta; numeru PESEL, który umożliwia uzyskanie informacji o dacie urodzenia; adresu poczty elektronicznej, którego nazwa wskazuje na imię i nazwisko, ale dzięki któremu nie da się uzyskać dodatkowych informacji poprzez wyszukiwarki internetowe; zdjęcia wysokiej jakości, które jednak nie wskazuje na okoliczności wykonania zdjęcia poprzez np. unikatowość miejsca, w którym zostało zrobione.

4) **I = 1** (poziom maksymalny), np. w przypadku: imienia i nazwiska, które w połączeniu z datą urodzenia jednoznacznie wskażą daną osobę; numeru PESEL uzyskanego razem z imieniem i nazwiskiem; numeru telefonu, który jest zarejestrowany w ogólnodostępnym rejestrze; adresie poczty elektronicznej, którego nazwa wskazuje na dodatkowe dane takie jak imię, nazwisko oraz może posłużyć do uzyskania dodatkowych informacji za pośrednictwem wyszukiwarek internetowych; zdjęcia wysokiej rozdzielczości, które umożliwia identyfikację osoby na nim się znajdującej wraz z miejscem w którym zostało zrobione, lub okolicznościami wykonania zdjęcia.

2. W momencie, kiedy naruszeniu ulegają dane wielu kategorii, jako wynik Łatwości Identyfikacji (I) wykorzystujemy najwyższy wynik.

§ 15.

Okoliczności Naruszenia (O)

Elementami analizowanymi w ramach określania Okoliczności Naruszenia jest utrata bezpieczeństwa (**poufność, integralność, dostępność**) oraz złego zamiaru i uzupełniają Kontekst Przetwarzania Danych i Łatwość Identyfikacji w następujący sposób:

1) **Utrata poufności** (występuje wtedy, gdy informacje są dostępne dla stron, które są nieupoważnione lub nie maja prawnie do tego celu dostępu)

Naruszenie danych bez zaistnienia dowodów na nielegalne przetwarzanie	0
Udostępnienie danych znanej liczbie określonej odbiorców	+ 0,25
Udostępnienie danych nieznanej ilości odbiorów	+ 0,5

2) **Utrata integralności** (występuje wtedy, gdy oryginalne dane są zmienione i podstawione)

Zmiana danych bez zidentyfikowanego nieprawidłowego lub nielegalnego użycia	0
Zmiana danych wraz z możliwością ich nieprawidłowego lub nielegalnego wykorzystania, ale przy możliwości odzyskania oryginalnych informacji	+ 0,25
Zmiana danych wraz z możliwością ich nieprawidłowego lub nielegalnego użycia, bez możliwości odzyskania oryginalnych informacji	+ 0,5

3) **Utrata dostępności** (występuje wtedy, gdy nie można uzyskać oryginalnych danych, wtedy, gdy istnieje do dostępu potrzeba. Może to być czasowe lub trwałe)

Utrata danych, możliwych do odzyskania bez żadnych trudności	0
Tymczasowa niedostępność danych	+ 0,25
Kompletna niedostępność (bez możliwości odzyskania danych)	+ 0,5

§ 16.

Obliczanie ciężkości

1. Obliczanie wysokość poziomu ryzyka dla praw i wolności osób, których dane dotyczą, podmiot wyznaczony należy skorzystać z następującego wzoru:

$$R = K \times I + O$$

Poziom Ryzyka = Kontekst Przetwarzania Danych x Łatwość Identyfikacji + Okoliczności Naruszenia

2. Podmiot wyznaczony przez Administratora Danych Osobowych dokonuje oceny ryzyka wpływu naruszenia na prawa i wolności osób, których dane dotyczą.
3. Końcowy wynik pokazuje poziom ciężkości danego naruszenia.

Poziom ryzyka wpływu naruszenia na prawa i wolności, których dane dotyczą		
$R < 2$	**Mały**	Osoby, których dane zostały naruszone nie odczują tego skutku, bądź spotkają się z nielicznymi niedogodnościami, nie stanowiącymi większego problemu (np. czas poświęcony na ponowne wprowadzenie danych, rozdrażnienie, irytacja)
$2 \leq R < 4$	**Średni**	Osoby, których dane zostały naruszone mogą napotkać znaczne niedogodności, które będą w stanie pokonać pomimo kilku trudności (np. dodatkowe koszty, niemożność korzystania z usług biznesowych, strach, brak zrozumienia, stres, dolegliwości fizyczne itp.)
$4 \leq R$	**Wysoki**	Osoby, których dane zostały naruszone mogą napotkać znaczne, konsekwencje, których nie mogą pokonać (trudności finansowe, takie jak czarne listy banków, dług, szkody materialne lub niemożność pracy, długoterminowe dolegliwości psychologiczne, itp.)

§ 17.

Notyfikacja organu nadzorczego

1. Jeżeli po przeprowadzonej ocenie, istnieje ryzyko naruszenia praw i wolności osób fizycznych, Administrator Danych zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.
2. Zgłoszenie naruszenia przez Administratora Danych następuje elektronicznie za pomocą odpowiedniego formularza dostępnego na stronie internetowej pod adresem https://uodo.gov.pl/pl/134/233
3. Wzór zgłoszenia naruszenia stanowi **wzór nr 1.**
4. Jeżeli w przypadku wejścia w posiadanie nowych informacji nastąpiła zmiana opisywanej sytuacji lub administrator zastosował dodatkowe środki, administrator zgłasza bez zbędnej zwłoki wszystkie nowe informacji organowi nadzorczemu.
5. Administrator danych dokumentuje wszystkie naruszenia ochrony danych, w tym jego okoliczności, skutki oraz podjęte działania zaradcze, zgodnie **z wzorem nr 2.**
6. Rejestr naruszeń prowadzony jest w formie elektronicznej oraz papierowej.

§ 18.

W zawiadomienie osób fizycznych, których dane zostały naruszone

1. Jeżeli po przeprowadzonej ocenie, poziom ryzyka wpływu naruszenia na prawa i wolności osób, których dane zostały naruszone został określony jako wysoki, Administrator Danych prostym i jasnym językiem zawiadamia bez zbędnej zwłoki osoby, których dane osobowe zostały naruszone.
2. W zależności od ilości osób, których dane zostały naruszone, Administrator Danych Osobowych zawiadamia podmioty, których dane dotyczą poprzez:
1) Pisemnie, korespondencyjnie, na znany nam adres podmiotu (wzór pisemnego zgłoszenia określa **wzór nr 3**);
2) W przypadku braku możliwości korespondencyjnego zawiadomienia, Administrator Danych Osobowych wykorzystuje posiadane możliwości zawiadomienia (np. telefonicznie, drogą elektroniczną);
3) Wydanie publicznego komunikatu (wzór publicznego komunikatu określa **wzór nr 4)**

§ 19.

Działania zaradcze

Administrator Danych Osobowych wyznacza podmiot do podjęcia działań zaradczych w celu zmniejszenia ryzyka ponownego wystąpienia naruszenia ochrony danych osobowych.

Wzór Nr 1

Zgłoszenie naruszenia ochrony danych osobowych

1. Dane wnioskodawcy

A. Podaj typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

- ○ Zgłoszenie kompletne/jednorazowe
- ◉ Zgłoszenie wstępne
- ○ Zgłoszenie uzupełniające/zmieniające

Podaj datę poprzedniego zgłoszenia

Kliknij tutaj, aby wprowadzić datę.

2. Podmiot zgłaszający

A. Dane administratora danych

Pełna nazwa administratora	Kliknij tutaj, aby wprowadzić tekst.
REGON – jeśli został podany (opcjonalnie)	Kliknij tutaj, aby wprowadzić tekst.
Sektor (opcjonalnie)	Dla sektora publicznego: Wybierz element. / Dla sektora prywatnego: Wybierz element.

B. Adres siedziby administratora danych

Państwo	Kliknij tutaj, aby wprowadzić tekst.	Miejscowość	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Ulica	Kliknij tutaj, aby wprowadzić tekst.
Powiat	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer / Numer lokalu: Podaj numer

C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk +, który pojawi się po prawej stronie)

D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal biznes.gov.pl.
Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

E. Inspektor ochrony danych

Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.
Numer telefonu	Kliknij tutaj, aby wprowadzić tekst.
Adres e-mail	Kliknij tutaj, aby wprowadzić tekst.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logow systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

☐ Trwające naruszenie
Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

C. Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

A. Charakter

☐ Naruszenie poufności danych

Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych

Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych

Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

B. Na czym polegało naruszenie?

☐ Zgubienie lub kradzież nośnika/urządzenia

☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ Nieuprawnione uzyskanie dostępu do informacji

☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ Niezamierzona publikacja

☐ Dane osobowe wysłane do niewłaściwego odbiorcy

☐ Ujawnienie danych niewłaściwej osoby

☐ Ustne ujawnienie danych osobowych

Opisz na czym polegało naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

C. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznane)

Kliknij tutaj, aby wprowadzić tekst.

4.1. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzą: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub haszowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu

Kliknij tutaj, aby wprowadzić tekst.

B. Dane podstawowe

☐ Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

☐ Krajowy numer identyfikacyjny

np. PESEL, SSN

☐ Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

☐ Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

☐ Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

☐ Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

☐ Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

C. Dane szczególnej kategorii

☐ Dane o pochodzeniu rasowym lub etnicznym

☐ Dane o poglądach politycznych

☐ Dane o przekonaniach religijnych lub światopoglądowych

☐ Dane o przynależności do związków zawodowych

☐ Dane dotyczące seksualności lub orientacji seksualnej

☐ Dane dotyczące zdrowia

☐ Dane genetyczne

☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

D. Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących

☐ Dane dotyczące czynów zabronionych

☐ Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

E. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

4.2. Kategorie osób

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie osób, których dane dotyczą

☐ Pracownicy

☐ Użytkownicy

☐ Subskrybenci

☐ Studenci

☐ Uczniowie

☐ Służby mundurowe (np. wojsko, policja)

☐ Klienci (obecni i potencjalni)

☐ Klienci podmiotów publicznych

☐ Pacjenci

☐ Dzieci

☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie.

Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób, których mogło dotyczyć naruszenie — Kliknij tutaj, aby wprowadzić tekst.

5. Środki bezpieczeństwa zastosowane przed naruszeniem

A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem (opcjonalnie)

Kliknij tutaj, aby wprowadzić tekst.

6. Możliwe konsekwencje

A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- ☐ Utrata kontroli nad własnymi danymi osobowymi
- ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- ☐ Ograniczenie możliwości realizowania praw
- ☐ Dyskryminacja
- ☐ Kradzież lub sfałszowanie tożsamości
- ☐ Strata finansowa
- ☐ Naruszenie dobrego imienia
- ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

B. Ryzyko naruszenia praw i wolności osób fizycznych

- ○ Niskie
- ◉ Średnie
- ○ Wysokie

7. Środki zaradcze

A. Komunikacja z osobami, których dane dotyczą

Czy osoby, których dane dotyczą, zostały powiadomione o naruszeniu?

(•) Tak

( ) Nie, ale zostaną powiadomione

( ) Nie, nie zostaną powiadomione

( ) Nie oceniłem jeszcze

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić podmioty danych, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

Czy indywidualnie?

( ) Tak

( ) Nie, gdyż indywidualne powiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został wydany publiczny komunikat lub zastosowano podobny środek, za pomocą którego osoby, których dane dotyczą, zostały poinformowane w równie skuteczny sposób.

Wskaż datę kiedy osoby, których dane dotyczą, zostały powiadomione o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

Wskaż datę kiedy zamierzasz powiadomić osoby, których dane dotyczą, o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

☐ Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą

Liczba zawiadomionych osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Powód niezawiadomienia osób, których dane dotyczą:

( ) Przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych

( ) Po naruszeniu zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

Opis tych środków

Kliknij tutaj, aby wprowadzić tekst.

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Treść zawiadomienia

Kliknij tutaj, aby wprowadzić tekst.

B. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.

Kliknij tutaj, aby wprowadzić tekst.

C. Transgraniczne przetwarzanie i inne powiadomienia

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE (opcjonalnie)

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Litwa	☐ Luksemburg
☐ Łotwa	☐ Malta	☐ Niemcy	☐ Portugalia
☐ Rumunia	☐ Słowacja	☐ Słowenia	☐ Szwecja
☐ Węgry	☐ Wielka Brytania	☐ Włochy	

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu spoza UE (opcjonalnie)

Wymień inne organy nadzorcze spoza UE, którym naruszenie zostało lub zostanie zgłoszone

Kliknij tutaj, aby wprowadzić tekst.

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE z powodu innych zobowiązań prawnych (opcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

Kliknij tutaj, aby wprowadzić tekst.

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO[1], a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza wniosku na platformie E-PUAP oraz Wojewoda Podlaski w związku z korzystaniem przez Prezesa UODO z systemu elektronicznego zarządzania dokumentacją (EZD PUW).

Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 i art. 58 ust. 2 RODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

---

[1] 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 (RODO) oraz podjętych działań.

Wzór nr 2 do Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Lp.	Data wystąpienia naruszenia	Rodzaj naruszenia	Kategoria osób, których dane zostały naruszone wraz z kategorią naruszonych danych osobowych	Okoliczności naruszenia	Skutki naruszenia	Pracownik zgłaszający incydent	Powiadomienie osób, których dane dotyczą o zaistniałym incydencie TAK?NIE	Podpis Administratora/ IOD

Wzór nr 3 do Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo

.....
(miejscowość, data)

Urząd Gminy Mrągowo
Ul. Królewiecka 60A
11-700 Mrągowo

Do:
.....
.....
.....

ZGŁOSZENIA W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Zgodnie z art. 34 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu . . . . . w Urzędzie Gminy Mrągowo.

Zgłoszenie te ma na celu umożliwienie podjęcia niezbędnych działań zapobiegawczych w celu minimalizacji potencjalnych niekorzystnych skutków naruszenia.

1.	Charakter naruszenia ochrony danych:	
3.	Kategoria danych osobowych, które uległy naruszeniu:	
4.	Możliwe konsekwencje naruszenia ochrony danych:	
5.	Zalecenia co do minimalizacji potencjalnych niekorzystnych skutków:	
6.	W celu uzyskania dodatkowych wyjaśnień, proszę o kontakt z:	

.....
(czytelny podpis Administratora Danych)

Wzór nr 4 do Procedury postępowania w przypadku naruszenia ochrony danych osobowych w Urzędzie Gminy Mrągowo

ZGŁOSZENIA W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Zgodnie z art. 34 ogólnego rozporządzenia o ochronie danych, informuję iż doszło do naruszenia ochrony danych osobowych, które miało miejsce w dniu . . . . . w Urzędzie Gminy Mrągowo.

Zgłoszenie te ma na celu umożliwienie podjęcia niezbędnych działań zapobiegawczych w celu minimalizacji potencjalnych niekorzystnych skutków naruszenia.

Charakter naruszenia miał postać . . . . . .

Naruszeniu ochrony danych osobowych uległy dane . . . . . (określić kategorię osób, których dane uległy naruszeniu wraz z kategoriami danych osobowych).

Możliwymi konsekwencjami zaistniałego naruszenia są . . . . . .

W celu zminimalizowania potencjalnych skutków naruszenia zaleca się . . . . . .

W celu uzyskania dodatkowych wyjaśnień, proszę o kontakt z:

.....

(czytelny podpis Administratora Danych)