ZARZĄDZENIE NR GKG.GPK.0200.21.2021
DYREKTORA POWIATOWEGO OŚRODKA DOKUMENTACJI
GEODEZYJNEJ I KARTOGRAFICZNEJ z dnia 3 marca 2021r.

w sprawie: reagowania w przypadku naruszenia ochrony danych osobowych Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej jako Podmiotu przetwarzającego

Na podstawie §10 ust. 3 pkt 1 Regulaminu Organizacyjnego Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej przyjętego Uchwałą Zarządu Powiatu w Poznaniu nr 1860/2020 z dnia 21 grudnia 2020 r. zarządzam, co następuje:

§1
Postanowienia ogólne
1. Zarządzenie określa sposób postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych lub powzięcia podejrzenia o wystąpieniu takiego naruszenia.
2. Zarządzenie przedstawia przypadek gdy naruszenie ochrony danych osobowych dotyczy naruszenia bezpieczeństwa zbioru danych osobowych dla, których Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej w Poznaniu, w rozumieniu art. 4 pkt. 8 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 (dalej RODO) jest Podmiotem przetwarzającym.
3. Ilekroć w zarządzeniu jest mowa o:
1) Administratorze Danych - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2) Administratorze Systemów Informatycznych PODGiK w Poznaniu - rozumie się przez to osobę wyznaczoną w PODGiK w Poznaniu w celu nadzorowania i zapewnienia prawidłowego funkcjonowania systemów informatycznych,
3) Inspektorze Ochrony Danych - rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony danych osobowych,
4) Inspektorze Ochrony Danych PODGiK w Poznaniu - rozumie się przez to osobę wyznaczoną w PODGiK w Poznaniu w celu nadzorowania i przestrzegania zasad ochrony danych osobowych,
5) naruszeniu ochrony danych osobowych - rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
6) PODGiK - Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej.
7) Podmiocie przetwarzającym - rozumie się przez to PODGiK w Poznaniu, reprezentowany przez Dyrektora PODGiK w Poznaniu tj. osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych.
4. Przestrzeganie postanowień niniejszego Zarządzenia służy właściwemu reagowaniu na przypadki naruszeń ochrony danych osobowych w PODGiK w Poznaniu w sytuacji gdy PODGiK w Poznaniu występuje jako Podmiot przetwarzający.

5. Zarządzenie ma zastosowanie do wszystkich danych osobowych niezależnie od formy, w jakiej są przechowywane (elektronicznej, papierowej).
6. Naruszeniem ochrony danych osobowych może być w szczególności:
1) Infekcja złośliwego oprogramowania w systemie informatycznym PODGiK w Poznaniu,
2) Ujawnienie haseł dostępu do systemów informatycznych PODGiK w Poznaniu,
3) Przełamanie zabezpieczeń informatycznych systemów informatycznych PODGiK w Poznaniu,
4) Nieuprawniona obserwacja i analiza ruchu w sieci PODGiK w Poznaniu,
5) Modyfikacja/usunięcie danych osobowych bez uprawnienia,
6) Kradzież/zgubienie dokumentów lub nośników z danymi osobowymi,
7) Nieuprawnione uszkodzenie/zniszczenie danych osobowych,
8) Ujawnienie danych osobowych osobom nieuprawnionym,
9) Wyciek danych osobowych,
7. Polityka bezpieczeństwa funkcjonująca w PODGiK w Poznaniu wskazuje formy naruszeń ochrony danych osobowych w PODGiK w Poznaniu oraz sposoby postępowania w przypadku wystąpienia zagrożenia. Przedstawiono tam przykłady możliwych naruszeń w sposób przystępny dla osób pracujących na danych osobowych oraz opisano wstępne czynności jakie niezwłocznie należy podjąć w momencie wystąpienia zagrożenia.
8. Niniejsze zarządzenie opisuje dalsze działania, które należy podjąć po powzięciu informacji o możliwym wystąpieniu naruszenia ochrony danych osobowych.

§2
Reagowanie na naruszenie ochrony danych osobowych
1. Każde wystąpienie naruszenia ochrony danych osobowych wymaga odpowiedniej reakcji, w tym w szczególności poinformowania o wystąpieniu naruszenia Inspektora Ochrony Danych PODGiK w Poznaniu, a w sytuacjach gdy zdarzenie dotyczy zagadnień z obszaru informatycznego również Administratora Systemów Informatycznych PODGiK w Poznaniu.
2. Inspektor Ochrony Danych PODGiK w Poznaniu ma obowiązek poinformowania o możliwości wystąpienia naruszenia ochrony danych osobowych Podmiot przetwarzający.
3. Po powzięciu informacji o możliwości wystąpienia naruszenia ochrony danych osobowych niezwłocznie podejmuje się czynności zaradcze, minimalizujące ryzyko i skutki incydentu oraz takie, które pozwolą na powrót do stabilnego stanu.
4. Podmiot przetwarzający uruchamia zespół szybkiego reagowania (dalej Zespół), w skład którego wchodzi:
1) Inspektor Ochrony Danych PODGiK w Poznaniu,
2) Administrator Systemów Informatycznych PODGiK w Poznaniu jeśli zdarzenie dotyczy zagadnień z obszaru informatycznego,
3) Wyznaczeni przez Podmiot przetwarzający Kierownicy Wydziałów, których obecność w Zespole zostanie wykazana w sprawozdaniu, o którym mowa w ust. 6 pkt 5,
4) Wyznaczeni przez Kierowników Wydziałów i/lub Podmiot przetwarzający inni pracownicy, których obecność w Zespole zostanie wykazana w sprawozdaniu, o którym mowa w ust. 6 pkt 5.
5. Zespół analizuje zdarzenie w celu ustalenia czy doszło do naruszenia ochrony danych osobowych.
6. Jeżeli doszło do naruszenia ochrony danych osobowych, to:
1) Inspektor Ochrony Danych PODGiK w Poznaniu powiadamia o wynikach analizy, o której mowa w ust. 5 Podmiot przetwarzający,
2) Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych

bez zbędnej zwłoki zgłasza je Administratorowi Danych,
3) Zespół niezwłocznie przygotowuje wstępne zgłoszenie do Administratora Danych zawierające podstawowe informacje, w czasie umożliwiającym dochowanie przez Administratora Danych terminów, o których mowa w ust. 7 i 8. Wzór zgłoszenia stanowi Załącznik nr 1 do Zarządzenia.
4) Podmiot przetwarzający poprzez pracę Zespołu jest zobowiązany do pomagania Administratorowi Danych z wywiązania się z obowiązków określonych w art. 33 RODO np. poprzez udzielanie dostępnych mu w danej sprawie informacji
5) Inspektor Ochrony Danych PODGiK w Poznaniu przygotowuje sprawozdanie podsumowujące dla Dyrektora PODGiK w Poznaniu zgodnie z Polityką Bezpieczeństwa funkcjonującą w PODGiK w Poznaniu, zawierające informacje o podjętych działaniach.
7. W przypadku naruszenia ochrony danych osobowych, Administrator Danych bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je do Prezesa Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego Prezesowi Urzędu Ochrony Danych Osobowych po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

§3
Działania po przywróceniu stabilnego stanu
1. Po przywróceniu stabilnego stanu, Zespół przeprowadza szczegółową analizę zdarzenia w celu podjęcia środków zaradczych, które wyeliminują wystąpienie podobnych zdarzeń w przyszłości.
2. Zespół do przeprowadzenia analizy, o której mowa w pkt. 1 może posłużyć się procedurą oceny ryzyka oraz oceny skutków dla ochrony danych stosowaną w PODGiK w Poznaniu, o której mowa w Zarządzeniu Dyrektora PODGiK w Poznaniu w sprawie stosowania podejścia opartego na ryzyku w zakresie przetwarzania danych osobowych.

§4
W razie nieobecności Inspektora Ochrony Danych PODGiK w Poznaniu, Administratora Systemów Informatycznych PODGiK w Poznaniu, Kierowników Wydziałów ich obowiązki wykonują osoby je zastępujące.

§5
Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do zarządzenia nr GKG.GPK.0200.21.2021
Dyrektora PODGIK z dnia 3 marca 2021 r.

Poznań, Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Znak sprawy Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Zgłoszenie wystąpienia naruszenia ochrony danych osobowych Administratorowi Danych przez PODGIK w Poznaniu

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Administrator Danych

1. Osoba powiadamiająca PODGiK w Poznaniu o zaistniałym zdarzeniu:
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
(imię, nazwisko, stanowisko, dane kontaktowe)
2. Czas stwierdzenia naruszenia
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
(data, godzina)
3. Sposób stwierdzenia naruszenia
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
(np. zgłoszenie osoby, której dane dotyczą; cykliczny przegląd logów; zgłoszenie przez pracownika itp.)
4. Opis naruszenia w tym kategorie osób, których dotyczy naruszenie
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
5. Przyczyna naruszenia
1) Wewnętrzne działanie niezamierzone
2) Wewnętrzne działanie zamierzone
3) Zewnętrzne działanie niezamierzone
4) Zewnętrzne działanie zamierzone
6. Charakter naruszenia
1) Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych
2) Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania
3) Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną
7. Kategorie danych osobowych
1) Dane podstawowe:
a) Nazwiska i imiona
b) Imiona rodziców
c) Data urodzenia
d) Numer rachunku bankowego
e) Adres zamieszkania lub pobytu

f) Numer ewidencyjny PESEL
g) Adres e-mail
h) Nazwa użytkownika i/lub hasło
i) Dane dotyczące zarobków i/lub posiadanego majątku
j) Nazwisko rodowe matki
k) Seria i numer dowodu osobistego □ Numer telefonu
l) Wizerunek
m) Inne:
n) Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
2) Dane szczególnej kategorii:
a) Dane o pochodzeniu rasowym lub etnicznym
b) Dane o poglądach politycznych
c) Dane o przekonaniach religijnych lub światopoglądowych
d) Dane o przynależności do związków zawodowych
e) Dane dotyczące seksualności lub orientacji seksualnej
f) Dane dotyczące zdrowia
g) Dane genetyczne
h) Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej
3) Dane, o których mowa w art. 10 RODO
a) Dane dotyczące wyroków skazujących
b) Dane dotyczące czynów zabronionych
c) Inne:
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
8. Dotychczas podjęte działania
Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
9. Podpis osoby sporządzającej zgłoszenie

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Podmiot przetwarzający

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Podpis osoby sporządzającej zgłoszenie

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Podpis osoby sporządzającej zgłoszenie

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Podpis osoby sporządzającej zgłoszenie

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Podpis osoby sporządzającej zgłoszenie

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Podpis osoby sporządzającej zgłoszenie