Zarządzenie Wewnętrzne Nr 23 /10

Dyrektora Zespołu Ośrodków Wsparcia w Lublinie

z dnia 1 września 2010 r.

w sprawie ochrony danych osobowych w Zespole Ośrodków Wsparcia w Lublinie

Na podstawie § 3 Rozporządzenia Ministra Spraw Wewnętrznych 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, Nr 100, poz. 1024 z późń. zm) oraz art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002, Nr 101, poz. 926 z późn. zm) zarządzam, co następuje:

§ 1

1. Wyznaczam Panią Emilię Śliwińską – inspektora ds. kadr jako administratora bezpieczeństwa informacji, zwanym dalej ABI.
2. Zadaniem ABI jest nadzór nad przestrzeganiem zasad przetwarzania danych osobowych, a w szczególności nadzór nad zabezpieczeniem danych przed osobami nieupoważnionymi, zmianą, utratą lub zniszczeniem oraz przetwarzaniem z naruszeniem ustawy.
3. ABI określa hasła użytkowania komputerów dla przetwarzania danych osobowych i zmienia je w razie potrzeby.

§ 2

1. Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby posiadające stosowne upoważnienia.
2. Wzór upoważnienia oraz oświadczenia pracownika stanowi Zał. Nr 1 do niniejszego zarządzenia.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych zawiera:
   - imię i nazwisko oraz stanowisko pracy osoby upoważnionej,
   - nazwę komórki organizacyjnej,
   - datę nadania oraz ustania oraz zakres upoważnienia do przetwarzania danych.

§ 3

1. Obszarami przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są wszystkie budynki wchodzące w skład Zespołu Ośrodków Wsparcia tj.:

   a) budynek Centrum Usług Socjalnych przy ul. Lwowskiej 28,
   b) budynek Dziennego Domu Pomocy Społecznej Nr 1 przy ul. Niecałej 16,
   c) budynek Dziennego Domu Pomocy Społecznej Nr 2 przy ul. Pozytywistów 16,
   d) budynek Dziennego Ośrodka Adaptacyjnego dla Dzieci Specjalnej Troski przy ul. Poturzyńskiej 1,
   e) budynek Środowiskowego Domu Samopomocy przy ul. Nałkowskich 78

2. Przebywanie osób nieuprawnionych wewnątrz obszaru, o którym mowa w ust. 1 jest dopuszczalne tylko w obecności osób upoważnionych do przetwarzania danych osobowych lub za zgodą ABI.
3. Ustalam procedurę pracy na stanowiskach, na których przetwarzane są dane osobowe w systemie komputerowym:
   - ustawienie monitorów w sposób uniemożliwiający dostęp do informacji osobom nieuprawnionym,
   - uruchomienie komputera odpowiednim hasłem,
   - w czasie przerw w pracy wylogowanie z systemu,
   - upewnienie się czy dane zostały zarejestrowane,
   - zakończenie pracy związanej z przetwarzaniem danych w systemie komputerowym powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.
4. Kopie informatyczne oraz wydruki zawierające dane osobowe są wykonywane w miarę potrzeb.
5. Kopie awaryjne okresowo sprawdzane są pod kątem przydatności.
6. Niepotrzebne dokumenty zawierające dane osobowe są starannie niszczone w sposób uniemożliwiający ich odczytanie (np. przy pomocy niszczarki).
7. Dokumenty zawierające dane osobowe, nośniki danych oraz wydruki nieprzeznaczone do udostępnienia przechowywane są w specjalnie zamykanych szafkach, do których dostęp mają tylko osoby uprawnione.
8. Pomieszczenia, w których znajdują się dokumenty zawierające dane osobowe są zamykane na klucz.
9. Klucze do pomieszczeń są deponowane w specjalnie zabezpieczonej szafce.
10. Ustalam procedurę pracy na stanowiskach, na których przetwarzane są dane osobowe w systemie papierowym:
    - zamykanie na klucz szafek zawierających dane osobowe po każdym ich otwarciu ,
    - w wypadku opuszczenia pomieszczenia każdorazowe zamykanie go na klucz,
    - zakończenie pracy związanej z przetwarzaniem danych osobowych w systemie papierowym powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.
11. Wszystkie awarie systemu naruszenia bezpieczeństwa wymagają zgłoszenia do ABI.
12. Instrukcja zarządzania systemem informatycznym stanowi Zał. Nr 2 do niniejszego zarządzenia.

§ 4

1. Wykaz zbiorów danych osobowych Zespołu stanowią:
   a) akta osobowe pracowników,
   b) akta uczestników,
   c) dokumentacja polityki kadrowej,
   d) ewidencja w sprawach pracowniczych,
   e) listy płac,
   f) deklaracje podatkowe, ubezpieczenia pracowników,
   g) archiwum
2. Dane przetwarzane są za pomocą systemu operacyjnego Win XP oraz programów:
   - Microsoft Office 97 – 2003 lub Microsoft Office 2007,
   - Qadr,
   - Qwark,
   - Płatnik,
   - Pekao Biznes 24,
   w komputerach ewidencjonowanych w spisie inwentarzowym.

§ 5

1. Wykonanie zarządzenia powierza się ABI oraz pracownikom upoważnionym do przetwarzania danych osobowych.
2. Nadzór nad realizacją zarządzenia powierzam ABI.
3. Dotychczasowe upoważnienia i oświadczenia pracowników złożone przed wejściem w życie niniejszego zarządzenia pozostają w mocy.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Maria Pawela

Mirosława Łuksza
radca prawny

Zał. Nr 1 do Zarządzenia
Wewnętrznego Nr 45 / 2010

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Część I

Na postawie - art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity - Dz.U. z 2002 r. nr 101, poz. 926 z późn. zmianami) - upoważniam

Panią/Pana ....,

zatrudnioną/zatrudnionego na stanowisku ..... w Zespole Ośrodków Wsparcia w Lublinie do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie informacji zawartych w

.....

.....

.....

Niniejsze upoważnienie ważne jest od dnia ..... i wygasa z chwilą rozwiązania bądź wygaśnięcia stosunku pracy, jak również przeniesieniem na inne stanowisko pracy nie wymagające dostępu do danych osobowych, a ponadto może być w każdym czasie zmienione lub odwołane.

.....
podpis pracodawcy

Część II

Zobowiązuję się zachować w tajemnicy w/wymienione dane osobowe oraz sposoby ich zabezpieczenia podczas zatrudnienia, jak też po ustaniu stosunku pracy.

.....
podpis upoważnionego

Zał. Nr 2 do zarządzenia
Wewnętrznego Nr 23 / 2010

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W ZESPOLE OŚRODKÓW WSPARCIA W LUBLINIE

Wprowadzenie

Niniejszy dokument jest dokumentem wewnętrznym wydanym przez Dyrektora Zespołu Ośrodków Wsparcia w Lublinie. Jest on przeznaczony dla osób upoważnionych do przetwarzania danych osobowych i został opracowany zgodnie z obowiązującymi aktami prawnymi:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002, Nr 101, poz. 926 z późn. zm),
2. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005, Nr 196, poz. 1631 z późń. zm).

Niniejszy dokument reguluje kwestie ochrony danych osobowych zawartych w systemach informatycznych działających w lokalnej sieci komputerowej oraz zbiorów danych osobowych zapisanych w postaci elektronicznej.

Definicje

Ilekroć w dokumencie występują słowa:

a) *Zespół* – należy przez to rozumieć Zespół Ośrodków Wsparcia w Lublinie,
b) *Administrator Danych Osobowych (ADO)* – należy przez to rozumieć Dyrektora,
c) *Administrator Bezpieczeństwa Informacji (ABI)* – należy przez to rozumieć pracownika Zespołu wyznaczonego przez ADO do nadzorowania przestrzegania zasad ochrony danych osobowych, o których mowa w zarządzeniu wewnętrznym Nr 23 / 2010.
d) *Identyfikator użytkownika* – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
e) *Hasło* – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
f) *Sieć wewnętrzna (sieć komputerowa, sieć lokalna)* – rozumie się przez to sprzęt komputerowy połączony pomiędzy sobą w celu przetwarzania danych osobowych,
g) *Użytkownik* – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w Zespole; użytkownikiem może być pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno – prawnej, osoby odbywającej staż lub wolontariat.

Procedury rozpoczęcia, zakończenia, zawieszenia i wznowienia pracy na stanowisku komputerowym

A. Procedura rozpoczęcia pracy

1. Sprawdzenie gotowości sprzętu komputerowego do pracy.
2. Uruchomienie komputera wchodzącego w skład systemu, podłączonego fizycznie do sieci lokalnej.
3. Zalogowanie się do systemu operacyjnego poprzez podanie identyfikatora i hasła.
4. Uruchomienie właściwej aplikacji i podanie identyfikatora i hasła.
5. Rozpoczęcie pracy.

B. Procedura zakończenia pracy

1. Zamknięcie wszystkich aplikacji.
2. Zamknięcie systemu.
3. Wyłączenie komputera.
4. Wyłącznie urządzeń preferencyjnych (np. drukarka).
5. Schowanie wymiennych nośników informacji do zamykanych szaf biurowych.

C. Procedura zawieszenia pracy

1. Przy opuszczeniu stanowiska komputerowego należy dopilnować, by na ekranie komputera nie były wyświetlone dane osobowe.
2. Przy opuszczeniu pokoju należy zabezpieczyć dostęp do danych osobowych osobom niepowołanym odpowiednimi środkami (np. zastosowanie wygaszacza ekranu, wylogowanie z systemu, wyłączenie monitora lub komputera).

D. Procedura wznowienia pracy

1. Należy zwrócić uwagę czy na stanowisku komputerowym nie ma oznak o próbie dostępu do stanowiska osób nieupoważnionych.
2. Wykonanie czynności niezbędnych do wznowienia pracy.

W przypadku zauważenia nieprawidłowości w działaniu systemu komputerowego, oprogramowania, a w szczególności podejrzenia o nieupoważnionym dostępie do danych osobowych należy niezwłocznie zawiadomić ABI lub ADO.

Procedury nadawania uprawnień do przetwarzania danych

A. Podstawowe zasady nadawania uprawnień

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się z:
   a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002, Nr 101, poz. 926 z późn. zm),
   b) Zarządzeniem Wewnętrznym Dyrektora Zespołu Ośrodków Wsparcia w Lublinie Nr 23 / 2010 w sprawie ochrony danych osobowych, instrukcji zarządzania systemem informatycznym oraz innej dokumentacji dotyczącej przetwarzania danych osobowych.

2. Osoby nieposiadające wymaganych upoważnień do przetwarzania danych osobowych lub do przebywania w pomieszczeniach gdzie przetwarza się dane osobowe, pod nieobecność osób upoważnionych, a które muszą przebywać w tych pomieszczeniach zobowiązane są do zgłoszenia się do ABI celem uzyskania upoważnienia.
3. W celu uzyskania upoważnienia do przetwarzania danych konieczne jest przeprowadzenie szkolenia.
4. Dokumenty oświadczenia wydane przez ABI o odbytym szkoleniu i zaznajomieniu się z konsekwencjami wynikającymi z ustawy o ochronie danych osobowych umieszczane są w aktach osobowych pracownika.

B. Procedura nadawania uprawnień do przetwarzania danych

1. ABI jest informowany przez inspektora ds. kadr o zatrudnieniu nowego pracownika, przyjęcia stażysty, zmiany stanowiska, zmiany zakresu obowiązków, wiążącej się z koniecznością przetwarzania danych osobowych itp. W informacji musi się znaleźć:
   - imię i nazwisko pracownika,
   - stanowisko,
   - zakres czynności.
2. Na podstawie informacji wymienionych w pkt. 1 ABI ma obowiązek przeprowadzenia szkolenia w zakresie obowiązujących przepisów o ochronie danych osobowych.
3. Przeprowadza szkolenie z procedur przetwarzania danych.
4. Pracownik podpisuje oświadczenie o przeprowadzonym szkoleniu i odpowiedzialności wynikającej z ustawy o ochronie danych osobowych.
5. ABI przygotowuje upoważnienie do przetwarzania danych osobowych i dostępie do odpowiednich zbiorów danych.
6. Upoważnienie przygotowane przez ABI podpisuje ADO.
7. ABI nadaje uprawnienia do dostępu do systemu poprzez nadanie identyfikatora i hasła, a następnie przekazuje je pracownikowi.
8. Sporządza odpowiedni wpis do rejestru osób upoważnionych do dostępu do określonych danych.

C. Procedura odbierania uprawnień do przetwarzania danych

1. ABI zdejmuje wskazanemu pracownikowi dostęp do określonych zbiorów danych oraz sporządza odpowiedni wpis w rejestrze osób upoważnionych do dostępu do określonych danych.

D. Procedura zmiany uprawnień do przetwarzania danych

1. ABI wykonuje procedurę C, a następnie procedurę D.

Elektryczne nośniki informacji: sposób, miejsce i okres przechowywania oraz sposób użytkowania

1. Dane osobowe w postaci elektronicznej przetwarzane są na nośnikach takich jak:
   - dysk twardy,
   - pamięć USB,
   - płyta CD lub DVD,
   - dyskietka.

2. Dane osobowe na nośnikach przetwarzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.
3. Nośniki z danymi osobowymi nie są wynoszone poza obszar przetwarzania danych.
4. Po zakończeniu pracy nośniki są przechowywane w zamykanych szafach lub sejfach.
5. Uszkodzone lub zużyte nośniki informacji są niszczone w sposób uniemożliwiający odczytanie z nich danych.

Zabezpieczenia systemu informatycznego przed działalnością osób nieupoważnionych i szkodliwego oprogramowania

Ochrona antywirusowa

1. W celu zapewnienia ochrony antywirusowej, na wszystkich stanowiskach komputerowych Zespołu instalowany jest program antywirusowy.
2. Sieć wewnętrzna jest połączona z Internetem za pomocą routera wyposażonego w firewall.
3. Dostęp do zasobów internetu dozwolony jest tylko w celach związanych z wykonywaniem czynności dotyczących powierzonych pracownikowi zadań.

Procedury wykonywania przeglądów i konserwacji systemów

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być przeprowadzane w terminach określonych przez producenta sprzętu.
2. Przeglądy i konserwacja oprogramowania i narzędzi programowych służących do przetwarzania danych przeprowadzane powinny być w przypadkach:
   a) zmiany systemu operacyjnego na serwerze plików lub na stanowisku użytkownika,
   b) zmiany lub aktualizacji oprogramowania na serwerze plików lub na stanowisku użytkownika,
   c) naprawy sprzętu lub oprogramowania na stanowisku użytkownika.
3. Przeglądy i konserwacje powinny być dokonywane w przypadku zgłoszenia przez użytkownika nieprawidłowości działania systemu lub oprogramowania służącego do przetwarzania danych osobowych.

DYREKTOR
Maria Pawela

Mirosława Łuksza
radca prawny