ZARZĄDZENIE NR GKG.GPK.0200.20.2021

DYREKTORA POWIATOWEGO OŚRODKA DOKUMENTACJI

GEODEZYJNEJ I KARTOGRAFICZNEJ

z dnia 3 marca 2021 **r.**

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

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. 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 (dalej RODO) jest Administratorem Danych.
3. Ilekroć w zarządzeniu jest mowa o:
   1) Administratorze Danych - rozumie się przez to PODGIK w Poznaniu tj. 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 - rozumie się przez to osobę wyznaczoną przez Administratora Danych (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 (PODGiK w Poznaniu) w celu nadzorowania i przestrzegania zasad ochrony danych osobowych,
   4) 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.

5) PODGiK – Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej.

4. Przestrzeganie postanowień niniejszego Zarządzenia służy właściwemu reagowaniu na przypadki naruszeń ochrony danych osobowych w PODGiK w Poznaniu.
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, a w sytuacjach gdy zdarzenie dotyczy zagadnień z obszaru informatycznego również Administratora Systemów Informatycznych.
2. Inspektor Ochrony Danych ma obowiązek poinformowania o możliwości wystąpienia naruszenia ochrony danych osobowych Administratora Danych.
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. Administrator Danych uruchamia zespół szybkiego reagowania (dalej Zespół), w skład którego wchodzi:
   1) Inspektor Ochrony Danych,
   2) Administrator Systemów Informatycznych jeśli zdarzenie dotyczy zagadnień z obszaru informatycznego,
   3) Wyznaczeni przez Administratora Danych 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 Administratora Danych 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:
   1) Czy doszło do naruszenia ochrony danych osobowych,
   2) Czy zachodzi konieczność zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, zgodnie z art. 33 RODO.
   3) Czy zachodzi konieczność zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, zgodnie z art. 34 RODO.
6. Jeżeli doszło do naruszenia ochrony danych osobowych, Inspektor Ochrony Danych:
   1) Powiadamia o wynikach analizy, o której mowa w ust. 5 Administratora Danych,
   2) Jeżeli zachodzi przesłanka wskazana w ust 5 pkt. 2 przygotowuje wraz z Zespołem stosowne zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych,
   3) Jeżeli zachodzi przesłanka wskazana w ust. 5 pkt. 3 przygotowuje wraz z Zespołem zawiadomienie do osoby, której dane dotyczą o naruszeniu ochrony danych osobowych,
   4) Jeżeli zachodzi przesłanka wskazana w ust. 5 pkt. 2 i 3 przekazuje do Administratora Danych dokumenty, niezwłocznie w terminie umożliwiającym dochowanie przez Administratora Danych terminów, o których mowa w ust. 7 i 8.
   5) Przygotowuje sprawozdanie podsumowujące dla Administratora Danych zgodnie z Polityką Bezpieczeństwa funkcjonującą w PODGiK w Poznaniu, zawierające informacje o podjętych działaniach, niezależnie od tego czy zachodzi przesłanka wskazana w ust.5 pkt. 2 i 3.
7. Zgłaszanie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych następuje bez zbędnej zwłoki – w miarę możliwość, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Do zgłoszenia przekazanego Prezesowi Urzędu Ochrony Danych Osobowych po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
8. Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych następuje bez zbędnej zwłoki.

9. W imieniu PODGiK w Poznaniu jako Administratora Danych zgłoszenia lub zawiadomienia dokonuje Dyrektor PODGiK w Poznaniu lub jego zastępca/pełnomocnik.
10. W przypadku gdy zgłoszenie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych nie było zgłoszeniem kompletnym, tj.
    1) nie zawierało wszystkich informacji o naruszeniu, a zostało wysłane ze względu na możliwe przekroczenie terminu 72 godzin wymaganych na zgłoszenie naruszenia,
    2) okazało się, że zawierało błędne dane lub dane możliwe do zaktualizowania,

Zespół ponownie, bez zbędnej zwłoki przygotowuje zgłoszenie uzupełniające dla Prezesa Urzędu Ochrony Danych Osobowych, które zostaje przekazane do Administratora Danych.

11. W imieniu PODGiK w Poznaniu jako Administratora Danych zgłoszenia uzupełniającego dokonuje Dyrektor PODGiK w Poznaniu lub jego zastępca/pełnomocnik.

§ 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, Administratora Systemów Informatycznych, Kierowników Wydziałów ich obowiązki wykonują osoby je zastępujące.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
GEODETA POWIATOWY
Tomasz Powroźnik

Inspektor
Ochrony Danych
Agnieszka Rogowska

RADCA PRAWNY
Ewa Woroniecka-Andrzejczak