Burmistrz Sośnicowic

ZARZĄDZENIE Nr 20/ 2019
Burmistrza Sośnicowic
z dnia 21.02.2019 r.

w sprawie wprowadzenia instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych

Na podstawie art. 33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2018 r. 994 z późn. zm.) w związku z art. 33 i 34 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) (Dz.U.UE.L.2016.119.1) zarządzam, co następuje:

§ 1

Wprowadza się instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Sośnicowicach.

§ 2

Zobowiązuję wszystkich pracowników Urzędu Miejskiego w Sośnicowicach do zapoznania się z niniejszą instrukcją.

§ 3

Zarządzenie wchodzi w życie z dniem 22.02.2019 r.

BURMISTRZ SOŚNICOWIC

BURMISTRZ
Leszek Kołodziej

Gmina Sośnicowice 44-153 Sośnicowice, Rynek 19

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W SOŚNICOWICACH

Telefon: 32 238 71 91, Fax: 32 238 75 50 NIP: 969 14 22 687, REGON: 276257788
email: um@sosonicowice.pl http://sosnicowice.pl

Spis treści

I. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

§ 1

Naruszeniem ochrony danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, zniszczenia, 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 ujawnienie danych,
5. pozyskiwanie danych z nielegalnych źródeł.

Naruszenie ochrony danych osobowych jest wynikiem przypadkowego lub niezgodnego z prawem działania powodującego utratę poufności, integralności lub dostępności przetwarzanych w Urzędzie Miejskim w Sośnicowicach danych osobowych.

II. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHORONY DANYCH OSOBOWYCH

§ 2

1. Każdy pracownik Urzędu Miejskiego w Sośnicowicach, który stwierdzi lub podejrzewa fakt naruszenia ochrony danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu przełożonemu. lub bezpośrednio Administratorowi Danych Osobowych (Burmistrzowi Sośnicowic) i Inspektorowi Ochrony Danych.
2. Typowe sytuacje, gdy użytkownik powinien dokonać powiadomienia:
   - ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   - awaria komputera/serwera/ dysku przenośnego
   - wadliwie działające oprogramowanie
   - losowe zdarzenia zewnętrzne np. pożar, zalanie, uszkodzenie instalacji elektrycznej / sieci komputerowej
   - dokumentacja jest niszczona bez użycia niszczarki;
   - otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) przechowywanych na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
   - niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych;
   - wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz jednostki bez upoważnienia/ polecenia służbowego;
   - udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;

- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- telefoniczne próby wyłudzenia danych osobowych;
- kradzież komputerów / smartfonów / tabletów lub twardych dysków z danymi osobowymi;
- utrata kontroli nad kopią danych osobowych;
- maile zachęcające do ujawnienia identyfikatora i/lub hasła;
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
- hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik Urzędu Miejskiego w Sośnicowicach, który stwierdzi fakt naruszenia ochrony danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych Osobowych, Inspektora Ochrony Danych lub innej osoby upoważnionej przez Administratora Danych Osobowych.

§ 5

Inspektor Ochrony Danych podejmuje następujące kroki:

1. Zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy.
2. Odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem.
3. Nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 6

Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 1.

§ 7

Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także odnosi się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - Rejestr incydentów i działań korygujących i zapobiegawczych.

III. NARUSZENIE OCHRONY DANYCH OSOBOWYCH - ODPOWIEDZIALNOŚĆ

§ 8

Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

IV. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

§ 9

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Sposób realizacji zgłoszenia – Załącznik nr 3.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
2.1. 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;
2.2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
2.3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
2.4. opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

V. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

§ 10

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. Zawiadomienie, o którym mowa w ust. 1 niniejszego paragrafu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 33 ust. 3 lit. b), c) i d) 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).

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   3.1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   3.2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   3.3. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Procedura zawiera:

Załącznik nr 1 - Raport z naruszenia ochrony danych osobowych

Załącznik nr 2 - Rejestr incydentów bezpieczeństwa, podjętych działań krygujących i zapobiegawczych

Załącznik nr 3 - Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Procedurę opracował

Inspektor Ochrony Danych ..... 21.02.2018 r. .....

(data i podpis)

Procedurę zatwierdził

Administrator Danych ..... 21.02.2018 r. ..... BURMISTRZ Leszek Kołodziej

(data i podpis)

Załącznik nr 1 do Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Sośnicowicach

RAPORT Z NARUSZENIA OCHRONY DANYCH W URZĘDZIE MIEJSKIM W SOŚNICOWICACH

1. Data ..... Godzina .....
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....

   (imię, nazwisko, stanowisko służbowe,):
3. Lokalizacja zdarzenia .....

   (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, 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)

REJESTR INCYDENTÓW BEZPIECZEŃSTWA, PODJĘTYCH DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH W URZĘDZIE MIEJSKIM W SOŚNICOWICACH

Zadanie / problem / incydent (*podać opis incydentu*)	Źródło zgłoszenia (*podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.*)	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację (*podać dane osoby lub funkcje osoby odpowiedzialnej*)	Przyczyna niezgodności (*podać przyczynę powstania incydentu*)	Działanie korygujące / zapobiegawcze (*opisać działania jakie podjęto w celu przywrócenia bezpieczeństwa*)	Ocena skuteczności (*opisać jakie skutki przyniosło działanie korygujące*)

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Instrukcja powiadomienia Prezesa UODO o naruszeniu znajduje się na stronie Urzędu Ochrony Danych Osobowych

https://uodo.gov.pl/pl/134/233

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

1. Zgłoszenia naruszenia dokonuje się elektronicznie **za pomocą odpowiedniego formularza**, który należy wypełnić a następnie...
2. ...załączyć do **pisma ogólnego dostępnego** **na platformie biznes.gov.pl**