

UMOWA O ADMINISTROWANIE SYSTEMU INFORMATYCZNEGO

zawarta w Łomży w dniu pomiędzy:

Miasto Łomża, Pl. Stary Rynek 14, 18-400 Łomża, NIP 718-214-49-19 reprezentowanym przez Bernadetę Krynicką – dyrektora Miejskiego Przedsiębiorstwa Gospodarki Komunalnej i Mieszkaniowej Zakład Budżetowy działającego z upoważnienia Prezydenta Miasta Łomża, zwanym w treści umowy „**Administratorem Danych**”

a

....., z siedzibą , NIP, REGON reprezentowanym przez:, zwanym w treści umowy „**Administratorem Systemu Informatycznego (ASI)**”

§ 1

1. Administrator Danych powierza Administratorowi Systemu Informatycznego sprawy z zakresu a ministrowania systemem informatycznym w MPGKiM ZB do których w szczególności należy:

- a) dbanie o prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację,
- b) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
- c) należyte wywiązywanie się z obowiązków wynikających z Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Szczegółowy zakres zadań został opisany jest w załączniku nr 1 do niniejszej umowy.

§ 2

W związku z powierzeniem spraw z zakresu administrowania systemem informatycznym może zaistnieć konieczność udostępnienia ASI posiadanych przez Administratora Danych informacji zawierających dane osobowe. ASI nie może przetwarzać danych osobowych znajdujących się w zbiorach danych Administratora Danych w żadnym celu.

§ 3

1. W celu właściwego zapewnienia bezpieczeństwa wszystkich danych, o których mowa w § 2 Umowy, ASI zobowiązuje się do zachowania szczególnej staranności, w tym do postępowania zgodnego z przepisami ustawy o ochronie danych osobowych oraz przepisów wykonawczych. ASI oświadcza, iż posiada odpowiednią wiedzę w zakresie IT i zobowiązuje się do bieżącego informowania Administratora Danych w zakresie nowych zagrożeń oraz pojawiających się na rynku rozwiązań w tematyce bezpieczeństwa informacji.

§ 4

ASI oświadcza, iż zna przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej RODO, Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) i zobowiązuje się do zabezpieczenia systemu informatycznego Administratora Danych zgodnie z tymi przepisami.

§ 5

1. Strony uzgadniają, że wszelkie dokumenty, materiały, dane i inne informacje związane z niniejszą Umową są poufne i są objęte tajemnicą. Strony zobowiązują się do dołożenia najwyższej staranności w

celu zapewnienia tajemnicy danych, o których mowa wyżej.

2. Ujawnienie jakiegokolwiek informacji dotyczącej niniejszej umowy dopuszczalne jest jedynie wyjątkowo i tylko w takim zakresie, jaki jest niezbędny do prawidłowego wypełnienia obowiązków wynikających z niniejszej umowy przez którąkolwiek ze Stron.

Zastrzeżenie to nie dotyczy udostępnienia niniejszej umowy ustawowym organom kontrolnym, właściwym dla każdej z umawiających się Stron.

3. Tajemnicą nie są objęte informacje ogólnie dostępne.

§ 6

Administrator Danych zastrzega sobie prawo do wykonywania audytu i kontroli procedur z zakresu zabezpieczenia systemu informatycznego.

§ 7

W przypadku wygaśnięcia lub rozwiązania Umowy ASI zobowiązany jest do przekazania Administratorowi Danych wszelkich materiałów związanych z wykonywaniem umowy, ze szczególnym uwzględnieniem haseł administratorskich. ASI zobowiązany jest do zachowania w tajemnicy wszelkich informacji prawem chronionych również po zakończeniu umowy.

§ 8

1. Jakiegokolwiek nieporozumienia, spory czy roszczenia wynikłe lub powstałe na tle niniejszej umowy, albo jej wykonywania, ważności czy złamania jej postanowień, będą w pierwszej kolejności rozstrzygane na drodze polubownej.

2. W razie nie rozwiązania sporu polubownie, sprawa zostanie oddana pod rozstrzygnięcie właściwego rzeczowo sądu w Łomży.

§ 9

1. W sprawach nieuregulowanych niniejszą Umową zastosowanie mieć będą odpowiednie przepisy Kodeksu Cywilnego, ustawy o ochronie danych osobowych oraz przepisy regulujące inne rodzaje tajemnicy w tym w szczególności tajemnicę przedsiębiorstwa.

2. Zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 10

Wynagrodzenie z tytułu realizacji zobowiązań wynikających z niniejszej umowy należne ASI określone zostanie przez Strony w Umowie o obsługę informatyczną.

§ 11

1. Umowa została sporządzona w jednobrzmiących egzemplarzach: egz. dla Zamawiającego, ... egz. dla Wykonawcy.

2. Integralną część umowy stanowi Załącznik nr 1 - Zadania ASI (Administratora Systemów Informatycznych).

.....
Administrator Danych

.....
Administrator Systemu Informatycznego

Zadania ASI – Administratora Systemów Informatycznych

Administrator Sytemu Informatycznego (ASI) jest odpowiedzialny za funkcjonowanie systemu zarządzania bezpieczeństwem informacji w obszarze bezpieczeństwa teleinformatycznego. W szczególności do obowiązków ASI należy:

1. Nadzór nad wdrażaniem i prawidłową realizacją Polityki Bezpieczeństwa Informacji w zakresie bezpieczeństwa teleinformatycznego oraz Instrukcji Zarządzania Systemem Informatycznym wdrożonymi do stosowania u Administratora Danych.
2. Nadzór nad przestrzeganiem procedur bezpieczeństwa systemów informatycznych.
3. Zaznajomienie pracowników z Instrukcją zarządzania systemem informatycznym.
4. Zapewnienie mechanizmów ochrony informacji przetwarzanej i przechowywanej na serwerach, komputerach stacjonarnych i komputerach przenośnych.
5. Nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzeniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemów informatycznych.
6. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe i inne informacje chronione.
7. Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, szkodliwego lub nielegalnego oprogramowania.
8. Nadzór nad przesyłaniem danych za pośrednictwem urządzeń teletransmisji do i z sieci zewnętrznych.
9. Nadzór nad funkcjonowaniem mechanizmów uwierzytelnienia użytkowników w systemach informatycznych.
10. Podjęcie natychmiastowych działań zabezpieczających dowody oraz funkcjonowanie systemu informatycznego w przypadku naruszenia zabezpieczeń systemu informatycznego.
11. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa systemów informatycznych lub informacji w nich przetwarzanych, jeśli takie wystąpiło .
12. Sporządzenie inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania danych.
13. Identyfikowanie kluczowych aplikacji i dbałość o ich niezakłócone działanie.
14. Sprawdzanie sposobów zabezpieczania danych osobowych w systemach informatycznych, a szczególności sprawdzanie:
 - a) mechanizmów kontroli dostępu do danych przetwarzanych w systemach informatycznych,
 - b) zastosowanych środków ochrony danych osobowych przed utratą na skutek awarii systemu informatycznego, w tym zasilania w energię elektryczną,
 - c) zastosowanych zabezpieczeń przed zagrożeniami pochodzącymi z sieci publicznej,
 - d) zastosowanych zabezpieczeń przed zagrożeniami pochodzącymi z wewnętrznej sieci Administratora Danych, w tym rozliczalność wykonywanych operacji,
 - e) środków zapewniających poufność danych osobowych przesyłanych przy wykorzystywaniu sieci publicznej oraz lokalnych urządzeń bezprzewodowych,
 - f) środków zapewniających poufność danych osobowych przetwarzanych przy wykorzystywaniu elektronicznych przenośnych nośników informacji,
 - g) funkcjonalności zastosowanych w systemach informatycznych w zakresie realizacji wymogów wynikających z przepisów o ochronie danych osobowych.

.....
Administrator Danych

.....
Administrator Systemu Informatycznego