Zarządzenie Nr 21/2004

zarządzenie w sprawie powołania Administratora Bezpieczeństwa Informacji Danych Osobowych

ZARZĄDZENIE NR 21/2004
STAROSTY OTWOCKIEGO
z dnia 26 sierpnia 2004 roku.

w sprawie powołania Administratora Bezpieczeństwa Informacji Danych Osobowych

Na podstawie art. 36 w związku z art. 7 pkt. 4 ustawy z dnia 17 czerwca 2004 roku -tekst jednolity „o ochronie danych osobowych" (Dz.U. nr 101, poz. 926 - tekst jednolity) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku „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) zarządza się, co następuje:

§1

1. Wyznaczam pana Grzegorza Hermanowicza jako osobę odpowiedzialną za bezpieczeństwo Danych Osobowych w systemie informatycznym, zwanym dalej Administratorem Bezpieczeństwa Informacji Danych Osobowych.
2. Administrator Bezpieczeństwa Informacji Danych Osobowych jest odpowiedzialny za przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są Dane Osobowe oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń ochrony Danych Osobowych.

§2

Wykonanie zarządzenia powierzam Sekretarzowi Powiatu.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 2

INSTRUKCJA
Określająca sposób zarządzania systemem informatycznym zbioru danych osobowych
Starostwa Powiatowego w Otwocku

Spis treści

Rozdział I Postanowienia ogólne

§1

Niniejsza Instrukcja /zwana dalej: instrukcją/, jest wewnętrznym dokumentem Starostwa powiatowego w Otwocku, /zwanego dalej: Administratorem/ i ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemie informatycznym Administratora.

§2

1. Instrukcja określa i tryb postępowania Administratora Danych i osób przez niego upoważnionych przy korzystaniu z danych osobowych.
2. Instrukcja została opracowana zgodnie z wymogami § 3 ust. 1 rozporządzenia ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024.).

§3

Następujące słowa, użyte w Instrukcji, oznaczają:
• administrator danych - Starostwo Powiatowe w Otwocku, zwany dalej Administratorem;
• administrator Bezpieczeństwa Informacji (ABI) - osoba wyznaczona przez administratora danych, odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
• osoba upoważniona lub użytkownik - osoba posiadająca upoważnienie wydane przez Administratora i dopuszczona w zakresie w nim wskazanym, jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych;
• osoba trzecia - to każda osoba nieupoważniona i przez to nieupoważniona do dostępu do danych osobowych lub zbiorów tych danych, będących w posiadaniu Administratora. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Administratora podejmująca czynności w zakresie przekraczającym ramy udzielonego jej upoważnienia;
• system informatyczny - system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje;
• zabezpieczenie systemu informatycznego - wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów technicznych oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią.

§4

1. Administrator Bezpieczeństwa Informacji może zlecić innej osobie, zatrudnionej u Administratora, dokonywanie czynności leżących w zakresie obowiązków ABI.
2. Kontrola prawidłowości wykonania ww. czynności należy do ABI.
3. Osoba o której mowa w ust. 1 niezwłocznie informuje ABI o podjętych czynnościach.

Rozdział II Przydział haseł i identyfikatorów

§5

Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizm uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych, dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło, tak aby bezpośredni dostęp do tych danych przetwarzanych w systemie informatycznym mógł mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników. Hasło znane jest tylko właścicielowi.

§6

Identyfikator użytkownika
1) jest niepowtarzalny a po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielony innej osobie;
2) jest wpisywany do ewidencji osób zatrudnionych przy przetwarzaniu danych wraz z imieniem i nazwiskiem użytkownika przez jest rejestrowany w systemie informatycznym.

§7

Hasło użytkownika:
1) jest przydzielane indywidualnie dla każdego z użytkowników i znane tyko użytkownikowi, który się nim posługuje;
2) nie jest zapisywane w systemie w postaci jawnej;
3) jest zmieniane co najmniej raz na 3 miesiące;
4) jest utrzymywane w tajemnicy, również po upływie jego ważności.

§8

Osobą odpowiedzialną za sposób przydziału haseł dla użytkowników, częstotliwość ich zmiany oraz rejestrację jest Administrator Bezpieczeństwa Informacji.

§9

3) hasła użytkowników nie mogą się powtarzać. Hasła nie mogą składać się z kombinacji znaków mogących ułatwić odszyfrowanie ich przez osoby nieupoważnione np. imię, nazwisko itp.;
4) hasło winno być zmienione przez użytkownika niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.

§10

1. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.
2. Użytkownik obowiązany jest utrzymywać hasła którymi się posługuje lub posługiwał w ścisłej tajemnicy, co obejmuje, w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem nawet po ustaniu jego ważności, czy też użycia hasła przez te osoby.
3. Naruszenie przez użytkownika postanowień ust. 1 lub 2 może stanowić podstawę dla pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.

Rozdział III

§11

1. Rejestrowanie i wyrejestrowania użytkowników dokonuje Administrator Bezpieczeństwa Informacji który prowadzi ewidencję.
2. Ewidencja zawiera:
- imię i nazwisko użytkownika,
- wskazanie komórki organizacyjnej, w której jest zatrudniony,
- identyfikator,
- datę zarejestrowania,
- datę wyrejestrowania,

3. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji podlega natychmiastowemu odnotowaniu.

§12

Aby dana osoba była zarejestrowana w systemie informatycznym, jako użytkownik muszą być spełnione następujące warunki:
1) Administrator musi wydać upoważnienie dopuszczające daną osobę w zakresie w nim wskazanym, jako użytkownika, do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych,
2) Administrator Bezpieczeństwa Informacji musi uzyskać informacje konieczne do zdefiniowania dla danej osoby jej profilu jako użytkownika oraz jej uprawnień. Informacji takich udziela osoba odpowiedzialna pod względem merytorycznym co do charakteru pracy danej osoby, mającej być użytkownikiem, mając na względzie treść wydanego tej osobie przez Administratora upoważnienia.

§13

Z chwilą zarejestrowania w systemie informatycznym, dana osoba jest informowana przez Administratora bezpieczeństwa Informacji o ustalonym dla niej identyfikatorze i konieczności posługiwania się hasłami.

§14

Użytkownik jest wyrejestrowany z systemu informatycznego w każdym przepadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
• ustania zatrudnienia tego użytkownika u Administratora - o czym informację Administrator Bezpieczeństwa Informacji uzyskuje od upoważnionego pracownika Działu Kadr, bądź od przełożonego użytkownika,
• zmiany zakresu obowiązków tego użytkownika - o czym informację Administrator Bezpieczeństwa Informacji uzyskuje od przełożonego użytkownika.

§15

Zmiany dotyczące użytkownika, takie jak:
1) rozwiązanie umowy o pracę,
2) utrata upoważnienia,
powodują wyrejestrowanie użytkownika, w trybie natychmiastowym, z ewidencji, o której mowa w § 3 ust. 1, jako identyfikatora z systemu informatycznego oraz unieważnienie hasła tego użytkownika.

§16

1. identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. ABI obowiązany jest gromadzić odrębnie identyfikatory, które utraciły ważność.
Rozdział IV Rozpoczęcie i zakończenie pracy w systemie

§17

Każdy użytkownik rozpoczynając pracę obowiązany jest „załogować się" do systemu komputerowego Administratora posługując się swoim identyfikatorem i hasłem.

§18

1. Maksymalna ilość prób wprowadzania hasła przy logowaniu się systemu wynosi.....
2. Po przekroczeniu liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika.
3. Użytkownik informuje ABI o zablokowaniu dostępu do zbioru danych, który ustala przyczyny zablokowania systemu oraz podejmuje odpowiednie działania.

§19

1. W przypadku bezczynności użytkownika na komputerze stacjonarnym przez dłuższy niż .....minut automatycznie włączony jest wygaszacz ekranu.
2. Wygaszacze ekranu powinny być zaopatrzone w hasła. Regulacje odnoszące się do haseł używanych przez użytkownika przy logowaniu, stosuje się odpowiednio do haseł wygaszacza.
3. Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz.
4. W przypadku, gdy przerwa w pracy trwa dłużej niż ..... minut, oraz kończąc
pracę użytkownik obowiązany jest „wylogować się" z aplikacji i systemu komputerowego oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka używane przez niego szafy i pomieszczenia, w których przechowuje się dokumentacje i nośniki informacji.

§20

1. W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego lud zauważenia, że stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych osobowych, użytkownik ten obowiązany jest postępować zgodnie z „Instrukcją postępowania w sytuacji naruszenia danych osobowych".
2. Użytkownik winien zwrócić na te okoliczności szczególną uwagę podczas rozpoczynania pracy.
Rozdział V
Tworzenie oraz przechowywanie kopii awaryjnych

§21

Za tworzenie i przechowywanie kopii awaryjnych w sposób zgodny z przepisami ustawy oraz poniższymi procedurami odpowiedzialny jest ABI.

§22

Kopie awaryjne są:
1) tworzone co.....dni oraz raz na.....sprawdzane pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
2) przechowywane w innych pomieszczeniach niż zbiory danych osobowych eksploatowane na bieżąco.

§23

1. Kopiowanie danych osobowych na nośniki informacji i robienie wydruków tych danych jest zabronione, chyba że konieczność ich sporządzania wynika z nałożonego na użytkownika zakresu obowiązków i jest uzasadniona potrzebą ich wykonywania oraz dozwolona przepisami prawa.

2. Wykorzystywanie nośników informacji lub wydruków i innym celu niż wskazany w ust. 1 jest zakazane.

§24

1. Kopie zapasowe po ustaniu ich użyteczności są bezzwłocznie wsuwane.
2. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
3. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
Rozdział VI Ochrona systemu informatycznego przed wirusami komputerowymi

§25

1. Na bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych pozwala oprogramowanie automatycznie monitorujące występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
2. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych w systemie, jak i do celów instalacyjnych.

§26

Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje Administrator Bezpieczeństwa Informacji.

§**27**

O każdokrotnym wykryciu wirusa przez oprogramowanie monitorujące użytkownik obowiązany jest niezwłocznie poinformować Administratora Bezpieczeństwa Informacji.

§28

1. Po usunięciu wirusa ABI sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
2. Administrator Bezpieczeństwa Informacji prowadzi rejestr przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych
w systemie.

Rozdział VII
Przechowywanie nośników informacji w tym kopii informatycznych i wydruków komputerowych

§29

Nośniki informacji w tym kopie informatyczne i wydruki komputerowe przechowuje się wyłącznie wówczas, gdy jest to konieczne i dozwolone przepisami prawa.

§30

Nośniki informacji przechowuje się w specjalnie w tym celu przygotowanych pomieszczeniach w:
1) szafach lub
2) innych meblach biurowych
posiadających zamknięcia uniemożliwiające dostęp do osób trzecich

§31

1. Pomieszczenia służące do przechowywania nośników informacji wyznaczone są przez ABI.
2. Pomieszczenia te powinny posiadać:
1) wewnętrzne ściany, gwarantujące trwałe oddzielenie ich od innych pomieszczeń;
2) pełne drzwi wejściowe zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania, tj. w szczególności zamek patentowy lub szyfrowy;
3) odpowiednie zabezpieczenie okien przed dostępem z zewnątrz i obserwacją;
4) oznakowanie i odpowiednie wywieszki zabraniające osobom trzecim wstępu i przebywania w tych pomieszczeniach.
3. W razie uzasadnionej potrzeby stosuje się dalej idące środki bezpieczeństwa.

§32

Szafy lub inne meble biurowe służące do przechowywania nośników informacji winny być:
1) zaopatrzone w co najmniej jeden zamek o skomplikowanym mechanizmie otwierania tj. w szczególności zamek patentowy lub szyfrowy;
2) po zakończeniu pracy zamknięte i w miarę możliwości opieczętowane.

Rozdział VIII Przeglądy i konserwacja systemu oraz zbioru danych osobowych

§33

Przeglądy i konserwacje sprzętu komputerowego wynikające z obciążenia sprzętu komputerowego, warunków zewnętrznych w których eksploatowane są dane urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego dokonywane są przez ABI.

§34

1. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy, gdzie wymagane jest zaangażowanie autoryzowanych firm zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora.
2. Wydruki komputerowe są bezzwłocznie usuwane po ustaniu użyteczności, czego dokonać można w szczególności poprzez zniszczenia ich w sposób trwały, tj. za pomocą niszczarki.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, 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, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały, tj. w sposób mechaniczny.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych, postępując zgodnie z ust. 3.
5. Trwałego zniszczenia zbędnych nośników i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

Rozdział IX Postępowanie w zakresie komunikacji w sieci komputerowej

§35

1. Komunikacja w sieci komputerowej jest dozwolona jedynie po właściwym załogowaniu się i podaniu własnego hasła użytkownika.
2. Wprowadzenie do systemu informatycznego informacji z zewnątrz, w tym danych osobowych, jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i tylko przez użytkownika zgodnie z zakresem jego obowiązków i wynikających z nich uprawnień.

§36

1. Konfiguracja systemu informatycznego jest dokonywana wyłącznie przez Administratora Bezpieczeństwa Informacji lub upoważnione przez niego osoby.
2. Jakiekolwiek zmiany konfiguracji systemu informatycznego są protokołowane.
3. W celu uniemożliwienia niekontrolowanej wymiany informacji, w tym danych osobowych, lub modyfikacji systemu informatycznego zapewniona jest maksymalna konfiguracja komputerowych stanowisk pracy.

Rozdział X
Wymagania sprzętowo - organizacyjne w zakresie ochrony przetwarzania danych osobowych

§37

sprzęt odsługujący zbiór danych Starostwa składa się z najwyższej klasy komputerów stacjonarnych klasy PC, zlokalizowanych w wydzielonych pomieszczeniach siedziby Administratora.

§38

1. Baza danych osobowych Starostwa przetwarzana jest na serwerze.
2. Serwer zamontowany jest w zamkniętej szafie i posiada własne zabezpieczenia.
gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały, tj. w sposób mechaniczny.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych, postępując zgodnie z ust. 3.
5. Trwałego zniszczenia zbędnych nośników i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

Rozdział IX Postępowanie w zakresie komunikacji w sieci komputerowej

§39

1. Ekrany monitorów ustawione są do wewnątrz sali wydzielonej do przetwarzania danych osobowych, w taki sposób, by uniemożliwić wgląd lub spisanie zawartości aktualnie wyświetlonej na ekranie monitora.
2. Osoby nieuprawnione do dostępu do danych osobowych mogą przebywać w pomieszczeniach w których przetwarzane są dane osobowe wyłącznie w obecności co najmniej jednego użytkownika, po uzyskaniu zgody Administratora.

§40

Decyzję o instalacji oprogramowania systemowego oraz oprogramowania użytkowego obsługującego przetwarzanie danych osobowych, podejmuje ABI.

§41

Administrator Bezpieczeństwa Informacji dokonuje doraźnych kontroli sprawności funkcjonowania zabezpieczeń nie rzadziej niż raz na 3 miesiące.

Rozdział XI Postanowienia końcowe

§42

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych obowiązany jest zapoznać się z Instrukcją ABI może nadzorować dział szkoleń lub prowadzić szkolenie.
2. W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) i rozporządzenia Ministra Spraw wewnętrznych i Administracji z dnia 3 czerwca 1998 roku 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 z późn. zm.).

§43

Instrukcja wchodzi w życie z dniem podpisania.