Zarządzenie Nr 10/2011
Dyrektora Powiatowego Zespołu Obsługi Finansowej Oświaty
w Tarnowskich Górach z dnia 20.07.2011r.

w sprawie ochrony danych osobowych w Powiatowym Zespole Obsługi Finansowej Oświaty w Tarnowskich Górach

Zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2002r. Nr 101, poz. 926, z późn. zm.) oraz zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 2004r. Nr 100, poz.1024)

zarządzam, co następuje:

§ 1

1. Przetwarzanie danych osobowych w Powiatowym Zespole Obsługi Finansowej Oświaty w Tarnowskich Górach służy jedynie realizacji zadań i celów Zespołu.
2. Przetwarzanie danych może odbywać się w systemach informatycznych oraz na wszelkich nośnikach papierowych (kartoteki, akta, zbiory ewidencyjne itp.).

§ 2

Przez użyte w Zarządzeniu pojęcia rozumie się:

- PZOFO – Powiatowy Zespół Obsługi Finansowej Oświaty w Tarnowskich Górach
- Administrator danych – Dyrektor PZOFO
- Zbiór danych – zestaw danych o charakterze osobowym
- Przetwarzanie danych – operacje wykonywane na danych osobowych, tj. zbieranie, przetwarzanie, utrwalania, przechowywanie, zmienianie, udostępnianie, usuwanie
- System informatyczny – zespół powiązanych ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych w celu przetwarzania danych,
- Plik elektroniczny – pojedynczy dokument w formie elektronicznej zawierający dane osobowe,
- Użytkownik systemu informatycznego – osoba pracująca z danym oprogramowaniem komputerowym (systemem), w którym są przetwarzane dane osobowe.

- Identyfikator – unikalna, niepowtarzalna nazwa użytkowania w systemie informatycznym,
- Hasło dostępu – ciąg znaków umożliwiający dostęp di systemu informatycznego,
- Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- Poufność danych – właściwość zapewniająca, że dane nie zostały udostępnione nieupoważnionym podmiotom,
- Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości.

§ 3

Określa się politykę bezpieczeństwa w sprawie ochrony danych osobowych gromadzonych w zbiorach PZOFO:

Procedura działania w sytuacji naruszenia zabezpieczeń danych osobowych:

1. Polityka bezpieczeństwa określa sposób postępowania w przypadku stwierdzenia naruszenia zabezpieczeń w systemie informatycznym, w którym przetwarzane są dane osobowe. Na naruszenie zasad wskazywać może stan urządzeń, zawartość zbioru danych, ujawnione metody pracy, jakość komunikacji w systemie informatycznym lub sposób działania programów.
2. W przypadku stwierdzenia naruszenia zabezpieczeń przez pracownika PZOFO, zobowiązany jest on do natychmiastowego zgłoszenia tego faktu swojemu bezpośredniemu przełożonemu, odcięcia dostępu do systemu informatycznego osobom postronnym, zastosowaniu wszelkich środków mających na celu ochronę danych i przeciwdziałających pogłębianiu się szkód oraz zabezpieczeniu dowodów mających posłużyć do wyjaśnienia przyczyn zaistniałej sytuacji.
3. Bezpośredni przełożony zobowiązany jest do niezwłocznego powiadomienia Administratora danych oraz zabezpieczenia dowodów mogących posłużyć do wyjaśnienia przyczyn, okoliczności oraz osób odpowiedzialnych za naruszenia danych osobowych.
4. Administrator danych po otrzymaniu informacji o naruszeniu ochrony danych osobowych ustala przyczyny i okoliczności zaistniałej sytuacji, ustala propozycję działań zmierzających do przywrócenia stanu przed naruszeniem ochrony danych, konsultuje z radcą prawnym opinię, co do konieczności powiadomienia organów ścigania o popełnieniu przestępstwa przeciwko ochronie danych (art.49 i nast. ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych lub przeciwko ochronie informacji (rozdział XXXIII kodeksu karnego).

Sposób przekazania sprzętu komputerowego do serwisowania:

1. Podmioty lub osoby dokonujące serwisowania sprzętu komputerowego, w którym przetwarzane są dane osobowe, przed przystąpieniem do serwisu składają pisemne oświadczenie o odpowiedzialności karnej wynikającej z ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 ze zm.), które stanowi załącznik Nr 1 do Zarządzenia.

2. Oświadczenie przechowywane jest w dokumentacji administratora danych.

Sposób dopuszczenia pracownika do pracy przy przetwarzaniu danych osobowych.

1. Każdy pracownik, stażysta, praktykant odbywający staż przed dopuszczeniem do pracy w PZOFO zobowiązany jest do złożenie pisemnego oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych. Oświadczenie określa Załącznik Nr 2 do Zarządzenia.
2. Oświadczenie przechowywane jest w aktach osobowych pracownika.
3. Administrator danych przekazuje pracownikom, stażystom, praktykantom, których czynności związane są z przetwarzaniem danych osobowych stosowane upoważnienie stanowiące Załącznik Nr 3 do Zarządzenia, które przechowuje się w aktach osobowych pracownika.

Wymagania określające obszar dostępu do danych osobowych:

1. Administrator danych określa pomieszczenia, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
2. Wszystkie pomieszczenia należące do PZOFO, z wyjątkiem pomieszczenia nr 8, stanowią obszar, w którym przetwarzane są dane osobowe.
3. Przebywanie wewnątrz obszaru zastrzeżonego osób nieuprawnionych jest dopuszczalne tylko w obecności osoby zatrudnionej w PZOFO za zgodą Administratora danych.
4. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na czas nieobecności w nich osób zatrudnionych, w sposób uniemożliwiający dostęp osób niepowołanych.

Poziom bezpieczeństwa przetwarzania danych:

1. Poziomy bezpieczeństwa obowiązujące w PZOFO, określa się w następujący sposób:

    - Poziom podstawowy – w systemie informatycznym nie są przetwarzane dane osobowe, o których mowa w art. 27 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz.926) oraz żadne z urządzeń służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną,
    - Poziom podwyższony: w systemie informatyczne są przetwarzane dane osobowe, o których mowa w art. 27 ustawy z 2002r. Nr 101, poz. 926) oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną,
    - Poziom wysoki: stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

§ 4

Wprowadza się Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz sposób przechowywania danych osobowych na nośnikach papierowych.

Rejestrowanie i wyrejestrowania użytkowników:

1. System informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelniania użytkowników, tj. identyfikator i hasło oraz powinien zawierać identyfikację użytkownika, modyfikującego dane osobowe.
2. Dla każdego użytkowania systemu informatycznego administrator danych określa hasło i identyfikator.
3. Dostęp do danych osobowych może mieć miejsce wyłącznie po podaniu identyfikatora i hasła dostępu.
4. Hasło użytkownika należy przekazywać bezpośrednio użytkownikowi w zamkniętej kopercie.
5. Hasło dostępu, powinno być zmienione po ustaniu zatrudnienia dotychczasowego użytkownika.
6. Ewidencja osób zatrudnionych przy przetwarzaniu danych oraz wykaz aktualnych haseł przechowywany jest u administratora danych. Ewidencję określa Załącznik Nr 4 do Instrukcji.
7. Hasła dostępu zmieniane są cyklicznie nie rzadziej niż raz w miesiącu.
8. Nie aktualne listy haseł osób zatrudnionych niszczy się przy pomocy niszczarki w obecności Głównego Księgowego.
9. Identyfikator osoby, która utraciła prawo do przetwarzania danych należy usunąć z systemu i uniemożliwić dostęp do danych osobowych oraz unieważnić hasło dostępu.
10. Dane osobowe przechowywane na nośnikach papierowych powinny być umieszczone w zamkniętych szafach, do których dostęp mają wyłącznie pracownicy pracujący na bazie danych oraz Administrator danych.

Procedury rozpoczynania i kończenia pracy w systemie, w którym przetwarzane są dane osobowe:

1. Pracownik uruchamiający system, w którym przetwarzane są dane osobowe, powinien upewnić się czy od czasu poprzedniego ukończenia pracy nie nastąpiło naruszenie zabezpieczeń systemu lub innej formy ingerencji.
2. W razie stwierdzenia naruszenia ochrony danych pracownik postępuje zgodnie z polityką bezpieczeństwa.
3. W pomieszczeniach, w których przebywają osoby postronne, monitory powinny być ustawione w taki sposób by uniemożliwić tym osobom wgląd w dane osobowe.

Tworzenie kopii awaryjnych:

1. Kopie awaryjne tworzy się poprzez dodatkowe zapisanie danych na dysku wymiennym np. (dyskietka, CD-RW, nośniki strimerowskie):
2. Kopie awaryjne wykonywane na CD, steamerach powinny być przechowywane w zamkniętych szafach lub sejfach.
3. Kopie awaryjne należy niezwłocznie usuwać po ustaleniu ich użyteczności lub nadpisywać aktualnymi danymi tej samej grupy informacji.

Sprawdzanie obecności i usuwanie wirusów komputerowych:

1. W celu wykrywania i usuwania wirusów komputerowych należy w systemie przetwarzania danych osobowych zainstalować odpowiednio dobrane programy antywirusowe.
2. Badania na obecność wirusa przeprowadza się każdego dnia.
3. Każdy użytkownik jest zobowiązany do sprawdzania własnego zestawu komputerowego przed wirusami.

Postępowanie ze sprzętem komputerowym i nośnikami danych:

1. Urządzenia i systemy informatyczne do przetwarzania danych osobowych zasilane energią elektryczną powinny być zabezpieczone przed utratą tych danych spowodowanych awarią przez wykorzystanie UPS-ów.
2. Z urządzeń, dysków i pozostałych nośników przed naprawą usuwa się dane osobowe, a gdy nie jest to możliwe uszkadza się w sposób uniemożliwiający odczyt danych lub naprawia w obecności administratora danych.

Sposób postępowania w zakresie komunikacji w sieci komputerowej

1. Dostęp dodanych osobowych gromadzonych w sieci komputerowej możliwy jest tylko po podaniu hasła i identyfikatora.
2. Dane osobowe w sieci komputerowej zabezpiecza się dodatkowo przez program antywirusowy.
3. W przypadku braku dostępu do danych osobowych znajdujących się na dyskach sieciowych należy powiadomić niezwłocznie administratora danych.

§ 5

1. Udostępniane danych osobowych instytucjom i osobom spoza PZOFO może odbywać się wyłącznie na podstawie pisemnie umotywowanego wniosku, który powinien zawierać zakres danych do udostępnienia oraz ich przeznaczenie.
2. Udostępnienie danych możliwe jest jedynie za zgodą Administratora danych.
3. Wnioski o udostępnienie danych przechowywane są u Administratora danych.

§ 6

Uchyla się Zarządzenia Nr 9/2008 Dyrektora Powiatowego Zespołu Obsługi Finansowej Oświaty w Tarnowskich Górach z dnia 1 grudnia 2008r.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 3

Tarnowskie Góry, dn. ……..

UPOWAŻNIENIE

Na podstawie art. 37 oraz art. 39 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U z 2002r. Nr 101, poz.926, ze zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U z 2004r. Nr 100. poz. 1024, ze zm.)

upoważniam

Panią/Pana ……..

Stanowisko……..

Do przetwarzania danych osobowych stanowiących zakres działalności Powiatowego Zespołu Obsługi Finansowej Oświaty.
Podstawowym miejscem przetwarzania danych jest:

Pomieszczenie nr ……., stanowisko komputerowe nr ……...

Upoważnienie jest ważne od dnia …… do czasu jego cofnięcia.

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowaniu w tajemnicy informacji o ich zabezpieczeniu.

…….. ……

podpis Administratora danych podpis osoby upoważnionej

Załącznik Nr 4

Ewidencja osób zatrudnionych przy przetwarzaniu danych oraz wykaz aktualnych haseł dostępu do przetwarzania danych osobowych

Wykaz haseł do systemów (arkuszy, plików, itp.), w których przetwarza się dane osobowe zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101. poz. 926 i Nr 153, poz. 1271).

Okres obowiązywania hasła: …………………………

Nazwa zbioru (stanowisko komputerowe)	**Użytkownik**	**Hasło (min. 6-8 znaków)**