ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Koronowska
89-400 Sępólno Krajeńskie
tel. (052)
NIP 561-133-30-37

Załącznik Nr 3
zarządzenia Nr **ZD – PO.120.19.2021.AK** dyrektora
Zarządu Drogowego w Sępólnie Krajeńskim
z dnia **30 grudnia 2021** r.
w sprawie wprowadzenia w życie dokumentacji
związanej z przetwarzaniem i ochroną danych osobowych
w Zarządzie Drogowym w Sępólnie Krajeńskim.

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Zarządzie Drogowym w Sępolnie Krajeńskim

Sępólno Krajeńskie, grudzień 2021.

Spis treści:

Wykaz załączników:

Załącznik nr 1 – Raport z naruszenia ochrony danych;
Załącznik nr 2 - Rejestr bezpieczeństwa, działań naprawczych i zapobiegawczych;
Załącznik nr 3 - Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu.

Rozdział 1
Naruszenie danych osobowych

§ 1. Ilekroć w niniejszej Procedurze mowa jest o:

1) **Administratorze Danych Osobowych (ADO) lub Administratorze** – należy przez to rozumieć Zarząd Drogowy w Sępólnie Krajeńskim reprezentowany przez dyrektora ZD;
2) **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć osobę powołaną przez ADO zgodnie z „Polityką bezpieczeństwa i ochrony danych osobowych w Zarządzie Drogowym w Sępólnie Krajeńskim";
3) **Jednostce lub ZD** - należy przez to rozumieć Zarząd Drogowy w Sępólnie Krajeńskim.
4) **Administratorze Systemu Informatycznego (ASI)** – należy przez to rozumieć osobę wyznaczona przez ADO oraz posiadającą uprawnienia do zarządzania zasobami sieci i systemów informatycznych;
5) **Incydencie** (w zakresie danych osobowych) – należy przez to rozumieć sytuacje powodującą utratę poufności, integralności lub dostępności przetwarzanych danych.
6) **Danych osobowych** – należy przez to rozumieć informacje o zidentyfikowanego lub możliwej do zidentyfikowania osobie fizycznej;
7) **Procedurze** – należy przez to rozumieć „Procedurę postępowania w sytuacji naruszenia ochrony danych osobowych w Zarządzie Drogowym w Sępolnie Krajeńskim;
8) **Systemach informatycznych** – należy przez to rozumieć zespół systemów komputerowych, sieci i oprogramowania służących do przetwarzania danych osobowych.

§ 2. Naruszenie danych osobowych jest to każda sytuacja, w której stwierdzono fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zebrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego a w szczególności:

1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;
4) nielegalne ujawnianie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

Rozdział 2
Postępowanie w przypadku naruszenia danych osobowych

§ 3. Każdorazowe stwierdzenie lub podejrzenie naruszenia danych osobowych musi być niezwłocznie zgłoszone bezpośredniemu przełożonemu, który następnie obowiązany jest przekazać taką informacje Inspektorowi Ochrony Danych.

§ 4. Przykładowe sytuacje podlegające zgłoszeniu Inspektorowi Ochrony Danych:

1) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnie;
2) stwierdzenie próby modyfikacji danych lub zmian w strukturze danych bez odpowiedniego upoważnienia;
3) kradzież komputerów lub twardych dysków zawierających dane osobowe;
4) hasła do komputerów i programów zawierających dane osobowe przechowywane w sposób niezabezpieczony w pobliżu komputerów użytkowników;
5) stwierdzenie wystąpienia wirusów komputerowych niezneutralizowanych przez programy antywirusowe lub niestandardowa praca komputerów;
6) ślady na drzwiach, oknach i szafach z dokumentacją świadczące o próbie włamania;
7) niszczenie dokumentacji papierowej w inny sposób niż przy użyciu niszczarki;
8) wynoszenie danych osobowych w wersji papierowej lub elektronicznej poza teren jednostki bez upoważnienia Administratora Danych Osobowych;
9) obecność w budynku lub w pomieszczeniach, w których przechowywane są dane osobowe, osób budzących podejrzenia;
10) istnienie nieautoryzowanych kont dostępu do systemów informatycznych zawierających dane osobowych;
11) zewnętrzne próby wyłudzenia danych osobowych;
12) nieprawidłowości w zakresie zabezpieczeń miejsc przechowywania danych osobowych oraz na nośnikach elektronicznych.
13) niewłaściwe zachowanie pracowników zagrażające bezpieczeństwu danych osobowych.

§ 5. Wszyscy pracownicy Zarządu Drogowego mają obowiązek w przypadku stwierdzenia naruszenia danych osobowych podjąć czynności dążące do powstrzymania skutków naruszenia oraz zabezpieczyć dowody naruszenia.

§ 6. Administrator Systemu Informatycznego zobowiązany jest do informowania Inspektora Ochrony Danych o wszelkich anomaliach w pracy nad administrowanymi przez siebie urządzeniami, mogącymi być przyczyną lub skutkiem incydentu w zakresie ochrony danych osobowych.

§ 7. Inspektor Ochrony Danych w sytuacji naruszenia ochrony danych zobowiązany jest do:

1) zapoznania się z zaistniałą sytuacją;
2) ustalenia sposobu postępowania, biorąc pod uwagę zagrożenia w prawidłowości i ciągłości pracy;
3) przeprowadzania wywiadu w związku z zaistniałą sytuacją z osobą, która dopatrzyła się naruszenia oraz z innymi osobami posiadającymi informacje w sprawie naruszenia;
4) uzyskania opinii specjalistów zewnętrznych, gdy zachodzi taka potrzeba.

§ 8. Inspektor Ochrony Danych opisuje zaistniały przypadek naruszenia ochrony danych osobowych poprzez sporządzenie raportu **(zał. Nr 1)**.

§ 9. IOD po uzyskaniu niezbędnych opinii wprowadza działania naprawcze i ustosunkowuje się do kwestii ewentualnego otworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych w jednostce. Inspektor Ochrony Danych prowadzi rejestr bezpieczeństwa, działań naprawczych i zapobiegawczych **(zał. Nr 2)**.

Rozdział 3
Naruszenie danych osobowych a odpowiedzialność

§ 10. W stosunku do osoby, która nie zastosowała się do przepisów zawartych w niniejszej Procedurze a w szczególności nie powiadomiła właściwej osoby zgodnie z zasadami, wszczyna się postępowanie dyscyplinarne. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych.

§ 11. Kara dyscyplinarna nałożona na pracownika uchylającego się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej zgodnie z obowiązującymi przepisami oraz możliwości wniesienia wobec tego pracownika powództwa cywilnego przez pracodawcę.

Rozdział 4
Zgłoszenie organowi nadzorczemu faktu naruszenia ochrony danych osobowych

§ 12. Administrator w sytuacji naruszenia ochrony danych osobowych, zobowiązany jest bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadomić Prezesa Urzędu Ochrony Danych. Zgłoszenie nie jest wymagane, gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Wzór zgłoszenia stanowi **załącznik Nr 3** do niniejszej Procedury.

§ 13. W sytuacji, gdy dokonuje się zgłoszenia organowi nadzorczemu naruszenia ochrony danych, po upływie 72 godzin od naruszenia, do zgłoszenia należy dołączyć wyjaśnienie przyczyn opóźnienia.

§ 14. Zgłoszenie naruszenia ochrony danych osobowych zawiera:

1) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
2) opisywać charakter naruszenia ochrony danych osobowych w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 15. Administrator obowiązany jest dokumentować wszelkie naruszenia ochrony danych, opisując jednocześnie okoliczności i skutki naruszenia ochrony danych osobowych oraz podjęte działania zapobiegające możliwym naruszeniom.

Rozdział 5
Zawiadomienie o naruszeniu ochrony danych osobowych

§ 16. Administrator zobowiązany jest bez zbędnej zwłoki zawiadomić osobę, której dane zostały naruszone, gdy wystąpi prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności tej osoby fizycznej. Zawiadomienie w sposób jasny i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera co najmniej informacje zawarte w § 14 ust. 1, 3 i 4.

§ 17. Zawiadomienie opisane w § 16 nie jest wymagane w następujących przypadkach:

1) administrator zastosował właściwe techniczne i organizacyjne środki ochrony, zastosowane do danych osobowych objętych naruszeniem w szczególności środki takie jak szyfrowanie, uniemożliwiające osobom nieupoważnionym odczyt danych osobowych;
2) administrator wdrożył środki wykluczające prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
3) zawiadomienie wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku ogłaszany zostaje publiczny komunikat lub zastosowany zostaje podobny środek za pomocą, którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

ZARZĄDU DROGOWEGO

Załącznik Nr 1
do Procedury postępowania
w sytuacji naruszenia ochrony
danych osobowych
w Zarządzie Drogowym
w Sępólnie Krajeńskim.

Raport z naruszenia ochrony danych

1. Data naruszenia: ....., godzina naruszenia: .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub posiadające niezbędne informacje w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):
   .....
   .....
   .....

3. Lokalizacja zdarzenia (np. nr pokoju, określenie pomieszczenia, nr komputera, nazwa programu lub aplikacji itp.):
   .....
   .....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
   .....
   .....
   .....

5. Podjęte działania:
   .....
   .....
   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:
   .....
   .....

7. Postępowanie wyjaśniające i naprawcze:
   .....
   .....

....
(podpis pracownika) (data i podpis Inspektora Ochrony Danych)

Załącznik Nr 2
do Procedury postępowania
w sytuacji naruszenia ochrony
danych osobowych
w Zarządzie Drogowym
w Sępólnie Krajeńskim.

Rejestr bezpieczeństwa, działań naprawczych i zapobiegawczych

Opis incydentu	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Osoba odpowiedzialna za realizacje	Przyczyna powstania incydentu	Działania podjęte w celu przywrócenia bezpieczeństwa	Ocena działań korygujących

Załącznik Nr 3
do Procedury postępowania
w sytuacji naruszenia ochrony
danych osobowych
w Zarządzie Drogowym
w Sępólnie Krajeńskim.

.....
(pieczęć jednostki)

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Naruszenie ochrony danych osobowych miało miejsce w Zarządzie Drogowym w Sępólnie Krajeńskim na ulicy Koronowskiej 5, w dniu ..... o godzinie .....

2. Dane osoby powiadamiającej o naruszeniu (imię, nazwisko, stanowisko służbowe):
   .....,
   dane osób zaangażowanych lub posiadających informacje w związku z naruszeniem (imię, nazwisko, stanowisko służbowe) .....
   .....
   .....

3. Lokalizacja zdarzenia (np. nr pokoju, określenie pomieszczenia, nr komputera, nazwa programu lub aplikacji itp.):
   .....
   .....

4. Charakter naruszenia ochrony danych osobowych, wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorie i liczbę wpisów danych osobowych, których dotyczy naruszenie:
   .....
   .....
   .....

5. Podjęte działania:
   .....
   .....

6. Konsekwencje naruszenia ochrony danych osobowych:
   .....
   .....

7. Środki zastosowane lub proponowane przez Administratora Danych Osobowych w celu zapobiegania naruszeniom danych osobowych oraz środki wprowadzone w celu zminimalizowania ewentualnych negatywnych skutków:

   .....
   .....
   .....

8. Imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych:

   .....
   .....

.....
(podpis Administratora Danych Osobowych)