ZARZĄDZENIE NR 7/12
DYREKTORA ZAKŁADU GOSPODARKI KOMUNALNEJ LIPKA

z dnia 1 marca 2012 r.

w sprawie wprowadzenia instrukcji określającej sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz postępowania w sytuacji naruszenia ochrony danych osobowych.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. (t. j. Dz. U. z 2002 r. nr 101, poz. 926 z późniejszymi zmianami) o ochronie danych osobowych oraz § 3 i 5 Rozporządzenia Ministra Spraw Wewnetrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024 z późniejszymi zmianami) zarządzam co następuje:

§ 1. Wprowadza się instrukcję określającą sposób zarządzania systememi informatycznymi służącymi do przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej LIPKA. Instrukcja stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2. Wprowadza się instrukcję określającą sposób postepowania w sytuacji naruszenia ochrony danych osobowych w Zakładzie Gospodarki Komunalnej LIPKA. Instrukcja stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 3. Administrator sam wykonuje czynności administratora bezpieczeństwa informacji.

§ 4. Pracownicy Zakładu Gospodarki Komunalnej LIPKA zostaną zapoznani z treścią niniejszej instrukcji oraz zobowiążą się do jej przestrzegania.

§ 5. Zarządzenie wchodzi w życie z dniem podjęcia.

Załącznik Nr 1 do Zarządzenia Nr 7/12

Dyrektora Zakładu Gospodarki Komunalnej LIPKA

z dnia 1 marca 2012 r.

Instrukcja określająca sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Zakładzie Gospodarki Komunalnej LIPKA

§ 1. Instrukcja zarządzania systemami informatycznymi w Zakładzie Gospodarki Komunalnej LIPKA ma na celu osiągnięcie i utrzymywanie odpowiedniego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu.

§ 2. Każda osoba ma prawo do ochrony dotyczacych jej danych osobowych.

§ 3. Za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby.

§ 4. Przetwarzanie danych dopuszczalne jest tylko wtedy, gdy:

1. Osoba, której dane dotyczą wyrazi na to zgodę chyba, że chodzi o usunięcie dotyczących jej danych.

2. Jest to niebędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

3. Jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.

4. Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

5. Jest niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

§ 5. Z uwagi na ochronę interesów osób, których dane dotyczą, zapewnia się:

1. Przetwarzanie danych zgodne z prawem.

2. Zbieranie danych dla oznaczonych zgodnie z prawem celów, i nie poddawanie ich dalszemu przetwarzaniu niezgodnemu z tymi celami.

3. Poprawność merytoryczną danych i ich adekwatność w stosunku do celów, w jakich są przetwarzane.

4. Przechowywanie danych w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

§ 6. W Zakładzie Gospodarki Komunalnej LIPKA ustala się następujące obszary, w których przetwarzane sa dane osobowe z użyciem sprzętu komputerowego:

1. Biuro nr- 1.

2. Biuro nr 2.

§ 7. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych.

§ 8. Wewnątrz obszaru o którym mowa w par. 6 osoby postronne mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych osobowych.

§ 9. Stanowisko komputerowe może być zabezpieczone przed dostępem osób nieupoważnionych hasłem. Na stanowiskach, na których przetwarzane są dane osobowe stosowanie haseł jest obowiązkowe.

§ 10. Procedurę nadawania oraz zmiany haseł dokonuje administrator bezpieczeństwa informacji lub inna upoważniona do tego osoba. Hasła zmieniane są co najmniej raz w miesiącu. Prowadzi się ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych oraz rejestr haseł nadawanych na poszczególnych stanowiskach. Rejestr powinien zawierać określenie stanowiska komputerowego, nadane hasło, datę nadania (zmiany) hasła. Hasło użytkownika umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie jego ważności.

§ 11. Ekrany monitorów stanowisk dostępu do danych osobowych powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.

§ 12. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

§ 13. Przebywanie wewnątrz obszaru, w którym przetwarzane są dane (zwłaszcza dane osobowe) osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych i za zgodą administratora danych lub osoby przez niego upoważnionej.

§ 14. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 15. W przypadku kiedy stwierdzono naruszenie zabezpieczenia systemu informatycznego lub stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu mogą wskazywać na naruszenie zabezpieczeń tych danych należy postępować zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

§ 16. Nośniki danych (zwłaszcza zawierające dane osobowe) przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

§ 17. Urządzenia, dyski lub inne informatyczne nośniki danych przeznaczone do naprawy pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 18. Wydruki, które są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 19. Nośniki informacji oraz wydruki, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

§ 20. 1. Kopie awaryjne (zwłaszcza zawierające dane osobowe) nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

2. Kopie awaryjne należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 21. 1. Kontrolę systemów komputerowych pod kątem obecności wirusów komputerowych przeprowadza się co najmniej raz na kwartał oraz w każdym przypadku, kiedy sytuacja może wskazywać na zainfekowanie stanowiska komputerowego wirusem komputerowym. Kontroli pod kątem obecności wirusów komputerowych podlegają także:

1) zewnętrzne nośniki danych, których odczyt ma nastąpić na stanowisku komputerowym w Zakładzie Gospodarki Komunalnej LIPKA,

2) poczta elektroniczna (zwłaszcza gdy pochodzi od nieznajomego wysyłającego oraz zawiera informacje, których wykorzystanie jest bezcelowe)

§ 22. Kontrolę antywirusową przeprowadza pracownik, który użytkuje dane stanowisko komputerowe lub inna osoba upoważniona.

§ 23. W przypadku wykrycia lub podejrzenia istnienia wirusa komputerowego należy przeprowadzić kontrolę antywirusową za pomocą dostępnego programu oraz wezwać odpowiednią osobę celem usunięcia wirusa.

§ 24. Ochrona antywirusowa dokonywana jest przy pomocy dostępnych programów antywirusowych.

§ 25. Wprowadza się zakaz instalowania jakiegokolwiek oprogramowania na stanowiskach komputerowych przez pracowników Zakładu Gospodarki Komunalnej LIPKA z wyjątkiem administratora sieci oraz administratora bezpieczeństwa informacji.

§ 26. Urządzenia, dyski lub inne informatyczne nośniki danych (zwłaszcza zawierające dane osobowe), przeznaczone do naprawy pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§ 27. W przypadku udostępnienia danych osobowych w celach innych niż włączenie zbioru, administrator danych udostępnia posidane dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa zgodnie z art. 29 ust. 1 i 2 ustawy o ochronie danych osobowych (t. j. Dz. U. z 2002 r. nr 101, poz. 926 z późniejszymi zmianami).

§ 28. Udostępnianie danych osobowych w celach innych niż włączenie do zbioru, następuje na pisemny wniosek zgodnie z wzorem określonym w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Danych Osobowych (Dz. U. z 2004 r. nr 100, poz. 1025).

Załącznik Nr 2 do Zarządzenia Nr 7/12

Dyrektora Zakładu Gospodarki Komunalnej LIPKA

z dnia 1 marca 2012 r.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Zakładzie Gospodarki Komunalnej LIPKA

§ 1. Instrukcja jest przenaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym w Zakładzie Gospodarki Komunalnej LIPKA.

§ 2. Instrukcja określa tryb postępowania w przypadku gdy stwierdzono naruszenie zabezpieczenia systemu informatycznego oraz 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. Każda osoba zatrudniona w danej jednostce, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym osobę zatrudniona przy przetwarzaniu danych osobowych lub administratora bezpieczenstwa informacji albo inną upowaznioną przez niego osobę.

§ 4. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informacje lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji w jednostce lub inną upoważnioną przez niego osobę, a w przypadku ich nieobecności- bezpośrednio administratora danych osobowych.

§ 5. 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.

§ 6. 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:

1) Fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie upoważnionej.

2) Wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.

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

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

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

1) Stan urządzeń wykorzystywanych do przetwarzania danych osobowych.

2) Zawartość zbioru danych osobowych.

3) Sposób działania programu.

4) Jakość komunikacji w sieci telekomunikacyjnej.

5) Możliwość obecności wirusów komputerowych.

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

1)Rodzaju zaistniałego zdarzenia.

2)Metody dostępu do danych osoby nieupoważnionej.

3)Skali zniszczeń.

§ 10. 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.

§ 11. Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki w celu wyeliminowania 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 zabezpieczenie antywirusowe.

3)Jeżeli przyczyną było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu należy wyciągnąć konsekwencje regulowane ustawą.

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

5)Jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy przeprowadzić kontrolę serwisowo- programową.

§ 12. Administrator bezpieczeństwa informacji przygotowuje szczegółowo raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualnie kopie dowodów dokumentujących to zdarzenie) oraz w określonym terminie od daty zaistnienia zdarzenia przekazuje go administratorowi danych osobowych jednostki.