Zarządzenie Nr 27/2011
Starosty Rybnickiego
z dnia 14 czerwca 2011r.

W sprawie wprowadzenia zasad ochrony danych osobowych, bezpieczeństwa informacji oraz bezpieczeństwa systemów informatycznych w Starostwie Powiatowym w Rybniku.

Działając na podstawie ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. Nr 101, poz. 926 z 2002r., z późn. zm.), § 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. 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. Nr 100 poz. 1024)

zarządzam, co następuje:

§ 1

1. Powierzam Pani Danucie Iciaszczyk-Osubniak – inspektorowi w Wydziale Organizacyjnym, koordynowanie spraw związanych z ochroną danych osobowych w Starostwie Powiatowym w Rybniku i wyznaczam w/w do pełnienia funkcji Administratora Bezpieczeństwa Informacji
2. W razie nieobecności Pani Danuty Iciaszczyk-Osubniak funkcję Administratora Bezpieczeństwa Informacji pełni Monika Cieślik

§ 2

1. Wprowadzam Instrukcję Polityki Bezpieczeństwa Informacji Starostwa Powiatowego w Rybniku, stanowiącą załącznik Nr 1 do niniejszego Zarządzenia.
2. Do w/w włączam następujące akty:

- Zarządzenie Nr 3/07 Starosty rybnickiego z dnia 15 maja 2007r. w sprawie zasad bezpieczeństwa informatycznego w Starostwie Powiatowym w Rybniku
- Instrukcję Nr 1 Zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych
- Instrukcję Nr 2 Postępowanie w przypadku stwierdzenia naruszenia ochrony danych osobowych dla osób zatrudnionych przy przetwarzaniu danych osobowych
- Instrukcję Nr 3 Identyfikacja użytkownika w systemie informatycznym przetwarzającym dane osobowe

§ 3

Kierownicy Komórek Organizacyjnych Starostwa Powiatowego złożą w terminie do dnia 30 lipca br. do Sekretarza Powiatu wnioski o wydanie upoważnienia do przetwarzania danych osobowych i dostępu do systemu informatycznego(wzór stanowi Załącznik Nr 2 do Polityki Bezpieczeństwa).

§ 4

Wykonanie Zarządzenia powierzam Sekretarzowi Powiatu

§5

Traci moc Zarządzenie Nr 16/2011 Starosty Rybnickiego z dnia 21 marca 2011r.

§ 6

Niniejsze Zarządzenie wchodzi w życie z dniem podpisania

STAROSTA
inż. Damian Mrowiec

Załącznik Nr 1

do Zarządzenia Nr 27/2011

Starosty Rybnickiego z dnia14 czerwca 2011r.

INSTRUKCJA

Polityki Bezpieczeństwa Informacji

Starostwa Powiatowego w Rybniku

§1

Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Rybniku jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych zawartych w zbiorach danych zapisanych w formie papierowej lub elektronicznej.

§2

Przetwarzanie danych osobowych w Starostwie Powiatowym w Rybniku dopuszczalne jest tylko pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101 poz.926 z późn. zm.) i wydanych na jej podstawie przepisów wykonawczych oraz Zarządzenia Starosty Rybnickiego Nr 27/2011 z dnia 14 czerwca 2011r., a także przepisów wdrożonych w załącznikach do niniejszej INSTRUKCJI.

§3

Przez użyte w treści Instrukcji sformułowania należy rozumieć:

- **dane osobowe** to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
- **zbiór danych** to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy podzielony funkcjonalnie
- **przetwarzanie danych** to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym
- **system informatyczny** to zespół współpracujących ze sobą urządzeń , programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
- **zabezpieczenie danych w systemie informatycznym** to wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieupoważnionym przetwarzaniem
- **usuwanie danych** to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
- **ADO** to Administrator Danych Osobowych
- **ABI** to Administrator Bezpieczeństwa Informacji – zarządza bezpieczeństwem informacji

- **ASI** to Administrator Systemu Informatycznego – zarządza bezpieczeństwem systemu informatycznego

§4

ADO, o którym mowa w Instrukcji jest Starosta, który ponosi całkowitą odpowiedzialność za ochronę danych osobowych w starostwie Powiatowym w Rybniku. Może on wyznaczyć inne osoby (ABI i ASI) do realizacji całości lub części uprawnień lub zadań ADO chyba, że sam wykonuje te czynności. W tym celu wydaje upoważnienie, którego wzór stanowi ***załącznik nr1.***
Upoważnienie takie może zostać w każdej chwili cofnięte lub wygasać samoistnie.
Wzór odwołania upoważnienia stanowi ***załącznik nr 2***

§5

Dostęp do zbioru danych osobowych oraz ich przetwarzania w Starostwie Powiatowym w Rybniku maja wyłącznie osoby które:
- zostały wpisane do ewidencji (wzór ***załącznika nr 3)***, prowadzonej przez ABI na podstawie upoważnienia, którego wzór stanowi ***załącznik nr 4 część A.*** Upoważnienie może wygasać samoistnie lub zostać cofnięte – wzór stanowi ***załącznik nr 5***
- upoważnienie wydaje się na pisemny wniosek bezpośredniego przełożonego. Wzór wniosku o wydanie upoważnienia do przetwarzania danych osobowych i dostępu do systemu informatycznego stanowi ***załącznik nr 6***
- przed przystąpieniem do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych zapoznały się z obowiązującymi zasadami ochrony tych danych, a fakt ten udokumentowany jest podpisaniem oświadczenia, którego wzór stanowi ***załącznik nr 4 część B***
- w zakresie czynności odpowiada za ochronę danych osobowych

Załącznik Nr 4 przechowuje: 1x ABI, 1x akta osobowe

§6

Osoby zatrudnione w Starostwie Powiatowym w Rybniku przy przetwarzaniu danych osobowych są zobowiązane do:
- legalnego przetwarzania danych osobowych z zachowaniem §1 i §2 niniejszej Instrukcji
- postępowania zgodnie z postanowieniami zawartymi w Zarządzeniu Nr 3/07 Starosty Rybnickiego z dnia 15 marca 2007r. w sprawie zasad bezpieczeństwa informatycznego w Starostwie Powiatowym w Rybniku
- powiadomienia ABI o ewentualnych naruszeniach systemu bezpieczeństwa ochrony danych osobowych we wszystkich zbiorach. Tryb postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych określa Instrukcja stanowiąca ***załącznik nr 7***
- zachowania tajemnicy uzyskanych danych osobowych oraz sposobu ich zabezpieczenia *(patrz załącznik nr 4 część B)*
- pełnej ochrony danych osobowych, zawartych w laptopach służbowych, za które odpowiadają, jako dysponenci

§7

W Starostwie Powiatowym w Rybniku zabrania się przetwarzania danych ujawniających:
- pochodzenie rasowe lub etniczne
- poglądy polityczne
-przekonania religijne i filozoficzne
-przynależność wyznaniową
-przynależność partyjną lub związkową
- stan zdrowia, kod genetyczny, nałogi lub fakty z życia seksualnego
chyba, że pozwalają na to obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła na to pisemną zgodę, która to znajduje się w jej teczce osobowej.

§8

Pracownik, który:
- przetwarza dane osobowe, do których przetwarzania nie jest upoważniony, których przetwarzanie jest zabronione lub niezgodne z celem stworzenia zbioru
- udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym
- nie zgłasza ABI zbiorów danych podlegający rejestracji
- uniemożliwia osobie, której dane dotyczą korzystanie z przysługujących jej praw
podlega odpowiedzialności karnej zgodnie z ustawą oraz przepisami Kodeksu pracy.

§9

Wykonywanie czynności przetwarzania danych osobowych ze zbiorów Starostwa przez inne osoby (podmioty) nie będące pracownikami Starostwa jest dopuszczalne tylko po zawarciu pisemnej umowy powierzenia danych osobowych, której wzór stanowi ***załącznik nr 8***

§10

Dane osobowe przetwarzane w starostwie Powiatowym w Rybniku mogą być uzyskiwane:
- bezpośrednio od osób, których te dane dotyczą
- z innych źródeł, w granicach dozwolonych przepisami prawa

§11

Zbierane dane osobowe muszą być wykorzystane tylko do celów, w jakich są lub będą przetwarzane. Po ich wykorzystaniu powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.

§12

Kandydaci do pracy w Starostwie Powiatowym w Rybniku zobowiązani są przedłożyć pisemną zgodę na przetwarzanie ich danych w celach rekrutacyjnych. Dokumenty CV są przechowywane w komórce organizacyjnej, która je przetwarza.

§13

Jeżeli przepis szczególny nie stanowi inaczej udostępnienie danych osobowych innej osobie (podmiotowi) może nastąpić tylko na pisemny wniosek.

W razie udostępnienia danych osobowych przetwarzanych w systemie informatycznym należy odnotować w nim informację o odbiorcy danych oraz data i zakres udostępnienia.

Odmowa udostępnienia danych osobowych powinna mieć formę pisemną z adnotacją o prawie złożenia bezpośrednio do GIODO wniosku o wydanie decyzji nakazującej udostępnienie danych.

§14

Kierownicy komórek organizacyjnych Starostwa Powiatowego w Rybniku, w których przetwarzane są dane osobowe są zobowiązani do zgłoszenia do ABI:
- konieczności zawarcia umowy powierzenia przetwarzania danych osobowych ze zbiorów Starostwa przez inne osoby nie będące pracownikami starostwa
- planowanego rejestrowania nowych zbiorów danych osobowych,
- zmian w zakresie informacji w zbiorach już zgłoszonych (oba w terminie 30 dni od dnia dokonania zmiany w zbiorze danych)
- wykreślenia zbioru danych osobowych, jeżeli zaprzestano przetwarzania w nim danych osobowych w formie pisemnej wraz ze wskazaniem uzasadnienia do wykreślenia.
Wszelkich zmian należy dokonywać na odpowiednich formularzach dostępnych na stronie Głównego Inspektora Ochrony Danych Osobowych

§15

Kierownicy komórek organizacyjnych Starostwa Powiatowego w Rybniku są odpowiedzialni za stan bezpieczeństwa informacji w zakresie swojego wydziału/ referatu i sprawują nadzór nad przestrzeganiem zasad polityki bezpieczeństwa.

§16

Osoby przetwarzające dane osobowe w Starostwie Powiatowym w Rybniku zobowiązane są do przestrzegania następujących zasad i środków ochrony fizycznej obszaru przetwarzania danych osobowych w Starostwie Powiatowym w Rybniku:
- przed otwarciem pomieszczeń należy wizualnie sprawdzić stan drzwi, zamków ewentualnie innych zabezpieczeń zastosowanych przy zamykaniu pomieszczeń czy nie uległy uszkodzeniom;
- po wejściu do pomieszczenia stwierdzić stan zabezpieczeń sprzętu biurowego i składanych w nich dokumentów zawierających akta osobowe oraz stan zabezpieczenia komputerowego;
- w trakcie pracy skutecznie uniemożliwić osobom postronnym dostęp do danych osobowych;
- po zakończeniu dnia pracy należy bezwzględnie uporządkować swoje stanowisko pracy, wykonać czynności zabezpieczające adekwatne do zastosowanych rozwiązań technicznych i organizacyjnych, głownie polegających na:

- zabezpieczeniu dokumentacji przed jakimkolwiek dostępem do nich osób trzecich tzw. zasada „czystych biurek"
- zabezpieczeniu komputerów i wszelkich nośników danych
- wyłączeniu wszystkich urządzeń elektrycznych typu grzejnik, czajnik, wentylator itp. zgodnie z zasadami BHP
- zamknięciu okien i drzwi

- stosownym zamknięciu biurek, szaf i pomieszczeń
- niszczeniu zapisanych kartek, kopert, notatek podręcznych, itp. nie stanowiących dokumentacji w sprawie a zawierających dane osobowe, czyli niszczeniu tych wszystkich w taki sposób, aby uniemożliwić odtworzenie danych

- dokumenty zawierające dane osobowe przechowywać w pomieszczeniach i meblach zamykanych na klucz
- zasady postępowania z kluczami do pomieszczeń określone są w Zarządzeniu Starosty Rybnickiego Nr 7/07 z dnia 10 lipca 2007r. w sprawie zasad zabezpieczenia pomieszczeń Starostwa Powiatowego w Rybniku przed włamaniem – ***załącznik Nr 9***
- zasady bezpieczeństwa informatycznego w Starostwie Powiatowym w Rybniku określone są w Zarządzeniu Nr 3/07 Starosty Rybnickiego z dnia 15 marca 2007r. - ***załącznik nr 10*** oraz Instrukcja Nr 1 zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych zatwierdzona dn. 04.10.1999r. przez Starostę Rybnickiego – ***załącznik nr 11***

§17

W celu realizacji powierzonych zadań ABI ma prawo:
- kontrolować komórki Starostwa Powiatowego w Rybniku w zakresie właściwego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe i sporządzać raporty
- wydawać zalecenia i polecenia kierownikom i pracownikom Starostwa w zakresie bezpieczeństwa danych osobowych i składać raporty Starości również ustnie z przeprowadzonych kontroli
- żądać od wszystkich pracowników Starostwa Powiatowego w Rybniku wyjaśnień w sytuacji naruszenia bezpieczeństwa danych osobowych. Odmowa udzielenia wyjaśnień lub współpracy z ABI traktowane będzie jako naruszenie obowiązków pracowniczych.

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

UPOWAŻNIENIE NR .....

DO PEŁNIENIA FUNKCJI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Na podstawie art. 36 ust. 3 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2002 r. Nr 101, poz. z późn. zm.),

u p o w a ż n i a m

Panią/ Pana .....

zatrudnioną/nego w Starostwie Powiatowym w Rybniku

na stanowisku.....

do pełnienia funkcji Administratora Bezpieczeństwa Informacji

w okresie od ..... do .....[1]

w ramach wykonywania czynności służbowych.

Zadania ABI określa polityka bezpieczeństwa danych osobowych.

Administrator Danych Osobowych

.....
/data, pieczęć i podpis/

Zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych z 29 sierpnia 1997 roku (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), również po ustaniu stosunku pracy oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.

.....
/data i podpis osoby upoważnionej/

[1] Należy podać datę ważności upoważnienia lub wpisać „odwołania"

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

ODWOŁANIE NR .....

UPOWAŻNIENIA DO PEŁNIENIA FUNKCJI
ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Niniejszym odwołuję z dniem ..... upoważnienie nr ..... do pełnienia funkcji administratora bezpieczeństwa informacji wydane dnia.....

dla Pani/Pana .....

Administrator Danych Osobowych

.....
/data, pieczęć i podpis/

Załącznik Nr 3 do Polityki Bezpieczeństwa Informacji Starostawa Powiatowego w Rybniku

WZÓR EWIDENCJI OSÓB UPOWAZNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH					*str.....*
Lp.	**Imię i Nazwisko**	**Data nadania upoważnienia**	**Data ustania upowaznienia**	**Zakres upoważnienia**	**Identyfikator (dot.przetwarzania danych w systemie informatycznym)**
1					

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

część A

UPOWAŻNIENIE NR .....
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),

upoważniam

Pana/ią .....
zajmującą stanowisko.....
do wykonywania czynności związanych z przetwarzaniem danych osobowych gromadzonych w zbiorze danych osobowych o nazwie
„.....”
w okresie od ..... do ...../w czasie zatrudnienia w Starostwie Powiatowym w Rybniku * w ramach wykonywania czynności służbowych.

Upoważnienie obejmuje/ nie obejmuje* uprawnienie do pracy w lokalnym systemie informatycznym.
Upoważnienie nie może być przeniesione na innych pracowników ponadto może być w każdym czasie zmienione lub odwołane.

Administrator Danych Osobowych

Rybnik, dnia..... .....
/pieczęć i podpis/

---

część B

Ja, niżej podpisany/a zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, do których mam (będę miał/a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Starostwie Powiatowym w Rybniku, zarówno w trakcie obecnie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia. Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Starostwie wiążących się z ochroną danych osobowych. Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu pracy.

Rybnik dnia..... .....
/podpis osoby upoważnionej/

* - niepotrzebne skreślić

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

ODWOŁANIE NR .....

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym odwołuję z dniem ..... upoważnienie Nr ..... do przetwarzania danych osobowych wydane dla Pani/Pana .....

Administrator Danych Osobowych

.....
/data, pieczęć i podpis/

Załącznik Nr 6
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

WNIOSEK

O WYDANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH

Proszę o wydanie upoważnienia dla Pana/i .....

do przetwarzania danych osobowych w Starostwie Powiatowym w Rybniku

w Wydziale/Referacie.....

w zbiorze zawierającym dane osobowe o nazwie :

1.....

2 .....

3.....

w formie papierowej/elektronicznej* w ramach wykonywania czynności służbowych.

Rybnik, dnia.....

.....
(pieczątka i podpis bezpośredniego
przełożonego/kierownika komórki organizacyjnej)

* niepotrzebne skreślić

Załącznik nr 7
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

INSTRUKCJA
POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Cel instrukcji postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych

Celem niniejszego dokumentu jest określenie zasad postępowania użytkowników oraz administratorów bezpieczeństwa informacji w przypadku naruszenia bezpieczeństwa informacji dotyczących przetwarzania danych osobowych.

2. Definicja naruszenia bezpieczeństwa informacji

Przez naruszenie bezpieczeństwa informacji należy rozumieć wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata (np. kradzież lub zniszczenie) lub nieuzasadniona modyfikacja danych lub części danych (nawet, jeśli możliwe jest całkowite odtworzenie utraconych danych), a także możliwość dostępu do danych dla osób nieposiadających upoważnienia do ich przetwarzania.

Incydentem naruszenia bezpieczeństwa określa się każde określone zdarzenie lub działanie, naruszające bezpieczeństwo lub zasady ochrony informacji.

Na możliwość wystąpienia naruszenia bezpieczeństwa informacji mogą wskazywać:

- Nietypowy stan pomieszczeń przetwarzania (uszkodzone drzwi, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia);
- Zaginięcie sprzętu lub nośników informacji (dyskietek, dokumentów papierowych, itp.);
- Nieuzasadnione modyfikacje lub usunięcie danych, niezgodności w danych;
-

3. Obowiązki użytkownika

3.1. Po stwierdzeniu lub podejrzeniu wystąpienia incydentu naruszenia bezpieczeństwa informacji użytkownik powinien:

- Powstrzymać się od wszelkich czynności w pomieszczeniu przetwarzania mogących zatrzeć ślady naruszenia bezpieczeństwa informacji;
- Po zgłoszeniu incydentu do ABI lub ASI, zastosować się do ich poleceń;
- Sporządzić notatkę o zdarzeniu, jeśli ADO wyda takie polecenie. Notatka powinna zawierać: datę, godzinę, opis zdarzenia, informacje jakie dane zostały utracone lub zmodyfikowane, opis przebiegu zdarzeń poprzedzających.

W żadnym wypadku użytkownikowi nie wolno: porzucać, wyrzucać do śmieci, niszczyć lub

sprawdzać zawartość znalezionych nośników informacji.

3.2. Zgłaszanie incydentów

Użytkownicy systemów informatycznych i nieinformatycznych są zobowiązani do:

a) natychmiastowego informowania ABI oraz bezpośredniego przełożonego w przypadku:

- Stwierdzenia włamania i/lub kradzieży sprzętu lub nośników zawierających dane osobowe;
- Stwierdzenia zaginięcia nośnika zawierającego dane osobowe (wydruku, kopii bezpieczeństwa, dyskietki, itp.);
- Znalezienia poza pomieszczeniami przetwarzania wszelkich dokumentów, wydruków, dyskietek i innych nośników informacji;
- Przesłania danych osobowych do niewłaściwego miejsca lub adresata.

Użytkownik zobowiązany jest także do niezwłocznego zgłaszania ADO wszelkich wykrytych lub podejrzewanych słabości systemu lub zagrożeń z nimi związanych.

3.3 Postępowanie po wykryciu lub otrzymaniu zgłoszenia o incydencie

W przypadku otrzymania zgłoszenia o wystąpieniu lub podejrzeniu wystąpienia incydentu, ABI powinien:

- Ustalić, czy incydent rzeczywiście miał miejsce;
- Zabezpieczyć dowody zdarzenia;
- Zalecić użytkownikowi sposób dalszego postępowania lub, jeśli podejrzenie naruszenia bezpieczeństwa nie zostało potwierdzone, poinformować go o możliwości kontynuowania pracy

- Zawiadomić ADO o incydencie

4. Analiza incydentu

Dalsze działania związane z analizą skutków incydentu oraz opracowaniem zaleceń mających na celu podniesienie poziomu bezpieczeństwa systemu, przeprowadza komisja powołana przez ADO.

Analiza incydentu obejmuje sprawdzenie i ustalenie, m.in.:

- Stanu zabezpieczeń fizycznych;
- Stanu informacji (czy została zmodyfikowana, utracona lub ujawniona);
- Czy miał miejsce dostęp osób nieupoważnionych do zasobów;
- Czy miało miejsce, celowe lub przypadkowe, przekroczenie uprawnień przez osoby upoważnione;

Raport z analizy incydentu komisja przedkłada ADO. W zależności od celu i określonego zakresu działania komisji, raport może zawierać ocenę przyczyn incydentu oraz opinię, czy incydent był przypadkowy, czy spowodowany celowo. Jeżeli incydent został spowodowany nieprzestrzeganiem procedur lub błędnymi zapisami w procedurach, to w raporcie powinno być to zaznaczone. Raport powinien również zawierać opis wpływu incydentu na infrastrukturę systemu informatycznego, na stan zbiorów informacji oraz ocenę możliwych negatywnych przyszłych skutków incydentu z podziałem na krótkotrwałe i długofalowe. Raport powinien zawierać, jako wnioski końcowe, zalecenia w celu podniesienia poziomu bezpieczeństwa.

Wszelkie dalsze działania podejmuje ADO.

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
Starostwa Powiatowego w Rybniku

UMOWA POWIERZENIA
PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu.....pomiędzy Starostwem Powiatowym w Rybniku
reprezentowanym przez ..... zwanym
dalej Zleceniodawcą, a.....
z siedzibą ..... ul.....
reprezentowanym przez .....
zwanym dalej Zleceniobiorcą

§ 1

1. Zleceniodawca oświadcza, że jest administratorem zbioru danych osobowych o nazwie ..... w rozumieniu ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. Nr 101 poz. 926 z 2002r. z późn. zm.),
2. Określony w pkt. 1 zbiór danych osobowych zawiera następujące kategorie danych:
.....
.....

§ 2

1. Zleceniodawca upoważnia Zleceniobiorcę do wykonania następujących operacji w zbiorze danych:
.....
.....

2. Zleceniobiorca zobowiązuje się przetwarzać powierzone dane osobowe tylko w zakresie określonym w ust. 1 Jednocześnie zobowiązuje się, że powierzonych danych osobowych nie będzie udostępniał innym podmiotom oraz usunie je po wykonaniu umowy.

3. Zleceniobiorca zobowiązuje się do zastosowania przy przetwarzaniu danych osobowych, o którym mowa w ust. 1 środków technicznych i organizacyjnych zapewniających ochronę danych osobowych co najmniej w zakresie określonym w art. 36-39 ustawy.

4. Zleceniobiorca zobowiązany jest zapewnić aby urządzenia i systemy informatyczne służące do przetwarzania powierzonych mu danych były zgodne z wymogami zawartymi Zarządzeniu Starosty Rybnickiego z dnia ....

§ 3

Zleceniobiorca wykona czynności, o których mowa w § 2 ust. 1 w terminie do .....

§ 4

Strony ustalają wysokość wynagrodzenia na kwotę ..... (słownie .....)
którą Zleceniodawca uiści przelewem na konto Zleceniobiorcy w Banku .....
Nr .....

§ 5

1. Strony umowy podczas realizacji umowy będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie umowy.
2. Zleceniobiorca nie może powierzyć wykonania zadań określonych w niniejszej umowie innemu podmiotowi.
3. Zleceniodawca ma prawo do przeprowadzenia kontroli sposobu wykonania niniejszej umowy.

§ 6

W przypadku naruszenia przepisów ustawy o ochronie danych osobowych z przyczyn leżących po stronie Zleceniobiorcy ponosi on odpowiedzialność karną wynikającą z przepisów art. 49-54 ustawy o ochronie danych osobowych.

§ 7

1. W zakresie nieuregulowanym niniejszą umową mają zastosowanie przepisy ustawy oraz Kodeksu Cywilnego.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Zleceniodawca

Zleceniobiorca

Zarządzenie Nr 7/07oraz 3/07 Starosty Rybnickiego oraz Instrukcja nr 1 zarządzania syst inf. z 1999r stanowią zał. 9-11