ZARZĄDZENIE NR 20 /2000

Starosty Poznańskiego

z dnia 29.12.2000 rok

w sprawie : wprowadzenia instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych

Na podstawie art. 35 ust.2 ustawy z dnia 5 czerwca 1998r. - o samorządzie powiatowym / Dz.U.Nr 91, poz. 578 z późniejszymi zmianami /, oraz § 3 i § 6 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. - w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych / Dz.U.Nr 80 poz.521 /, zarządzam , co następuje :

§ 1

Zatwierdzam :

Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, stanowiącą załącznik do niniejszego Zarządzenia .

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA POZNAŃSKI
Ryszard Pomin

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych

INSTRUKCJA

postępowania w sytuacji naruszenia ochrony danych osobowych

Podstawę prawną do niniejszej instrukcji stanowią:

1. **Ustawa z dnia 29 sierpnia 1997rr. – o ochronie danych osobowych /Dz.U.Nr 133,poz.883/,**
2. **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r.- w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przechowywania danych osobowych /Dz.U.Nr 80,poz.521/,**

STAROSTA POZNAŃSKI
Ryszard Pomin

§ 1

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym .

§ 2

Instrukcja określa zasady postępowania w sytuacji naruszenia systemu ochrony danych osobowych, w szczególności gdy :

1) **stwierdzono naruszenie zabezpieczenia** systemu informatycznego ,

2) stan urządzenia , zawartość zbioru danych osobowych , ujawnione metody pracy , sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej **mogą wskazywać na naruszenie zabezpieczeń** tych danych .

§ 3

Za bezpieczeństwo danych osobowych przetwarzanych w systemie informatycznym odpowiada **administrator bezpieczeństwa informacji.**

§ 4

Każda osoba zatrudniona w Starostwie ,która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym , powinna **niezwłocznie poinformować** o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub administratora bezpieczeństwa informacji oraz pełnomocnika ds. ochrony informacji niejawnych .

§ 5

Osoba zatrudniona przy przetwarzaniu danych osobowych ,która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym , zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji w Starostwie oraz pełnomocnika ds. ochrony informacji niejawnych . a w przypadku ich nieobecności – bezpośrednio Starostę.

§ 6

Administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba powinna w pierwszej kolejności :

1. Zapisać wszelkie **informacje związane** z danym zdarzeniem a szczególnie : dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu .

2. Na bieżąco **wygenerować** i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie **możliwe dokumenty i raporty ,**które mogą pomóc w ustaleniu okoliczności zdarzenia , opatrzyć je datą i podpisem .

3. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia , zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej

§ 7

Niezwłocznie należy podjąć odpowiednie kroki w celu **powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej** , zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji , szczególnie przez :

a) **fizyczne odłączenie** urządzeń i segmentów sieci , które mogły umożliwić dostęp do bazy danych osobie nie upoważnionej ,

b) **wylogowanie** użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych ,

c) **zmianę hasła** na konto administratora i użytkownika , poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania .

§ 8

Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić **wstępną analizę stanu systemu** informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie.

§ 9

Administrator bezpieczeństwa informacji lub inna upoważniona przez niego osoba powinna sprawdzić :

a) stan urządzeń wykorzystywanych do przetwarzania danych osobowych ,

b) zawartość zbioru danych osobowych ,

c) sposób działania programu ,

d) jakość komunikacji w sieci telekomunikacyjnej ,

e) jak również wykluczyć możliwość obecności wirusów komputerowych .

§ 10

Po dokonaniu powyższych czynności administrator bezpieczeństwa informacji powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikację :

- rodzaju zaistniałego zdarzenia ,
- metody dostępu do danych osoby nie upoważnionej ,
- skali zniszczeń .

§ 11

Niezwłocznie należy **przywrócić normalny stan działania systemu ,** przy czym , jeżeli nastąpiło uszkodzenie bazy danych , niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności , mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną .

§ 12

Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu **wyeliminowanie podobnych zdarzeń w przyszłości .**

1. Jeżeli przyczyną zdarzenia był **błąd osoby zatrudnionej** przy przetwarzaniu danych osobowych w systemie informatycznym należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych .

2. Jeżeli przyczyną zdarzenia było **uaktywnienie wirusa** , należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe .

3. Jeżeli przyczyna zdarzenia było **zaniedbanie** ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych , należy wyciągnąć konsekwencje regulowane ustawą .

4. Jeżeli przyczyną zdarzenia było **włamanie w celu pozyskania** bazy danych osobowych , należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych .

5. Jeżeli przyczyną zdarzenia był **zły stan urządzenia** lub sposób działania **programu** należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo – programowe .

§ 13

Administrator bezpieczeństwa informacji **przygotowuje szczegółowy raport** o przyczynach , przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz w terminie 7 dni od daty zaistnienia zdarzenia przekazuje go Staroście i Pełnomocnikowi ds. ochrony informacji niejawnych.

STAROSTA POZNAŃSKI
Ryszard Pomin

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych
Beata Waitowicz