Załącznik Nr 15 do Zarządzenia Nr 150/18

Prezydenta Miasta Szczecin

z dnia 6 kwietnia 2018 r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta Szczecin

1. Instrukcja postępowania określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczeń systemu informatycznego,

2) istnieje podejrzenie naruszenia zabezpieczeń systemu informatycznego.

2. Do przypadków, które pozwalają przypuszczać, że zaistniał jeden z dwóch przypadków o których mowa w ust. 1 należą w szczególności:

1) awarie losowe (pożar, katastrofa budowlana, inne),

2) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na działanie umyślne w kierunku naruszenia ochrony danych,

3) pojawienie się odpowiedniego komunikatu od tej części systemu, która zapewnia ochronę przetwarzania danych osobowych,

4) jakość danych osobowych w systemie, wskazuje na działanie wirusa lub inną nieprzewidzianą modyfikację w systemie,

5) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innymi strzeżonymi elementami systemu zabezpieczeń,

6) praca w sieci wykazuje nieprzypadkowe odstępstwa od standardowego rytmu pracy zmierzające do zniesienia ochrony danych osobowych,

7) niedozwolone kopiowanie lub modyfikację danych osobowych,

8) informacja z infrastruktury telekomunikacyjnej wskazuje na dostęp do systemu osoby nieupoważnionej,

9) umyślna podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia,

10) rażące złamanie dyscypliny w zakresie procedur bezpieczeństwa informacji (nie plombowanie / zamykanie pomieszczeń, nie wykonywanie kopii bezpieczeństwa),

11) ujawnienie wykonywania prac na danych osobowych w celach pozasłużbowych,

12) wykrycie znamion włamania.

3. W przypadku wystąpienia sytuacji, o której mowa w ust. 2, po stwierdzeniu naruszenia zabezpieczeń systemu informatycznego lub uzyskaniu informacji na ten temat, użytkownik zobowiązany jest niezwłocznie, niezależnie od pory dnia do podjęcia następujących działań:

1) zawiadomić ABI tel. kom. 601086464 lub tel. 5702, Referat Wsparcia Użytkowników WInf - tel. 5708, a w przypadku braku kontaktu - kierownika, następnie Służbę Ochrony Mienia, Sekretarza Miasta, Zastępców Prezydenta Miasta oraz Prezydenta Miasta,

2) zaprzestać pracy w systemie, do czasu uzyskania zezwolenia od ABI, ASI lub ASU.

4. Zasady postępowania ABI lub osoby wyznaczonej do zastępowania ABI w okresie jego czasowych nieobecności:

1) wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia.

2) zidentyfikować rodzaj zaistniałego zdarzenia, określić skalę zniszczeń oraz metody dostępu do danych osób niepowołanych.

3) podjąć czynności w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód oraz zabezpieczenia przed usunięciem śladów ingerencji, szczególnie przez:

   a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych przez osobę niepowołaną,

   b) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczeń ochrony danych,

   c) zmianę hasła administratora i użytkownika, poprzez konto którego uzyskano nielegalny dostęp.

4) po wyeliminowaniu bezpośredniego zagrożenia przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych poprzez sprawdzenie:

   a) stanu urządzeń wykorzystywanych do przetwarzania danych,

   b) zawartości zbioru danych osobowych,

   c) sposobu działania programu,

   d) jakości komunikacji w sieci,

   e) wykluczenie możliwości obecności wirusów komputerowych.

5) przywrócić normalny stan działania systemu, a jeżeli nastąpiło uszkodzenie bazy danych, odtworzyć jej stan z ostatniej kopii awaryjnej.

6) wydać zgodę na wznowienie pracy w systemie informatycznym.

7) przeprowadzić szczegółową analizę zdarzenia w celu określenia sposobu i przyczyny naruszenia ochrony danych osobowych oraz wykonać działania, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. I tak:

   a) jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych, należy przeprowadzić dodatkowe szkolenie wszystkich osób uczestniczących w przetwarzaniu danych,

   b) jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać dodatkowe zabezpieczenia antywirusowe,

   c) jeżeli przyczyną zdarzenia było zaniedbanie osoby zatrudnionej przy przetwarzaniu danych osobowych, należy zastosować sankcje wynikające ustawy,

   d) jeżeli przyczyną było włamanie w celu pozyskania bazy danych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony,

   e) jeżeli przyczyną zdarzenia był zły stan urządzeń lub sposób działania programu, należy przeprowadzić kontrolne czynności serwisowe i powiadomić autora programu.

8) przygotować szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i przekazać go administratorowi danych osobowych.

5. W przypadku osoby, która w sytuacji naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w Instrukcji postępowania oraz nie powiadomiła odpowiedniej osoby, a także nie podjęła stosownego działania dokumentującego ten przypadek podejmowane są czynności kontrolne w celu ustalenia przebiegu zdarzenia.

6. Przypadki zaniechania obowiązków wynikających z Instrukcji mogą być potraktowane jako szczególnie rażące naruszenie ustalonego porządku, organizacji i dyscypliny pracy. Osoba taka może ponieść odpowiedzialność przewidzianą przepisami ustawy oraz Kodeksu Pracy.