



Urząd Miejski w Dąbiu
Plac Mickiewicza 1, 62-660 Dąbie
tel. 63 2628271 fax. 63 2710086
e – mail: sekretariat@dabie.nowoczesnagmina.pl

Załącznik Nr 2
do Zarządzenia Burmistrza Miasta Dąbie
Nr OR.0050.73.2015
z dnia 23 listopada 2015 r.

**INSTRUKCJA ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO
PRZETWARZANIA DANYCH OSOBOWYCH
w URZĘDZIE MIEJSKIM W DĄBIU**

OPRACOWAŁ:

Łukasz Królasik

Administrator Bezpieczeństwa Informacji

w Urzędzie Miejskim w Dąbiu

§ 1.**POSTANOWIENIA OGÓLNE**

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Dąbiu, określa:

- 1) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Dąbiu, zwana dalej „Instrukcją” określa zasady , tryb postępowania i zalecenia Administratora Danych Osobowych , które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych,
- 2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
- 3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
- 4) zasady i procedury rozpoczynania i kończenia pracy,
- 5) zasady i częstotliwość tworzenia kopii bezpieczeństwa.
- 6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
- 7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
- 8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
- 9) zasady postępowania w zakresie komunikacji w sieci komputerowej,
- 10) instrukcja opracowana została zgodnie z wymogami § 5 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 w systemach informatycznych.

§ 2.**DEFINICJE ZAWARTE W INSTRUKCJI**

Ilekoć w instrukcji jest mowa o :

- 1) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. , poz. 1182 ze zm.), zwaną dalej „ustawą”;
- 2) **Jednostka** – rozumie się przez to Urząd Miejski w Dąbiu

- 3) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 4) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 5) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.)
- 6) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
- 7) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
- 8) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 9) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 10) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- 11) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 12) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
- 13) **Administrator Danych (AD)** - w świetle przepisów ustawy o ochronie danych osobowych, art. 3 i 7 pkt 4 rozumie się przez to Burmistrza Miasta Dąbie, który decyduje o celach i środkach przetwarzania danych osobowych;
- 14) **Administrator Bezpieczeństwa Informacji (ABI)** - rozumie się przez to osobę wyznaczoną przez Administratora Danych (kierownika jednostki), nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- 15) **Administrator Systemu Informatycznego (ASI), zwanego też Administratorem Systemu** - rozumie się przez to osobę zatrudnioną przez Burmistrza Miasta Dąbie,

Urząd Miejski w Dąbiu

upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

16) **użytkownik systemu informatycznego** - rozumie się przez to upoważnionego przez kierownika jednostki, pracownika do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych.

§ 3.**ZASADY DOSTĘPU UŻYTKOWNIKA DO SYSTEMU**

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej „systemem” może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Administratora Bezpieczeństwa Informacji.

2. Rejestracja, o której mowa w ust. 1, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§ 4.**IDENTYFIKATOR**

1. Identyfikator składa się z minimum sześciu znaków.

2. W identyfikatorze pomija się polskie znaki diakrytyczne.

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Systemu po uzgodnieniu z ABI nadaje inny identyfikator.

§ 5.**H A S Ł A**

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

3. Zmiana hasła następuje nie rzadziej niż co 30 dni z zastrzeżeniem § 6.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§ 6.**WYREJESTROWANIE UŻYTKOWNIKA**

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika komórki organizacyjnej.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

- 1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
- 2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

- 3) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
- 4) zawieszenie w pełnieniu obowiązków służbowych,
- 5) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 7.**ROZPOCZĘCIE PRACY W SYSTEMIE**

Rozpoczęcie pracy w systemie odbywa się poprzez:

- 1) przygotowanie stanowiska pracy,
- 2) włączenie stacji roboczej,
- 3) wprowadzenie swojego identyfikatora i hasła.

§ 8.**ZAKOŃCZENIE PRACY W SYSTEMIE**

Zakończenie pracy w systemie odbywa się poprzez:

- 1) zamknięcie aplikacji,
- 2) odłączenie się od zasobów systemowych,
- 3) zamknięcie systemu operacyjnego,

- 4) wyłączenie stacji roboczej.

§ 9.

ZASADY PRACY W SYSTEMIE

1. Zabrania się użytkownikom pracującym w systemie:

- 1) udostępniania stacji roboczej osobom niezarejestrowanym z zastrzeżeniem pkt 2,
- 2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemu Informatycznego,
- 3) używania nielicencjonowanego oprogramowania.

§ 10.

NARUSZENIE BEZPIECZEŃSTWA SYSTEMU

1. Każdy przypadek naruszenia ochrony danych osobowych, które mogą wskazywać na naruszenie bezpieczeństwa podlega zgłoszeniu do Administratora Bezpieczeństwa Informacji, a w szczególności:

- 1) naruszenia bezpieczeństwa systemu informatycznego,
- 2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci).

2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:

- 1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
- 2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
- 3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
- 4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
- 5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
- 6) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,

Urząd Miejski w Dąbiu

- 7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
- 8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust 1, spoczywa na każdym użytkowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem Administratora Systemu jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

5. Użytkownik sieci i Administrator Systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.

6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§ 11.**KOPIE ZAPASOWE**

1. Kopie awaryjne tworzy się z następującą częstotliwością:

- 1) kopie systemu finansowo - księgowego – dwa razy w miesiącu,
- 2) kopie pozostałe - nie rzadziej niż raz na miesiąc.

2. Każdą kopię tworzy się na oddzielnym nośniku informatycznym.

3. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

4. Administrator Systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.

5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia Administratora Systemu do ich zniszczenia.

§ 12.**WIRUSY**

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 2, Administrator Systemu nie rzadziej niż raz na dwa miesiące przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.

§ 13.**ZASILANIE AWARYJNE**

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).

§ 14.**NAPRAWA, SERWIS URZĄDZEŃ**

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać do naprawy, do likwidacji dopiero po uprzednim uzyskaniu zgody Administratora Bezpieczeństwa Informacji.
2. Urządzenia, o których mowa w ust. 1 przed ich przekazaniem pozbawia się zapisu danych osobowych poprzez wymontowanie dysku twardego z zastrzeżeniem ust. 3.
3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem Administratora Systemu.

Urząd Miejski w Dąbiu

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§ 15.**PRZEGLĄD , KONSERWACJE**

1. Przeglądu i konserwacji systemu dokonuje Administrator Systemu doraźnie.
2. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na dwa tygodnie.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na dwa tygodnie.

§ 16.**BEZPIECZEŃSTWO KOMUNIKACJI**

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe Administrator Systemu zapewnia przy użyciu narzędzi w obrębie systemu.
2. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, Administrator Systemu powinien uwzględniać dedykowane przyzwolenia dostępu.

§ 17**KOMUNIKACJA WEWNĘTRZNA**

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.
2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, użytkownik systemu wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§ 18.**SIEĆ PUBLICZNA**

Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych i w oparciu o przepisy prawne regulujące sposób wysyłania tych danych.

§ 19.**OZNACZANIE NOŚNIKÓW DANYCH**

Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§ 20.**BEZPIECZEŃSTWO NOSNIKÓW, URZĄDZEŃ**

1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

§ 21.**PRZENOŚNE NOŚNIKI INFORMATYCZNE**

Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie Administratora Bezpieczeństwa Informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator Bezpieczeństwa Informacji może żądać usunięcia

Urząd Miejski w Dąbiu

danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

§ 22.**PRZENOSNY KOMPUTER**

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§ 23.**WYDRUKI**

1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu.

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

§ 24.**DANE UŻYTKOWNIKA**

System powinien umożliwić udostępnienie na piśmie, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:

- a) daty pierwszego wprowadzenia danych tej osoby,
- b) źródła pochodzenia danych,
- c) nazwy użytkownika wprowadzającego dane,
- d) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,
- e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych.

§ 25.**ODPOWIEDZIALNOŚĆ**

Naruszenie obowiązków wynikających z Polityki Bezpieczeństwa oraz przepisów ustawy o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

§ 26.**OBOWIĄZKI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI**

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) nadzór nad stosowaniem środków ochrony,
- 2) nadzór nad przestrzeganiem przez Administratora Systemów Informatycznych i użytkowników systemu - procedur bezpieczeństwa,
- 3) wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków,
- 4) prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, która jest częścią ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i zasady ochrony danych osobowych w Urzędzie Miejskim w Dąbiu,
- 5) kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.
- 6) prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych,
- 7) prowadzenie rejestru zbiorów będących w zasobach Administratora danych ,
- 8) współdziałanie z Generalnym Inspektorem Ochrony Danych Osobowych w zakresie sprawdzonych zleconych przez GIODO ,

- 9) uzgadnianie z Administratorem Systemów Informatycznych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.

§ 27.

OBOWIĄZKI ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

- 1) realizacja zadań związanych z przeszkoleniem użytkowników w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali,
- 2) zapoznanie użytkowników z treścią Instrukcji,
- 3) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych,
- 4) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,
- 5) kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
- 6) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień,
- 7) utrzymanie systemu w należytej sprawności technicznej,
- 8) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,
- 9) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których przetwarzane są dane osobowe.

PRZEPISY KOŃCOWE

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182, z późn. zm.) oraz rozporządzenie 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 r. Nr 100, poz. 1024).