Załącznik Nr 1 do Zarządzenia Nr 28/12
Burmistrza Pisza

Instrukcja
zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych

§ 1.

Dla każdego użytkownika systemu informatycznego, w którym przetwarza się dane osobowe, administrator bezpieczeństwa informacji ustala odrębny identyfikator i hasło. Hasła zmieniane są nie rzadziej niż raz na miesiąc i nie mogą być one zapisywane w miejscu dostępnym dla osób nieuprawnionych.

§ 2.

Administrator Bezpieczeństwa Informacji prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych zapisując identyfikator, pierwsze hasło oraz imię i nazwisko użytkownika, umożliwiając dostęp do systemu informatycznego, utrzymując je w tajemnicy, również po upływie ich ważności.

§ 3.

Administrator Bezpieczeństwa Informacji na bieżąco rejestruje i wyrejestrowuje użytkowników systemu gdy uzyskują lub tracą prawo do dostępu do systemu informatycznego. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego oraz unieważnić jej hasło.

§ 4.

Do obsługi programu komputerowego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, użytkownik może być dopuszczony wyłącznie posiadając upoważnienie wydane przez Administratora Bezpieczeństwa Informacji.

§ 5.

Bezpośredni dostęp do danych użytkownik ma dopiero po podaniu identyfikatora i właściwego hasła. Użytkownik nie może udostępniać identyfikatora, hasła i stanowiska roboczego osobom nieuprawnionym.

§ 6.

Przed rozpoczęciem pracy użytkownik powinien się upewnić, czy nie zostało naruszone zabezpieczenie systemu informatycznego. W przypadku jakichkolwiek podejrzeń co do tych zabezpieczeń należy niezwłocznie powiadomić o tym fakcie administratora danych osobowych lub inną upoważnioną przez niego osobę.Uruchamianie komputera użytkownik powinien przeprowadzać bez obecności osób postronnych (chodzi o ochronę haseł systemu).

§ 7.

Użytkownik ma obowiązek zamykania systemu i programu po zakończeniu pracy. Stanowisko komputerowe z uruchomionym systemem i programem nie może pozostać bez kontroli pracującego na nim użytkownika.

§ 8.

Jeżeli istnieją odpowiednie możliwości techniczne należy stosować ekranowe wygaszacze, które po określonym czasie nieaktywności użytkownika wygaszają monitor. Kontynuowanie pracy możliwe jest tylko po podaniu określonego hasła.

§ 9.

W pomieszczeniu przetwarzania danych osobowych monitory komputerowe powinny być ustawione w taki sposób aby uniemożliwić osobom nieuprawnionym wgląd w dane.

§ 10.

Pomieszczenia, w których przetwarzane są dane osobowe powinny być zabezpieczone przed dostępem do nich osób nieposiadających uprawnień. Osoby nieposiadające uprawnień wydanych zgodnie z "Instrukcją ochrony danych osobowych w Urzędzie Miejskim w Piszu" stanowiącą załącznik Nr 4 do Zarządzenia Nr 28/12 Burmistrza Pisza z dnia 28 marca 2012r. w sprawie wprowadzenia w Urzędzie Miejskim w Piszu wewnętrznych uregulowań dotyczących ochrony danych osobowych, mogą przebywać w nich jedynie w obecności osób uprawnionych.

§ 11.

Kopie awaryjne należy wykonywać codziennie na taśmach oraz płytach DVD.

§ 12.

Okres przechowywania nośników danych jest uzależniony od przydatności tych danych. Po upływie tego okresu należy je wykorzystać do nowych kopii lub w przypadku ich nieprzydatności – należy je zniszczyć w sposób uniemożliwiający ich odczyt.

§ 13.

Wszelkie wydruki oraz kartoteki zawierające dane osobowe należy przechowywać w miejscach uniemożliwiających ich odczyt przez osoby nieuprawnione (zamykać w szafach metalowych lub drewnianych), zaś po upływie czasu ich przydatności – przekazywać do archiwum lub niszczyć np. w niszczarkach.

§ 14.

Przynajmniej raz w miesiącu systemy komputerowe, programy oraz nośniki należy sprawdzać na obecność wirusa przy pomocy programów antywirusowych.

§ 15.

Należy przeprowadzać co miesiąc przeglądy i konserwacje systemów i zbiorów danych przez uprawnione do tego osoby pod nadzorem osoby upoważnionej przez administratora danych osobowych. Osoba przetwarzająca dane powinna sprawdzić spójność danych osobowych w kartotekach ręcznych z danymi w programie komputerowym. Dopilnować należy aby oprogramowanie użytkowe wykorzystywane przy przetwarzaniu danych było na bieżąco aktualizowane.

§ 16.

Dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji należy pozbawić zapisu tych danych, a w przypadku gdy nie jest to możliwe należy je uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności osoby upoważnionej przez administratora danych osobowych.

Załącznik Nr 2 do Zarządzenia Nr 28/12

Burmistrza Pisza

Instrukcja

przechowywania kopii zapasowych bazy danych osobowych oraz magnetycznych nośników informacji i wydruków

§ 1.

Kopie zapasowe wykonuje się na taśmach i przechowuje w kasie pancernej w pokoju nr 30. Wydruki z danymi osobowymi (kopie upoważnień, nakazów płatniczych) przechowuje się w zamykanych szafach drewnianych w pomieszczeniu przetwarzania danych.

§ 2.

Okres przechowywania nośników danych jest uzależniony od przydatności tych danych. Po upływie tego okresu należy je wykorzystać do nowych kopii lub w przypadku ich nieprzydatności – należy je zniszczyć w sposób uniemożliwiający ich odczyt.

§ 3.

Nośniki informacji należy sprawdzać na obecność wirusa z częstotliwością 1 miesiąca (o ile nie zajdzie inna potrzeba).

§ 4.

Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, w zamkniętych szafach lub pomieszczeniach i po upływie czasu ich przydatności należy je zniszczyć (np. w niszczarkach).

Załącznik Nr 3 do Zarządzenia Nr 28/12
Burmistrza Pisza

Instrukcja
postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1.

Instrukcja określa tryb postępowania w przypadku, gdy zawartość zbioru danych osobowych osobowych (brak lub nadmiar danych), ujawnione metody pracy, mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 2.

W przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczeń danych osobowych osoba przetwarzająca dane obowiązana jest niezwłocznie powiadomić o tym fakcie administratora danych osobowych lub inną upoważnioną przez niego osobę oraz Administratora Bezpieczeństwa Informacji.

§ 3

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) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.

§ 4

Niezwłocznie należy podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji.

§ 5

Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna sprawdzić:

1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych.

2) zawartość zbioru danych osobowych.

§ 6

Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowania podobnych zdarzeń w przyszłości:

1) jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych.
2) jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje regulowane ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r. Nr 101 poz. 926 z późn.zm.).
3) jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych.

§ 7

Administrator Bezpieczeństwa Informacji przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz w określonym terminie od daty zaistnienia zdarzenia przekazuje go administratorowi danych osobowych.

Załącznik Nr 4 do Zarządzenia Nr 28/12
Burmistrza Pisza

Instrukcja
ochrony danych osobowych
w Urzędzie Miejskim w Piszu

§ 1

Podstawę prawną do niniejszej instrukcji zwanej dalej „instrukcją" stanowią:

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 z późn.zm.); zwana dalej „ustawą";
2. Rozporządzenie 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.Nr 100, poz. 1024);
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229 poz. 1536).

§ 2

Instrukcja określa:

1) zasady postępowania przy przetwarzaniu danych osobowych,
2) prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych osobowych.

§ 3

Dane osobowe w Urzędzie Miejskim w Piszu zwanym dalej „UM w Piszu" mogą być przechowywane:

1) w systemach informatycznych (mogą być nimi również pojedyncze komputery)
2) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 4

Przetwarzanie danych osobowych jest możliwe tylko wtedy, gdy uzasadnia to:

1) dobro publiczne,
2) dobro osoby, której dane dotyczą,
3) dobro osób trzecich, a dane przetwarza się w zakresie i trybie określonych w ustawie.

ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 5

Administrator danych osobowych wyznacza Administratora Bezpieczeństwa Informacji, czyli osobę odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, a szczególnie za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym są przetwarzane dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

§ 6

Administratorem danych osobowych w UM w Piszu jest Burmistrz Pisza.

§ 7

Naczelnicy Wydziałów UM w Piszu, w których przetwarzane są dane osobowe w systemach informatycznych, w uzgodnieniu z administratorem danych osobowych oraz Administratorem Bezpieczeństwa Informacji:

1) określają cele, strategię i politykę zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
2) powinni zdefiniować i przeanalizować zagrożenia i ryzyko, na które może być narażone przetwarzanie danych osobowych,
3) określają potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, z uwzględnieniem potrzeby kryptograficznej ochrony danych osobowych, szczególnie podczas ich przesyłania za pomocą urządzeń teletransmisji danych,
4) monitorują działania zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania.

§ 8

Administrator danych osobowych, poprzez Naczelników Wydziałów UM w Piszu i wyznaczonego Administratora Bezpieczeństwa Informacji zapewnia stosowanie przez pracowników UM w Piszu przepisów instrukcji; Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych; Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych; Instrukcji przechowywania kopii zapasowych bazy danych osobowych oraz magnetycznych nośników informacji i wydruków oraz Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UM w Piszu stanowiącej załącznik do Zarządzenia Nr 166/04 Burmistrza Pisza z dnia 30 listopada 2004r. w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Piszu".

§ 9

1. Naczelnik Wydziału UM w Piszu przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych powinien zapoznać pracownika z:
   1) przepisami dotyczącymi ochrony danych osobowych, a szczególnie z przepisami karnymi wynikającymi z rozdziału ósmego ustawy,
   2) Zarządzeniem Nr 28/12 Burmistrza Pisza z dnia 28 marca 2012r. w sprawie wprowadzenia w Urzędzie Miejskim w Piszu wewnętrznych uregulowań dotyczących ochrony danych osobowych,
   3) Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UM w Piszu stanowiącą załącznik do Zarządzenia Nr 166/04 Burmistrza Pisza z dnia 30 listopada 2004r. w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Piszu".

2. Po dokonaniu czynności o której mowa w ust. 1 Naczelnik Wydziału UM w Piszu przekazuje administratorowi danych osobowych pisemne oświadczenia pracownika dotyczące tej czynności.
3. Wzór oświadczenia o którym mowa w ust. 2 stanowi załącznik nr 1 do instrukcji.
4. Oryginał oświadczenia dołączony zostanie do akt osobowych pracownika, kopia będzie przechowywania w Wydziale Spraw Obywatelskich, Promocji i Turystyki UM w Piszu,
5. Rejestr osób które złożyły oświadczenia znajduje się w Wydziale Spraw Obywatelskich, Promocji i Turystyki UM w Piszu.

§ 10

1. Wniosek o nadanie uprawnień w systemie informatycznym którego wzór stanowi załącznik Nr 2 do instrukcji winien być przekazywany przez Naczelnika Wydziału UM w Piszu przed przystąpieniem do pracy z danymi osobowymi Administratorowi Bezpieczeństwa Informacji zwanemu dalej „ABI".

2. Po rozpatrzeniu wniosku o którym mowa w ust. 1 oraz sprawdzeniu złożenia oświadczenia zgodnego z § 9 ust. 2 instrukcji ABI wydaje upoważnienie do przetwarzania danych osobowych, nadaje identyfikator (login), hasło oraz uprawnienia w systemie informatycznym w zakresie wynikającym z wniosku Naczelnika Wydziału .

3. Wzór upoważnienia stanowi załącznik Nr 3 do instrukcji.

4. Upoważnienie podpisują Burmistrz Pisza oraz ABI.

5. Rejestr upoważnień prowadzony jest przez ABI.

6. Oryginały dokumentów wymienionych w ust. 1 i 2 dołączone zostaną do akt osobowych pracownika, kopia będzie przechowywana przez ABI.

§ 11

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

§ 12

Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do:

1) likwidacji- pozbawia się wcześniej zapisu danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie,
2) przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych – pozbawia się wcześniej zapisu tych danych,
3) naprawy – pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych osobowych.

§ 13

Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

REJESTRACJA ZBIORÓW DANYCH OSOBOWYCH

§ 14

1. Naczelnik Wydziału UM w Piszu, w którym prowadzona jest lub prowadzona będzie baza danych osobowych zobowiązany jest do przygotowania wniosku potrzebnego do zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych na formularzu, którego wzór określa Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229 poz. 1536).

2. Wniosek należy przygotować w takim terminie, aby administrator danych osobowych mógł dokonać rejestracji bazy przed rozpoczęciem przetwarzania.

§ 15

Jeżeli w zarejestrowanym zbiorze danych osobowych dokonana zostaje zmiana polegająca na przetwarzaniu nowej kategorii danych Naczelnik Wydziału UM w Piszu, w którym baza jest prowadzona powinien niezwłocznie poinformować o tym administratora danych osobowych, tak aby mógł on wywiązać się z obowiązku zgłoszenia tej zmiany w ciągu 30 dni od jej dokonania Generalnemu Inspektorowi Ochrony Danych Osobowych.

GŁÓWNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

§ 16

Administrator danych osobowych ma obowiązek udzielania informacji osobom, których dane przetwarza.

§ 17

W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych osobowych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie ,
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
3) źródle danych,
4) prawie dostępu do treści swoich danych oraz ich poprawiania,
5) prawie żądania zaprzestania przetwarzania danych oraz prawie sprzeciwu.

§ 18

Każdej osobie, której dane osobowe są przetwarzane w UM w Piszu przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby administratora danych osobowych;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 19

Przetwarzanie danych osobowych znajdujących się w UM w Piszu może zostać powierzone innemu podmiotowi, w drodze umowy zawartej na piśmie wyłącznie w zakresie i celu przewidzianym w umowie.

§ 20

Wszyscy pracownicy UM w Piszu pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia.

Załącznik Nr 1 do instrukcji

Pisz, dnia_____

_____
(nazwisko i imię)

_____
(nazwa komórki)

_____
(stanowisko)

O Ś W I A D C Z E N I E

Oświadczam, że w związku z przetwarzaniem danych osobowych wynikających z wykonywanych przeze mnie czynności służbowych zapoznałem(am) się z:

1. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz.U. z 2002r. Nr 101, poz. 926 z późn.zm.),
2. 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.Nr 100, poz. 1024);
3. Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w UM w Piszu stanowiącą załącznik do Zarządzenia Nr 166/04 Burmistrza Pisza z dnia 30 listopada 2004r. w sprawie ustalenia „Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Piszu".
4. Zarządzeniem Nr 28/12 Burmistrza Pisza z dnia 28 marca 2012r. w sprawie wprowadzenia w Urzędzie Miejskim wewnętrznych uregulowań dotyczących ochrony danych osobowych wraz z załącznikami.

Załącznik Nr 2 do instrukcji

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis zakresu uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
	Akceptacja ABI

Załącznik Nr 3 do instrukcji

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana .....

(imię i nazwisko upoważnianego)

zatrudnioną/-ego na stanowisku .....

w .....

(nazwa administratora – pracodawcy)

do dostępu do następujących danych osobowych:

– .....

– .....

– .....

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba,

lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator: .....

(wypełnia się w przypadku, gdy dane przetwarzane są w systemie informatycznym)

3. Okres trwania upoważnienia: .....

(okres obowiązywania upoważnienia)

Wystawił: .....

(podpis administratora lub osoby reprezentującej administratora)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....