Regulamin Ochrony Informacji dla wykonawcy Urzędu Miasta Olsztyna

Dokument wydrukowany i niepodpisany jest dokumentem nienadzorowanym.

Opracowali:	Sprawdzili:	Zatwierdzili:
Mariola Iciak przy współpracy firmy ARTSYSTEMS Artur Cieślik	Rafał Ruchlewicz	Piotr Grzymowicz
Data: 25.03.2015	Data: 25.03.2015	Data: 25.03.2015

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja, usuwanie, dodawanie:

1. Administrator Bezpieczeństwa Informacji.

Zakres dostępu do dokumentu – odczyt:

2. Podmioty i instytucje upoważnione na podstawie przepisów prawa.

KARTA ZMIAN:			
Nr	Opis dokonanej zmiany w treści dokumentu	Data zmiany	Podpis uprawnionego pracownika
1	W nagłówku załącznika nr 13 dodaje się konieczność uzupełnienia przez osobę podpisującą danych: imię i nazwisko oraz umowy/zakresu, którego oświadczenie dotyczy.	2015-05-29	
2			
3			
4			
5			
6			
7			
8			
9			
10			

Spis treści

1 Cel

Celem dokumentu w Urzędzie Miasta Olsztyna jest:

1. Określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla podmiotów zewnętrznych.
2. Określenie minimalnych wymagań w zakresie zabezpieczeń systemów teleinformatycznych.

2 Zakres

1. Niniejszy dokument stosują wszystkie podmioty zewnętrzne wykonujące prace na rzecz Urzędu Miasta, związane z przetwarzaniem aktywów informacyjnych Urzędu.
2. Niniejszy dokument należy stosować we wszystkich umowach z podmiotami zewnętrznymi, których przedmiot jest związany z ochroną informacji.

3 Terminologia

Pojęcia używane w Polityce Bezpieczeństwa Informacji Urzędu Miasta Olsztyna oraz innych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji są zdefiniowane w dokumencie ***Słownik pojęć używanych w dokumentach Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Olsztyna.***

4 Postanowienia ogólne

1. Regulamin Ochrony Informacji dla Wykonawcy Urzędu Miasta Olsztyna, zwany dalej Regulaminem, określa zakres obowiązków i odpowiedzialności podmiotów zewnętrznych w zakresie bezpieczeństwa informacji. Regulamin obejmuje swym zakresem wszystkich użytkowników podmiotów zewnętrznych, mających dostęp do systemów teleinformatycznych Urzędu Miasta Olsztyna (zwanego dalej Urzędem). Regulamin jest syntezą informacji zawartych w Polityce Bezpieczeństwa Informacji Urzędu Miasta Olsztyna, Polityce Bezpieczeństwa Systemów Teleinformatycznych Urzędu Miasta Olsztyna.
2. Podmiot zewnętrzny spełnia wymagania niniejszego Regulaminu **przed** uzyskaniem dostępu do Systemu Teleinformatycznego Urzędu Miasta Olsztyna.
3. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych, których administratorem jest Prezydent Miasta Olsztyna, podmiot zewnętrzny powinien spełnić warunki:
   a. Podpisać zobowiązanie do zachowania poufności przetwarzanych danych na wzorze obowiązującym w Urzędzie, będącym załącznikiem nr 1 do Regulaminu.
   b. Podpisać umowę powierzenia przetwarzania danych osobowych na wzorze obowiązującym w Urzędzie, będącym załącznikiem nr 2 do Regulaminu.

5 Nadawanie, zmiana bądź odebranie uprawnień

1. W przypadku podmiotów zewnętrznych zakres uprawnień w poszczególnych systemach i aplikacjach ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych danych osobowych.
2. Lista użytkowników podmiotu zewnętrznego powinna być dostarczona przez osoby ze strony podmiotu zewnętrznego wskazane w umowie jako odpowiedzialne za jej realizację.
3. Po każdej zmianie użytkowników ze strony podmiotu zewnętrznego, jest on zobowiązany do przekazania listy użytkowników ze wskazaniem zmian w ich zakresie uprawnień.
4. Rejestrowanie/wyrejestrowanie użytkowników zewnętrznych Systemu Teleinformatycznego Urzędu Miasta Olsztyna oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez pracowników Wydziału Informatyki zgodnie ze schematem postępowania:
   a. Podczas rejestracji użytkownika zewnętrznego nadawany jest unikalny identyfikator użytkownika oraz ustawiane jest hasło tymczasowe niezbędne do logowania po raz pierwszy Systemu (zgodne z zasadami opisanymi w niniejszej procedurze) dla użytkownika zewnętrznego Systemu Teleinformatycznego.
   b. Na podstawie informacji przekazanych przez GABS nadawane lub modyfikowane są uprawnienia użytkownika.
   c. O nadaniu/zmianie/odebraniu uprawnień właściwych identyfikatorów w odpowiednich systemach i aplikacjach i nadaniu właściwych uprawnień jest informowany GABS oraz przedstawiciel podmiotu zewnętrznego.

6 Metody i środki uwierzytelniania

Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do Systemu Teleinformatycznego.

6.1 Hasła użytkowników

1. Hasła użytkowników do systemów powinny podlegać następującym zasadom:
   a. hasło składa się z minimum 8 znaków,
   b. hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),
   c. hasło musi być zmieniane minimum co 30 dni,
   d. kolejne hasła muszą być różne,
   e. hasła należy przechowywać w sposób gwarantujący ich poufność,
2. Zabrania się udostępniania haseł innym osobom.
3. Zabrania się tworzenia haseł na podstawie:
   a. cech i numerów osobistych (np. dat urodzenia, imion itp.),
   b. sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
   c. identyfikatora użytkownika
4. Zabrania się tworzenia haseł łatwych do odgadnięcia.
5. Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.
6. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.
7. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko użytkownikowi.
8. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego znaków obowiązkiem użytkownika jest zmiana hasła zgodnie z zasadami określonymi w ust. poprzednich.
9. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
10. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.
11. Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:
    a. w plikach,
    b. na kartkach papieru w miejscach dostępnych dla osób trzecich,
    c. w skryptach,
    d. w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
12. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą być natychmiast zmienione przez użytkownika lub Administratora Systemu.
13. Hasło użytkownika sytemu, umożliwiające dostęp do Systemu Teleinformatycznego, utrzymuje się w tajemnicy również po upływie jego ważności.
14. Zmiany hasła dokonuje użytkownik. W przypadku, gdy użytkownik zapomniał hasła, właściwy Administrator Systemu ustawia hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania.
15. Hasła przez użytkowników nie powinny być przekazywane ani przesyłane za pomocą telefonu, faksu ani poczty e-mail w formie jawnej.

7 Dostęp zdalny

1. Wydział Informatyki prowadzi pisemny wykaz osób i podmiotów zewnętrznych posiadających dostęp zdalny do zasobów Systemu Teleinformatycznego Urzędu Miasta Olsztyna.
2. Dostęp zdalny podmiotów zewnętrznych, możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym Regulaminie.
3. Dla każdej umowy z podmiotem zewnętrznym Dyrektor Wydziału Informatyki wyznacza Koordynatora Prac Zdalnych Wydziału Informatyki Urzędu Miasta Olsztyna (dalej zwany KPZ).
4. Podmiot zewnętrzny powierzając prace swoim pracownikom we własnym zakresie udziela im niezbędnych pełnomocnictw.
5. Dostępu udziela się na czas obowiązywania umowy na podstawie pisemnego wniosku przekazanego przez podmiot zewnętrzny do KPZ o podanie potrzebnych identyfikatorów i haseł dostępu.
6. W ramach dostępu zabrania się podmiotowi zewnętrznemu trwale usuwać dane, przeprowadzać jakiekolwiek operacje na dyskach mogące prowadzić do ich uszkodzenia lub utraty danych, w szczególności ich formatowania. Przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, o których wie, że w konsekwencji doprowadzić one mogą do zniszczenia danych, musi poinformować przedstawiciela Zamawiającego i dopiero po jego akceptacji podjąć może te czynności.
7. Podmiot zewnętrzny, przed przystąpieniem do prac, przedstawia scenariusz planowanych prac wraz z oceną ryzyka podejmowanych czynności. Podmiot zewnętrzny odpowiada za odstępstwa od przedstawionego scenariusza. Scenariusz powinien obejmować:
    a. Kto będzie prowadził prace.
    b. Kiedy, przewidywany czas trwania.
    c. Zakres wykonywanych prac.
    d. Informację czy wymagana jest przerwa w pracy użytkowników.
    e. Potencjalne ryzyka podejmowanych czynności.
8. Pracownik lub przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, co do których istnieje wysokie ryzyko utraty danych, informuje o ryzyku KPZ.
9. Po formalnej, pisemnej akceptacji ryzyka przez KPZ, pracownik podmiotu zewnętrznego może rozpocząć realizację czynności objętej wskazanym ryzykiem.
10. Wykonywanie prac polegających na standardowej obsłudze serwisowej, prac nad rozwojem programu będącego w fazie wdrażania nie wymaga każdorazowego ustalenia warunków realizacji czynności, będącej ich częścią. W ramach wykonywania tych czynności obowiązują warunki uzgodnione wcześniej. W szczególności nie wymagają każdorazowego ustalenia warunków realizacji te czynności, które wynikają z przedmiotu umowy i nie są objęte ryzykami opisanymi w pkt. 6-8. Wykonywanie czynności niestandardowych wymaga każdorazowo określenia warunków.
11. Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci Urzędu Miasta Olsztyna.
12. KPZ w porozumieniu z właściwymi administratorami ogranicza zasoby dostępne dla sesji zdalnej, do niezbędnego minimum, chyba, że wymagałoby rozległej ingerencji w konfigurację urządzeń dostępowych.
13. KPZ wraz z właściwymi administratorami ustalają wymagane zasoby. Podmiot zewnętrzny zobowiązuje się do wykorzystywania tylko i wyłącznie ustalonych zasobów, nawet, jeśli dostępne są inne niż tylko wymagane.

Zobowiązanie powinno przyjmować formę pisemną i być podpisane przez uprawnionego przedstawiciela podmiotu zewnętrznego.

14. Tworzona jest lista zasobów dostępnych dla sesji zdalnej, ze szczególnym uwzględnieniem zasobów innych niż wymagane. Za prowadzenie tej listy odpowiedzialny jest KPZ.

15. Na potrzeby realizacji umowy KPZ może udzielić dostępu zdalnego do następujących środowisk:

    a. Testowych.

    b. Produkcyjnego.

16. Zabrania się dostępu zdalnego z komputerów dostępnych publicznie np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci miejskie.

8 Wymagania zabezpieczeń

8.1 Zasady zabezpieczeń stacji roboczych

1. Do systemu informatycznego mogą być podłączane wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, w szczególności:

    a. System antywirusowy jest zainstalowany w systemie operacyjnym i jego sygnatury są aktualne.

    b. System operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń.

    c. Firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera.

    d. Zainstalowane na komputerze oprogramowanie pochodzi z godnych zaufania źródeł.

    e. Oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.

    f. Oprogramowanie nie łamie Ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. z późniejszymi zmianami.

8.2 Stosowanie zabezpieczeń kryptograficznych

W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. Miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi, w szczególności należy stosować zabezpieczenia kryptograficzne:

1. Na dyskach twardych komputerów przenośnych.

2. Na pendrive'ach.

3. Na nośnikach kopii zapasowych przechowywanych poza Systemem Teleinformatycznym Urzędu.

4. Na urządzeniach typu smartfon oraz tablet w aplikacjach, które przechowują dane objęte ochroną np. dane osobowe.

5. Tunelach VPN.

6. Wiadomościach poczty elektronicznej, w których przesyłane są dane objęte ochroną, w szczególności dane osobowe.

7. Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności.

8. Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES o długości klucza min. 128 bit.

9 Reagowanie na incydenty

1. Każde naruszenie bezpieczeństwa informacji należy zgłaszać Głównemu Administratorowi Bezpieczeństwa Systemów lub Koordynatorowi Dostępu Zdalnego lub w formie e-mail za potwierdzeniem odbioru na adres informatycy@olsztyn.eu z tematem wiadomości „Naruszenie bezpieczeństwa informacji”
2. Jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa, osoby wskazane w punkcie powyżej mogą zdecydować o natychmiastowym odebraniu uprawnień w systemach użytkownikom podmiotu zewnętrznego i bez zbędnej zwłoki przekazują informację o blokadzie dostępu osobie upoważnionej ze strony podmiotu zewnętrznego.
3. Upoważnione osoby z podmiotu zewnętrznego zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa.
4. W szczególnych przypadkach Główny Administrator Bezpieczeństwa Systemu informuje organy ścigania o zaistniałej sytuacji.
5. Główny Administrator Bezpieczeństwa Systemu w Wydziale Informatyki Urzędu Miasta Olsztyna sporządza notatkę dotyczącą naruszenia bezpieczeństwa i kieruje ją do Głównego Administratora Bezpieczeństwa Informacji Urzędu Miasta Olsztyna.
6. Ostatnim etapem zamykania naruszenia bezpieczeństwa jest usunięcie skutków naruszenia bezpieczeństwa oraz wprowadzenie dodatkowych zabezpieczeń (np. zmieniając konfigurację) w porozumieniu z uprawnionym przedstawicielem podmiotu zewnętrznego.
7. Każdy incydent związany z naruszeniem bezpieczeństwa informacji musi być zarejestrowany w rejestrze incydentów prowadzonym przez Głównego Administratora Bezpieczeństwa Systemu.

10 Postanowienia końcowe

1. Za nadzór nad przestrzeganiem postanowień Regulaminu odpowiada:
   a. Ze strony podmiotu zewnętrznego uprawniony przedstawiciel tego podmiotu.
   b. Ze strony Urzędu Miasta Olsztyna Główny Administrator Bezpieczeństwa Systemów i Administrator Bezpieczeństwa Informacji.
2. Naruszając Regulamin podmiot zewnętrzny może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów art. 49-54 ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych wraz z późniejszymi zmianami.

11 Lista dokumentów związanych

1. Polityka Bezpieczeństwa Informacji Urzędu Miasta Olsztyna.
2. Polityka Bezpieczeństwa Danych Osobowych Urzędu Miasta Olsztyna.
3. Polityka Bezpieczeństwa Systemów Teleinformatycznych Urzędu Miasta Olsztyna.
4. Procedura reagowania na incydenty Urzędu Miasta Olsztyna.

12 Załączniki

12.1 Załącznik nr 1 do Regulaminu ochrony informacji dla wykonawcy Urzędu Miasta Olsztyna - wzór zobowiązania do zachowania poufności przetwarzanych danych

UMOWA O ZACHOWANIU POUFNOŚCI INFORMACJI

(zwana dalej „Umową")

zawarta w […] pomiędzy:

[…]

zwaną dalej „**Stroną Ujawniającą**", reprezentowaną przez:

[…]

a

[…]

reprezentowaną przez:

[…]

zwaną dalej „**Odbiorcą Informacji Poufnych**" lub „**Odbiorcą**",

zwane dalej łącznie „**Stronami**".

1. Dla celów Umowy:

„Informacje Poufne" oznaczają wszelkie materiały i/lub informacje Strony Ujawniającej, zarówno handlowe, finansowe, techniczne, technologiczne i inne, ujawnione Odbiorcy, **w związku z realizacją usług świadczonych przez Odbiorcę dla Strony Ujawniającej w związku z umową […], dotyczących […]** (dalej „Usługa"), w formie ustnej, pisemnej lub w jakikolwiek inny sposób, zapisane w jakiejkolwiek formie (w tym między innymi w formie prezentacji, rysunków, filmów, dokumentów, w formie elektronicznej). Jeżeli, w związku z Usługą, którakolwiek ze Stron posiada dostęp do bazy danych osobowych (w rozumieniu obowiązującej Ustawy o ochronie danych osobowych) drugiej Strony, to informacje z takiej bazy danych będą traktowane jako Informacje Poufne;

Postanowienia Umowy będą miały zastosowanie w przypadku, gdy w związku z Usługą, Strona Ujawniająca ujawni Odbiorcy **Informacje Poufne.**

1. Odbiorca **Informacji Poufnych** zobowiązuje się:
   (a) zachować w tajemnicy uzyskane **Informacje Poufne**;
   (b) nie przekazywać ani nie ujawniać bez każdorazowej uprzedniej pisemnej zgody Strony Ujawniającej, jakichkolwiek **Informacji Poufnych** żadnej osobie, z wyjątkiem:
      (i) pracowników Odbiorcy wyznaczonych do realizacji Usługi, którzy potrzebują takich informacji w związku z realizacją Usługi, pod warunkiem podpisania przez nich Oświadczenia stanowiącego Załącznik do niniejszej Umowy, zawierającego zobowiązanie do zachowania w poufności;
      (ii) przypadków, w których Odbiorca jest zobowiązany do takiego ujawnienia przez sąd lub w przypadku ustawowego obowiązku takiego ujawnienia, z zastrzeżeniem, że Odbiorca dołoży właściwych starań w celu uprzedniego pisemnego poinformowania Strony Ujawniającej przed dokonaniem takiego ujawnienia;

(iii) osób trzecich zaangażowanych przez Odbiorcę do realizacji Usługi pod warunkiem podpisania przez nich Oświadczenia stanowiącego Załącznik do niniejszej Umowy, zawierającego zobowiązanie do zachowania w poufności;

(c) ponieść wobec Strony Ujawniającej odpowiedzialność za naruszenie obowiązków w zakresie zachowania w tajemnicy **Informacji Poufnych**, również w przypadku, gdy naruszenie jest dokonane przez osobę trzecią, o której mowa w pkt (b) iii, za której działania Odbiorca odpowiada jak za działania własne;

(d) nie wykorzystywać i nie rozpowszechniać **Informacji Poufnych** w ramach swojej działalności, z wyjątkiem wykorzystywania lub rozpowszechniania wyłącznie w zakresie koniecznym dla celów Usługi;

(e) dołożyć odpowiednich starań w celu zapewnienia i utrzymania odpowiednich środków zabezpieczających ochronę **Informacji Poufnych** przed dostępem i bezprawnym wykorzystaniem przez osoby nieuprawnione;

(f) spowodować, na żądanie Strony Ujawniającej, aby którekolwiek z osób i organów, o których mowa w pkt. (b) - (ii), podpisały przed udostępnieniem Informacji Poufnych odrębne zobowiązanie do zachowania poufności, z tym, że obowiązek określony powyżej ma zastosowanie w sytuacjach, gdy jest to prawnie dopuszczalne.

2. Obowiązku zachowania poufności, o którym mowa w ust. 2 powyżej, nie stosuje się: do jakiejkolwiek części **Informacji Poufnych**, w stosunku, do których Odbiorca może wykazać, że informacje takie: są lub stały się publicznie znane z przyczyn, za które pozostają poza kontrolą Odbiorcy; lub zostały zgodnie z prawem otrzymane od niezależnej osoby trzeciej bez naruszenia obowiązku zachowania poufności; lub w dacie ich ujawnienia przez Stronę Ujawniającą lub otrzymania od Strony Ujawniającej były już znane Odbiorcy bez obowiązku zachowania poufności;
3. Każda Strona może ujawnić **Informacje Poufne** otrzymane od drugiej Strony wyłącznie w celu wykorzystania w związku z realizacją Usługi. Każda Strona będzie odpowiedzialna za przestrzeganie postanowień niniejszej Umowy.
4. Po zakończeniu lub zaprzestaniu realizacji Usługi, Odbiorca bezzwłocznie zwróci Stronie Ujawniającej wszelkie Materiały dostarczone przez Stronę Ujawniającą, zawierające **Informacje Poufne** oraz wszystkie ich kopie oraz zniszczy lub usunie wszelkie **Informacje Poufne** zapisane w jakimkolwiek urządzeniu służącym do przechowywania danych.
5. Zakończenie realizacji Usługi z jakiejkolwiek przyczyny nie będzie miało wpływu na obowiązki określone w niniejszej Umowie.
6. Umowa podlega prawu polskiemu. W sprawach nie uregulowanych niniejszą Umową zastosowanie mają przepisy kodeksu cywilnego.
7. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
8. Niniejsza Umowa sporządzona została w dwóch egzemplarzach w języku polskim, po jednym egzemplarzu dla każdej ze Stron.

Strona Ujawniająca **Odbiorca**

Załącznik do Umowy o zachowaniu poufności informacji z dnia …….

/WZÓR/

OŚWIADCZENIE

……., dnia …… r.

Niniejszym oświadczam, że znana mi jest treść Umowy o zachowaniu poufności informacji z dnia …… zawartej pomiędzy …… a …….. z siedzibą w …….. przy ul. …… i wynikające z niej zobowiązania do utrzymywania w tajemnicy ujawnionych Informacji Poufnych.

Niniejszym zobowiązuję się jako pracownik …….. (nazwa firmy)/zleceniobiorca* …… do zachowania w tajemnicy wszelkich Informacji Poufnych, które zostały mi ujawnione w związku z moim uczestnictwem w realizacji Usługi, na warunkach określonych w Umowie o zachowaniu poufności. Jestem świadomy, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

……

* niepotrzebne skreślić

12.2 Załącznik nr 2 do Regulaminu ochrony informacji dla wykonawcy Urzędu Miasta Olsztyna - wzór umowy powierzenia przetwarzania danych osobowych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

dotycząca umowy:

zawarta w Olsztynie, w dniu …… roku, pomiędzy:

Gminą Olsztyn, z siedzibą w Olsztynie, Pl. Jana Pawła II 1, 10-101 Olsztyn

reprezentowaną przez

Prezydenta Olsztyna - Pana Piotra Grzymowicza

(zwaną dalej **Powierzającym**)

a

,

reprezentowaną przez

1.

(zwaną dalej **Przetwarzającym**)

§ 1.

1. *Powierzający* oświadcza, że jest, w rozumieniu przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U.2014.1182 j.t. ze zm., zwaną dalej Ustawą), administratorem danych osobowych, w szczególności zgromadzonych w bazie danych systemu ……..w zakresie:

< Należy wymienić zakres danych osobowych określony we wniosku o zgłoszenie zbioru do GIODO w punkcie 7.>

2. Na podstawie art. 31 ust. 1 Ustawy *Powierzający* powierza *Przetwarzającemu* przetwarzanie danych osobowych zgromadzonych w bazie danych systemu ……. wyłącznie w celu wykonania zobowiązań w zakresie realizacji zadań wynikających z umowy:

……

§ 2.

1. *Powierzający* przekazuje *Przetwarzającemu* jako załącznik do niniejszej umowy, „ Regulaminu ochrony informacji dla Wykonawcy,", na którą składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które *Przetwarzający* powinien stosować przetwarzając powierzone mu na podstawie niniejszej umowy dane osobowe.
2. W przypadku stwierdzenia przez Przetwarzającego nieadekwatnego poziomu zabezpieczeń w przekazanym mu Regulaminie ochrony informacji dla Wykonawcy wynikających ze stosowanej u *Powierzającego* dokumentacji przetwarzania danych osobowych jest on zobowiązany do powiadomienia o tym fakcie Powierzającego, a do momentu wyeliminowania nieprawidłowości stosować środki techniczne i organizacyjne odpowiednie do wykrytych nieprawidłowości.
3. *Przetwarzający* jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przekazany mu na podstawie umowy zbiór danych, o których mowa w art. 36 – 39, oraz spełnić wymagania

określone w przepisach, o których mowa w art. 39a ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych. W zakresie przestrzegania tych przepisów *Przetwarzający* ponosi odpowiedzialność jak administrator danych. W szczególności *Przetwarzający* zobowiązuje się do :

a. zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
b. dopuszczenia do obsługi służącego do przetwarzania powierzonych danych osobowych systemu informatycznego oraz wchodzących w jego skład urządzeń wyłącznie osób posiadających wydane przez niego upoważnienie,
c. zapewnienia kontroli nad prawidłowością przetwarzania powierzonych danych osobowych,
d. prowadzenia ewidencji osób upoważnionych do przetwarzania powierzonych danych osobowych, dochowania szczególnej staranności, aby osoby upoważnione do przetwarzania tych danych zachowały je w tajemnicy, również po zakończeniu realizacji niniejszej umowy, między innymi poprzez poinformowanie ich o prawnych konsekwencjach naruszenia poufności danych,
e. prowadzenia dokumentacji opisującej sposób przetwarzania powierzonych danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania tych danych, w tym w szczególności Politykę Bezpieczeństwa Danych Osobowych oraz Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych,

4. *Powierzający* ma prawo przez cały okres objęty umową kontrolować poprawność zabezpieczeń i przetwarzania danych przekazanych *Przetwarzającemu.*
5. *Przetwarzający* zobowiązuje się do nieudostępniania przetwarzanych danych jakiemukolwiek innym podmiotom i osobom innym niż *Powierzający.*
6. *Powierzający i Przetwarzający* zobligowani są do zachowania w tajemnicy wszelkich informacji powziętych z związku z realizowaną Umową również po jej zakończeniu.
7. *Przetwarzający* zobowiązany jest do dołożenia należytej staranności przy wykonywaniu niniejszej Umowy.
8. *Przetwarzający pozostaje w posiadaniu danych do przetwarzania, przekazanych przez Powierzającego, przez okres trwania umowy* o której mowa w §1 ust. 2 *oraz zobowiązuje się do bezzwłocznego trwałego usunięcia tych danych natychmiast po jej wygaśnięciu.*

§ 3.

1. *Przetwarzający* odpowiada za szkody, jakie powstaną wobec *Powierzającego* lub osób trzecich w wyniku niezgodnego z Umową przetwarzania danych osobowych zgromadzonych w bazie danych, o której mowa w §1 ust. 2. *Przetwarzający* może się uwolnić od odpowiedzialności względem *Powierzającego*, jeżeli wykaże, że stosował co najmniej środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych określone w istotnych wymogach przekazanych mu przez *Powierzającego* zgodnie z §2 ust. 1 umowy, w odniesieniu do danych osobowych zgromadzonych w bazach danych, o których mowa w §1 ust. 1.
2. Odpowiedzialność *Przetwarzającego* ograniczona jest do zakresu danych osobowych znajdujących się w jego faktycznym posiadaniu w związku z wykonywaniem czynności zgodnie z umową o której mowa w § 1 wymagających dostępu do danych osobowych i czasu wykonywania tych czynności.

§ 4.

Umowa zostaje zawarta odpowiednio na czas trwania umowy, o której mowa w § 1.

§ 5.

1. Zmiana niniejszej Umowy wymaga zachowania formy pisemnej pod rygorem nieważności.
2. W sprawach nie unormowanych niniejszą umową, a dotyczących jej przedmiotu mają zastosowanie przepisy Kodeksu cywilnego.

3. Wszelkie unormowania związane z ochrona danych osobowych, reguluje ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Powierzającego i jeden dla Przetwarzającego.

POWIERZAJĄCY **PRZETWARZAJĄCY**

12.3 Załącznik nr 3 - Wzór oświadczenia pracownika (firmy zewnętrznej) o zachowaniu poufności informacji chronionych

…….
(nazwa firmy)

…….
(imię i nazwisko)

Dotyczy: ……
(numer umowy/ zakres)

Oświadczenie pracownika o zachowaniu poufności informacji chronionych

Olsztyn, dnia.....

1. Za „Informacje chronione" w rozumieniu niniejszego oświadczenia uważa się wszelkie zagadnienia techniczne, finansowe lub handlowe, w szczególności dane osobowe w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2014.1182 j.t. ze zm.)., oraz inne dane prawnie chronione przez Urząd Miasta Olsztyna. Ponadto za „informacje chronione" mogą być również uważane dane powiązane z czynnościami wykonywanymi w Urzędzie Miasta Olsztyna lub mające na nie wpływ. Za Informacje chronione w rozumieniu niniejszego oświadczenia uważa się również dane przetwarzane we wszelkiej postaci, w tym dane przechowywane w systemie teleinformatycznym oraz wszystkie informacje związane z tym systemem. W szczególności uważa się szczegóły dotyczące systemów informatycznych, ich bezpieczeństwa oraz konfiguracji, w tym haseł, bez względu na sposób i formę, w jaki Urząd Miasta Olsztyna lub jego pracownicy weszli w posiadanie informacji.
2. Zobowiązuję się do zachowania w poufności informacji chronionych Urzędu Miasta Olsztyna. Jednocześnie zobowiązuję się do zachowania poufności sposobów zabezpieczenia informacji chronionych Urzędu Miasta Olsztyna również po zakończeniu wykonywania obowiązków lub innych zadań dla Urzędu Miasta Olsztyna.
3. Niniejsze oświadczenie obliguje mnie do przestrzegania warunków zawartych w umowie łączącej mnie z Urzędem Miasta Olsztyna we wskazanym zakresie danych i informacji przetwarzanych na stanowisku pracy. Zobowiązuję się nie wykorzystywać żadnych danych oraz informacji bez upoważnienia w celu innym niż wykonywanie wyżej wymienionej umowy.
4. Zapoznałem się z treścią obowiązujących przepisów prawa w zakresie ochrony danych osobowych, w szczególności z:
   1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   2) 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 (Dz.U.2004.100.1024).
5. Zapoznałem się z treścią obowiązujących przepisów prawa w zakresie odpowiedzialności wynikającej z Kodeksu Karnego (Dz.U.1997.88.553 ze zm.), w szczególności z artykułami:
   3) Art. 266. § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie obowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
   4) Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej,
   5) otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej
   6) lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub
   7) inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

8) Art. 267. § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
9) Art. 267. § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
10) Art. 267. § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.
11) Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
12) Art. 268. § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
13) Art. 268. § 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcydo lat 5.
14) Art. 287. § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
15) Art. 287. § 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

6. Oświadczam, że znana jest mi odpowiedzialność za naruszenie podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, co w szczególności może stanowić podstawę do podjęcia przez Urząd Miasta Olsztyna przysługujących mu środków prawnych.

…….....

podpis pracownika