ZARZĄDZENIE Nr 2/2014
DYREKTORA ZAKŁADU USŁUG KOMUNALNYCH W WĘGLIŃCU
z dnia 03.03.2014 roku
w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym w Zakładzie Usług Komunalnych w Węglińcu

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz § 3 i 4 rozporządzenia 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), oraz § 7 ust. 3 Statutu Zakładu Usług Komunalnych w Węglińcu stanowiącego załącznik nr 1 do uchwały Nr 152/XLVI/02 Rady Gminy i Miasta Węgliniec z dnia 27.02.2002r.

zarządzam, co następuje:

§ 1.

Wprowadzam w Zakładzie Usług Komunalnych w Węglińcu **Politykę Bezpieczeństwa**, której treść stanowi ***załącznik nr 1*** do zarządzenia, oraz **Instrukcję zarządzania systemem informatycznym**, która stanowi ***załącznik nr 2*** do zarządzenia.

§ 2.

Każdy pracownik, upoważniony do przetwarzania danych osobowych, jest obowiązany zapoznać się z treścią załączników nr 1 i 2 do zarządzenia.

§ 3.

Zobowiązuję wszystkich upoważnionych pracowników do przestrzegania Polityki Bezpieczeństwa oraz stosowania w pracy Instrukcji pod sankcją konsekwencji służbowych, przewidzianych prawem.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
mgr inż. Krzysztof Polewski

Załącznik 1 do Zarządzenia Nr 2/2014
Dyrektora Zakładu Usług Komunalnych w Węglińcu
z dnia 03.03.2014 roku

POLITYKA BEZPIECZEŃSTWA W ZAKŁADZIE USŁUG KOMUNALNYCH W WĘGLIŃCU

§ 1.

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w ***Zakładzie Usług Komunalnych***, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
2. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych.
3. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:
1.zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2.przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3.systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4.zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5.usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6.administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r. Nr 101, poz. 926 za zm), decydujące o celach i środkach przetwarzania danych osobowych,
7.administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w § 1, chyba, że Administrator Danych sam wykonuje te czynności.
8.podmiocie – rozumie się przez to firmę, instytucję.

§ 3.

Administrator Danych w podmiocie ***Zakład Usług Komunalnych*** sam wykonuje czynności Administratora Bezpieczeństwa Informacji.

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 1 do „Polityki Bezpieczeństwa".**

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa **załącznik nr 2 do „Polityki Bezpieczeństwa".**

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa **załącznik nr 3 do „Polityki Bezpieczeństwa".**

§ 7.

Administrator Danych dba o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty powinny znajdować się w pomieszczeniu zamykanym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych**. **Administrator Danych** jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Danych nadaje uprawnienia pracownikom którzy przetwarzają dane poprzez podpisanie oświadczenia które stanowi **załącznik nr 4 do „Polityki Bezpieczeństwa"**. Administrator Danych prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie a w szczególności:

1. Ewidencja osób przetwarzających dane w zakładzie posiadających upoważnienie została określona w **załączniku nr 5** do „Polityki Bezpieczeństwa".

2. Zestawienie danych osobowych określających kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane zostało określone w **załączniku nr 6** do „Polityki Bezpieczeństwa".

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym w Zakładzie Usług Komunalnych w Węglińcu.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa" mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA 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**

Podpis Administratora Danych Osobowych

DYREKTOR
mgr inż. Krzysztof Polewski

.....

Podpis

Załącznik 2 do Zarządzenia Nr 2/2014
Dyrektora Zakładu Usług Komunalnych w Węglińcu
z dnia 03.03.2014

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W ZAKŁADZIE USŁUG KOMUNALNYCH W WĘGLIŃCU

Ilekroć w „instrukcji" jest mowa o:
1) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
2) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) sieci telekomunikacyjnej — 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.)
5) publicznej sieci telekomunikacyjnej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne;
6) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
7) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
8) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
10) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
11) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w **Zakładzie Usług Komunalnych w Węglińcu** zapisów „instrukcji" odpowiedzialny jest Administrator Danych.

§2

W związku z tym, że w **Zakładzie Usług Komunalnych w Węglińcu** przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim,** a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób

nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Danych. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego
•poprzez zainstalowanie programu antywirusowego o nazwie **ESET Endpoint Antivirus**
•poprzez zainstalowanie firewall (zapora sieciowa).
2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień

4. Kopie zapasowe:
a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pokoju Kadry w szafie pancernej zaopatrzonej w zamek patentowy.
b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 60 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Danych ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w zakładzie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok.

§6

W przypadku stwierdzenia uchybień dotyczących przetwarzania danych w zakładzie Administrator Danych wprowadza takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej „instrukcji" mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIEM 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**

Podpis Administratora Danych Osobowych

.....

Podpis