WZÓR

UMOWA nr _____

zawarta w Olsztynie, w dniu _____ pomiędzy:

Gminą Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1, 10-101 Olsztyn, NIP 739-384-70-26, reprezentowaną przez Pana Piotra Grzymowicza - Prezydenta Olsztyna, w imieniu którego działa _____ – _____ Centrum Informatycznych Usług Wspólnych Olsztyna

zwaną dalej „**Zamawiającym**"

a

_____

_____

_____

zwaną/ym dalej „**Wykonawcą**",

w wyniku przeprowadzenia przez Zamawiającego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, zgodnie z ustawą Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (t.j. Dz. U. z 2019 r. poz. 1843. z późn. zm.; dalej jako „ustawa pzp"), pn. „dostawa systemu kolekcji i korelacji logów - SIEM" zawarta została umowa o następującej treści:

§ 1. PRZEDMIOT UMOWY.

1.1. Przedmiotem umowy jest:

1) zapewnienie Zamawiającemu – Gminie Olsztyn udzielenia licencji na system kolekcji i korelacji logów (security information and event management - SIEM) w postaci maszyny wirtualnej uruchomionej na środowisku wirtualizacyjnym Zamawiającego, spełniającego wymagania opisane w załączniku nr 1 do umowy (dalej jako: „System");
2) instalacja i uruchomienie Systemu oraz konfiguracja po jednym ze źródeł logów i flow-ów wskazanych przez Zamawiającego, w tym przeprowadzenie strojenia Systemu w celu otrzymywania efektywnych monitów o zagrożeniach;
3) wykonanie kopii zapasowej skonfigurowanego Systemu;
4) przeprowadzenie instruktażu stanowiskowego dla 2 osób wskazanych przez Zamawiającego;
5) sporządzenie i dostarczenie Zamawiającemu dokumentacji powykonawczej w postaci papierowej lub elektronicznej zawierającej m.in.:
   a) konfigurację Systemu,
   b) pełną instrukcję odzyskiwania Systemu z backupu;
6) zapewnienie udzielenia przez producenta Systemu wsparcia technicznego (gwarancji) w zakresie i na warunkach określonych w § 5 umowy, w tym usuwania awarii oraz aktualizacji Systemu oraz nowych wersji oprogramowania.

1.2. System posiadać będzie:

1) zgodność z posiadanym przez Zamawiającego środowiskiem VMware vSphere 6.5.;
2) możliwość analizy minimum 1500 zdarzeń na sekundę (EPS) i minimum 75000 przepływów na minutę (FPM) oraz możliwość rozbudowy licencyjnej do minimum 5000 zdarzeń na sekundę i 200000 przepływów na minutę.

1.3. System musi być zgodny z parametrami technicznymi i użytkowymi oraz warunkami świadczenia gwarancji i serwisu określonymi w Szczegółowym opisie przedmiotu zamówienia stanowiącym załącznik nr 1 do niniejszej umowy (dalej: „SOPZ") oraz ofertą Wykonawcy stanowiącą załącznik nr 2 do umowy.

1.4. Wykonawca zapewnia, że System będzie nowy, nieużywany, pochodzący z legalnego kanału dystrybucyjnego producenta Systemu, dopuszczony do dystrybucji i używania w Polsce oraz objęty gwarancją producenta. Zamawiający jest uprawniony do weryfikacji legalności Systemu i wykorzystywanego w Systemie oprogramowania.

1.5. Wykonawca zapewnia, że System jest odpowiedniej jakości i funkcjonalności, a także wolny od wad i nie jest przedmiotem praw lub roszczeń osób trzecich.

§ 2.ZASADY REALIZACJI UMOWY.

2.1. Wykonawca zapewni realizację przedmiotu umowy na koszt i ryzyko Wykonawcy, **w terminie 30 dni od daty zawarcia umowy**, z zastrzeżeniem szczegółowych terminów wskazanych w ust. 2.2:

2.2. Wykonawca zrealizuje przedmiot umowy w następujących terminach szczegółowych:

1) zapewni Zamawiającemu udzielenie licencji na System oraz dostarczy System i wykona instalację Systemu w terminie 10 dni od daty zawarcia umowy;

2) wykona uruchomienie na wskazanym przez Zamawiającego środowisku wirtualizacyjnym i skonfigurowanie Systemu wraz ze strojeniem, w celu otrzymywania efektywnych monitów o zagrożeniach, w terminie 20 dni po zapewnieniu Zamawiającemu udzielenia licencji na System oraz po wykonaniu instalacji Systemu, o czym mowa w ust. 2.1 pkt 2.2 z uwzględnieniem zapisów ust. 2.1 pkt 3);

3) w terminie umownym, o którym mowa w ust. 2.1., po dostarczeniu oraz instalacji, uruchomieniu i skonfigurowaniu Systemu, Wykonawca:

(a) wykona kopię zapasową skonfigurowanego z Systemu,

(b) sporządzi i dostarczy Zamawiającemu dokumentację powykonawczą, o której mowa w ust. 1.1 pkt 5)

(c) przeprowadzi instruktaż stanowiskowy dla 2 osób wskazanych przez Zamawiającego.

2.3. Wraz z Systemem Wykonawca dostarczy Zamawiającemu:

1) odpowiednie dokumenty w postaci papierowej lub elektronicznej potwierdzające, zgodnie z zasadami dystrybucji producenta bądź dystrybutora, fakt uzyskania przez Zamawiającego stosownych uprawnień do korzystania z Systemu;

2) dokumenty w postaci papierowej lub elektronicznej potwierdzające fakt uzyskania przez Zamawiającego uprawnień gwarancyjnych producenta, o których mowa w § 5 Umowy.

2.4. Po zrealizowaniu przez Wykonawcę obowiązków wskazanych w § 1 ust. 1.1 pkt 1) - pkt 1.1.5) Zamawiający przystąpi do procedury odbiorowej, w ramach której dokona m. in. weryfikacji zgodności przedmiotu umowy opisanego w § 1 ust. 1.1 pkt 1) - pkt 1.1.5) z wymaganiami określonymi w umowie. W przypadku braku wad wyżej wymienionego przedmiotu umowy, w tym prawidłowego działania Systemu i prawidłowej współpracy Systemu ze środowiskiem wirtualizacyjnym, o czym mowa w ust. 2.1 pkt 2), Zamawiający dokona odbioru i podpisze protokół odbioru końcowego, którego wzór stanowi załącznik nr 3 do umowy.

2.5. Zamawiający ma prawo zgłoszenia uwag co do zgodności Systemu z umową w razie stwierdzenia jego wad lub nieprawidłowości. W takim przypadku Zamawiający podpisze protokół odbioru z uwagami.

2.6. W wypadku zgłoszenia uwag przez Zamawiającego, Wykonawca dostarczy Zamawiającemu przedmiot umowy, w tym System, bez wad, zgodnie z wymaganiami określonymi w umowie lub usunie wady bądź nieprawidłowości w inny uzgodniony z Zamawiającym sposób, w terminie 5 dni roboczych. Za dzień roboczy uznaje się dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Polsce zgodnie z ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jedn.: Dz.U. z 2015 r., poz. 90 z późn. zm.).

2.7. Za datę wykonania przedmiotu umowy, o którym mowa w ust. 1.1. pkt 1) - 5), uważa się datę wskazaną w protokole odbioru końcowego przedmiotu umowy bez uwag, o którym mowa w ust. 2.4., wskazującą na termin wykonania poszczególnych czynności przedmiotu umowy określonego w ust. 1.1.

2.8. Wykonawca zobowiązuje się udzielać Zamawiającemu wszelkich informacji oraz udostępniać wszelkie dokumenty niezbędne do realizacji umowy, w których jest w posiadaniu lub powstałych w związku z jej realizacją.

2.9. Wykonawca zobowiązany jest informować niezwłocznie Zamawiającego o wszelkich okolicznościach mogących mieć wpływ na niewykonanie przez niego obowiązków lub mogących mieć wpływ na niedotrzymanie przez niego terminów określonych w umowie, co nie zwalnia go z odpowiedzialności za terminowe i należyte wykonanie umowy. Informacje, o których mowa w zdaniu poprzednim, będą przekazywane Zamawiającemu w formie dokumentowej.

§ 3.PRAWO DO KORZYSTANIA.

3.1. Zapewnienie prawa do korzystania z Systemu (oprogramowania systemowego, narzędziowego i zarządzającego maszyną wirtualną), polega na udzieleniu Zamawiającemu (Gminie Olsztyn) licencji lub zapewnienie udzielenia Zamawiającemu (Gminie Olsztyn) licencji przez podmiot uprawniony, bądź przeniesie na Zamawiającego (Gminę Olsztyn) licencji na korzystanie z Systemu bez ograniczeń terytorialnych, na potrzeby prowadzonej przez Zamawiającego (Gminę Olsztyn) działalności, na polach eksploatacji obejmujących trwałe lub czasowe zwielokrotnianie Systemu w całości lub w części, jakimikolwiek środkami i w jakiejkolwiek formie, przez czas nieokreślony, o ile rozwiązanie to pozwoli na uzyskanie przez Zamawiającego uprawnień opisanych umową.

3.2. Zapewnienie Zamawiającemu (Gminie Olsztyn) licencji możliwe jest również na podstawie innej formy prawnej korzystania z Systemu, w szczególności w oparciu o tzw. prawa legalnego nabywcy egzemplarza Systemu, jednak z wyłączeniem zapewnienia korzystania z Systemu w oparciu o model „Software as a Service", o ile rozwiązanie to pozwoli na uzyskanie przez Zamawiającego analogicznych uprawnień do Systemu, jak w przypadku licencji.

3.3. Zgodnie z przyjętym modelem dystrybucji Systemu, na warunkach wskazanych w umowie, Wykonawca zapewni Zamawiającemu (Gminie Olsztyn) prawo do korzystania z Systemu poprzez _____[1].

3.4. Wykonawca udziela Zamawiającemu nieograniczoną czasowo licencję na korzystanie z dokumentacji powykonawczej o której mowa w ust. 1.1 pkt 5), na polach eksploatacji obejmujących:

1) w zakresie utrwalania i zwielokrotniania utworu - wytwarzanie dowolną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;

2) w zakresie obrotu oryginałem albo egzemplarzami, na których utwór utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;

3) w zakresie rozpowszechniania utworu w sposób inny niż określony w pkt 2 - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.

3.5. Wykonawca udziela Zamawiającemu zgody na wykonywanie przez Zamawiającego z praw zależnych do dokumentacji powykonawczej, o której mowa w ust. 3.4.

3.6. W przypadku konieczności aktywacji uprawnień do korzystania, Wykonawca zapewni taką aktywację najpóźniej z momentem zapewnienia prawa do korzystania z Systemu, np. za pośrednictwem zdalnego dostępu.

[1] Do opisania przed zawarciem umowy model dystrybucji Systemu – przy wykorzystaniu mechanizmów wskazanych w ustępach powyżej.

3.7. W przypadku udzielenia licencji Wykonawca zobowiązuje się, że podmiot uprawniony nie wypowie Zamawiającemu (Gminie Olsztyn) udzielonej licencji z innego powodu niż naruszenie przez Zamawiającego warunków licencyjnych przez okres co najmniej 30 lat. Wypowiedzenie warunków korzystania z Systemu lub dokumentacji z powodu naruszenia warunków tego korzystania winno być poprzedzone pisemnym wezwaniem do zaniechania naruszeń warunków korzystania i bezskutecznym upływem wyznaczonego Zamawiającemu (Gminie Olsztyn) 30 dniowego terminu na zaniechanie naruszeń.

3.8. W przypadku aktualizacji lub poprawek Systemu z dniem udostępnienia aktualizacji lub poprawek Zamawiającemu (Gminie Olsztyn) Wykonawca zapewni udzielenie Zamawiającemu (Gminie Olsztyn) prawa do korzystania z aktualizacji Systemu na zasadach określonych w ust. 3.3.

3.9. Do niniejszej umowy nie znajdują zastosowania żadne ograniczenia zakresu licencji zawarte w standardowych warunkach licencjonowania Systemu, stosowanych przez Wykonawcę lub producenta Systemu, za wyjątkiem ograniczeń wyraźnie zaakceptowanych przez Zamawiającego (Gminę Olsztyn), poprzez pisemne zaakceptowanie treści certyfikatów lub innych dokumentów licencyjnych.

3.10. Podmiotami uprawnionym do korzystania z Systemu, bez ograniczeń, będą wszystkie jednostki organizacyjna Gminy Olsztyn, zarówno istniejące jak i przyszłe. Wykonawca zobowiązuje się nie wprowadzać żadnych ograniczeń prawnych ani technicznych, które by uniemożliwiały albo utrudniały realizację tego celu.

§ 4. WYNAGRODZENIE.

4.1. Za realizację przedmiotu umowy, o którym mowa w ust. 1.1., Zamawiający zobowiązuje się zapłacić Wykonawcy wynagrodzenie w łącznej wysokości _____ złotych netto (słownie: _____/100), powiększone o wartość podatku VAT w wysokości: _____ zł (słownie: _____/100), co daję kwotę brutto: _____ zł (słownie: _____/100).

4.2. Wykonawca oświadcza, że posiada firmowy rachunek bankowy związany z prowadzoną działalnością gospodarczą, zapłata wynagrodzenia zostanie dokonana z wykorzystaniem metody podzielonej płatności (split payment).

4.3. Zapłata wynagrodzenia nastąpi w formie przelewu na rachunek bankowy Wykonawcy wskazany na fakturze. Zapłata nastąpi w terminie 30 (trzydziestu) dni od dnia wystawienia faktury pod warunkiem doręczenia faktury w terminie 7 (siedmiu) dni od dnia jej wystawienia. W przypadku doręczenia faktury po terminie 7 (siedmiu) dni od dnia jej wystawienia, termin zapłaty ulega wydłużeniu o ilość dni przekroczenia wskazanego wyżej 7 (siedmio) dniowego terminu.

4.4. Podstawą do wystawienia faktury jest podpisany przez Zamawiającego protokół odbioru bez uwag, o którym mowa w ust. 2.4. umowy.

4.5. Na fakturze winny znajdować się następujące dane:

NABYWCA:	ODBIORCA:
Gmina Olsztyn,	Centrum Informatycznych Usług Wspólnych Olsztyna
Plac Jana Pawła II 1	Plac Jana Pawła II 1
10-101 Olsztyn	10-101 Olsztyn
NIP: 739-38-47-026	

4.6. Faktura powinna być dostarczona Zamawiającemu w następujący sposób:

1) na adres Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1, 10-101 Olsztyn, lub

2) na adres e-mail: sekretariat@ciuwo.olsztyn.eu według oświadczenia złożonego przez Strony zgodne z załącznikiem nr 4, lub

3) przy użyciu Platformy Elektronicznego Fakturowania (PEF).

4.7. W przypadku, gdy Wykonawca skorzysta z możliwości wysyłania Zamawiającemu faktury (tzw. ustrukturyzowanej faktury elektronicznej) przy użyciu Platformy Elektronicznego Fakturowania, o czym mowa w ust. 4.6.3), numer PEPPOL Zamawiającego to 7393921082. Oprócz danych zawartych w ust. 4.4. w opisie ustrukturyzowanej faktury elektronicznej Wykonawca zobowiązany jest do wskazania numeru i daty zawarcia niniejszej umowy.

4.8. Strony zgodnie postanawiają, że korekty faktur i noty księgowe (tzw. inne ustrukturyzowane dokumenty elektroniczne) mogą być wysyłane przy użyciu Platformy Elektronicznego Fakturowania, z uwzględnieniem postanowień ust. 4.7.

4.9. Za dzień zapłaty wynagrodzenia Strony uznają datę obciążenia rachunku bankowego Zamawiającego.

4.10. W przypadku nieterminowej zapłaty należności wynikającej z umowy Zamawiający zapłaci Wykonawcy odsetki w ustawowej wysokości z tytułu opóźnienia.

4.11. Wynagrodzenie określone w ust. 4.1. obejmuje wszelkie koszty i opłaty związane z realizacją przedmiotu umowy oraz wynikające z przepisów prawa, w tym koszty czynności wskazanych w § 1 ust. 1.1, w tym koszty zapewnienia udzielenia licencji, udzielenia gwarancji, a także podatek od towarów i usług, jeśli jest należny.

4.12. Wykonawca oświadcza, że jest czynnym podatnikiem podatku VAT i zgodnie z art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2018 r., poz. 2174 z późn. zm.) znajduje się w wykazie podmiotów zrejestrowanych jako podatnicy VAT (tzw. biała lista podatników VAT), w którym m.in. ujawniony został numer rachunku bankowego związany z prowadzoną przez Wykonawcę działalnością gospodarczą, służący do rozliczenia transakcji w ramach tej działalności i który zostanie wskazany na fakturze VAT wystawionej Zamawiającemu zgodnie z postanowieniami niniejszego paragrafu. Wykonawca oświadcza, że teraz i na przyszłość zrzeka się wszelkich roszczeń wobec Zamawiającego, w szczególności z tytułu braku terminowej zapłaty wynagrodzenia i wstrzymania się przez Zamawiającego z zapłatą wynagrodzenia w ramach niniejszej umowy w przypadku, gdy okaże się, że wskazany przez Wykonawcę na fakturze VAT numer rachunku bankowego nie będzie w dniu dokonania zapłaty przez Zamawiającego kwoty tytułem wynagrodzenia w ramach niniejszej umowy tożsamy z numerem rachunku bankowego ujawnionym na tzw. białej liście podatników VAT albo nie będzie ujawniony na tzw. białej liście podatników VAT – jeżeli zapłata wynagrodzenia na rachunek Wykonawcy nie ujęty na tzw. białej liście podatników VAT łączyłoby się dla Zamawiającego z jakimikolwiek negatywnymi konsekwencjami prawnymi - do czasu wskazania przez Wykonawcę rachunku bankowego ujawnionego na tzw. białej liście podatników VAT lub ujęcia na tej liście wskazanego wcześniej rachunku bankowego Wykonawcy.

§ 5.GWARANCJA

5.1. System, określony w § 1 ust. 1.1 umowy musi być objęty …….[2] roczną/letnią[3] gwarancją (wsparciem technicznym) producenta na warunkach nie gorszych niż określone w pkt 4 załącznika nr 1 do niniejszej umowy (SOPZ) oraz ofercie Wykonawcy będącej załącznikiem nr 2 do umowy.

5.2. Początkiem okresu gwarancyjnego dla Systemu jest dzień podpisania protokołu odbioru bez uwag, o którym mowa w ust. 2.4.

5.3. Wszelkie koszty związane z zapewnieniem obsługi w ramach gwarancji, a w szczególności: koszty dojazdu, instalacji i konfiguracji ponosi podmiot udzielający gwarancji.

§ 6.ODPOWIEDZIALNOŚĆ

[2] Do uzupełnienia przed zawarciem umowy, zgodnie z ofertą wybranego Wykonawcy, nie mniej niż 12 miesięcy.
[3] Niewłaściwe skreślić.

6.1. W razie opóźnienia w:

1) zapewnieniu Zamawiającemu udzielenia licencji na System, dostarczeniu Systemu oraz wykonaniu instalacji Systemu w stosunku do terminu, o którym mowa w ust. 2.1 pkt 2.2;

2) uruchomieniu i skonfigurowaniu Systemu, w tym strojeniu Systemu w stosunku do terminu, o którym mowa w ust. 2.1 pkt 2);

3) wykonaniu kopii zapasowej skonfigurowanego Systemu w stosunku do terminu, o którym mowa w ust. 2.1;

4) sporządzenia i dostarczenia Zamawiającemu dokumentacji powykonawczej w stosunku do terminu, o którym mowa w ust. 2.1;

5) przeprowadzenia instruktażu stanowiskowego dla 2 osób wskazanych przez Zamawiającego w stosunku do terminu, o którym mowa w ust. 2.1;

Wykonawca zapłaci Zamawiającemu za każde ww. naruszenie za każdy dzień opóźnienia karę umowną w wysokości 0,2 % ceny brutto określonej w ust. 4.1. umowy.

6.2. W razie uchybienia przez Wykonawcę terminowi – czas reakcji na wady Systemu - określonemu w pkt 4.1.4 lub 4.1.5. załącznika nr 1 do niniejszej umowy (SOPZ), Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 200 zł za każdy dzień przekroczenia terminu, za każdy z wyżej wymienionych terminów, za każde zgłoszenie.

6.3. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20 % ceny brutto określonej w ust. 4.1. w przypadku odstąpienia od umowy lub wypowiedzenia umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy.

6.4. W razie wykonania przez Zamawiającego prawa odstąpienia od umowy lub wypowiedzenia umowy Zamawiający może dochodzić zarówno kary umownej przewidzianej w ust. 6.3. jak i innych kar umownych należnych do dnia odstąpienia od umowy lub wypowiedzenia umowy.

6.5. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przewyższającego kary umowne na zasadach ogólnych.

§ 7. PRZETWARZANIE DANYCH OSOBOWYCH I ZACHOWANIE POUFNOŚCI INFORMACJI

7.1. Wykonawca zobowiązuje się do przestrzegania Regulaminu Ochrony Informacji dla wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna, który stanowi załącznik nr 5.

7.2. Wykonawca zobowiązuje się do zapewnienia przestrzegania przepisów o ochronie danych osobowych. Wobec faktu, że w ramach wykonywania niniejszej umowy Wykonawca będzie miał dostęp do danych osobowych przetwarzanych przez Zamawiającego, Strony zawarły umowę powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji, która stanowi załącznik nr 6.

7.3. Wykonywanie przez Wykonawcę obowiązków wynikających z umowy powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji odbywać się będzie w ramach wynagrodzenia należnego Wykonawcy z tytułu wykonania umowy i Wykonawca nie będzie uprawniony do żądania od Zamawiającego dodatkowego wynagrodzenia z tego tytułu.

7.4. Wykonawca pozostaje w posiadaniu Informacji Poufnych, przekazanych przez Zamawiającego, przez okres trwania umowy oraz zobowiązuje się do nieujawniania, nieprzekazywania, ani do niewykorzystywania we własnej działalności, w zakresie szerszym niż niezbędny do realizacji umowy, informacji uzyskanych w związku z wykonaniem umowy niezależnie od formy przekazania tych informacji, ich źródła i sposobu przetwarzania oraz bezzwłocznego trwałego ich usunięcia natychmiast po jej wygaśnięciu. Zasady poufności znajdują się w umowie powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji stanowiącej załącznik nr 6.

§ 8.OSOBY ODPOWIEDZIALNE

8.1. Osobami upoważnionymi do kierowania całością spraw związanych z realizacją umowy, w tym podpisania protokołu odbioru, o którym mowa w ust. 2.4, są:

1) w imieniu Zamawiającego:

(a) Dyrektor CIUWO, p.o. Dyrektora CIUWO, Zastępca Dyrektora CIUWO lub osoba upoważniona przez Dyrektora CIUWO

2) w imieniu Wykonawcy:

(a) _____

(b) _____

8.2. Osobami odpowiedzialnymi za realizację zapisów umowy, ze strony Zamawiającego, w zakresie zgłaszania uwag co do zgodności Systemu z umową, w razie stwierdzenia jego wad lub nieprawidłowości oraz w zakresie realizacji uprawnień gwarancyjnych, będą:

1) _____ mail: _____, tel.: _____;

2) _____ mail: _____, tel.: _____.

8.3. Osobami odpowiedzialnymi za realizację zapisów umowy, ze strony Wykonawcy, będą:

1) _____ mail: _____, tel.: _____;

2) _____ mail: _____, tel.: _____.

8.4. Zmiana osób wymienionych w ust. 8.1. - 8.3. w trakcie realizacji umowy wymaga poinformowania drugiej Strony w formie dokumentowej i nie stanowi zmiany umowy.

8.5. Strony zobowiązują się do kierowania wszelkiej korespondencji i oświadczeń, co do których umowa nie dopuszcza zachowania formy dokumentowej, na adresy stron wymienione w komparycji umowy, a w przypadku zmiany adresu, do niezwłocznego, pisemnego powiadomienia o tym fakcie drugiej Strony.

8.6. W przypadku braku powiadomienia, o którym mowa w ust. 8.5., doręczenie korespondencji na adres wskazany w komparycji umowy wywiera przewidziane prawem skutki prawne.

§ 9.ODSTĄPIENIE I ROZWIĄZANIE

9.1. Zamawiający może odstąpić od umowy, bez wyznaczania dodatkowego terminu, w przypadku gdy opóźnienie w stosunku do terminu określonego w ust. 2.1. (zgodnie z którym Wykonawca zapewni realizację przedmiotu umowy na koszt i ryzyko Wykonawcy, w terminie 30 dni od daty zawarcia umowy) przekroczy 10 dni, a także w przypadkach określonych w kodeksie cywilnym dla umowy o dzieło.

9.2. Zamawiający ma prawo odstąpić od umowy na zasadach określonych w art. 145 ustawy pzp. W przypadku odstąpienia od umowy na zasadach określonych w art. 145 ustawy pzp, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

9.3. Zamawiający ma prawo rozwiązać umowę na zasadach określonych w art. 145a ustawy pzp. W przypadku rozwiązania umowy na zasadach określonych w art. 145a ustawy pzp Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

9.4. Złożenie oświadczenia o wypowiedzeniu umowy oraz o odstąpieniu od umowy wymaga formy pisemnej pod rygorem nieważności.

§ 10.ZABEZPIECZENIE.

10.1. Wykonawca przed zawarciem umowy ustanowił zabezpieczenie należytego wykonania umowy, w wysokości 5 % wynagrodzenia brutto, o którym mowa w ust. 4.1. w celu zabezpieczenia roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania umowy w formie ……..[4].

10.2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.

10.3. Jeżeli zabezpieczenie wniesiono w pieniądzu, Zamawiający przechowa je na oprocentowanym rachunku bankowym. Zamawiający zwróci zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.

10.4. W trakcie realizacji umowy Wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w art. 148 ust. 1 ustawy pzp.

10.5. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.

10.6. W przypadku nieprzedłużenia lub niewniesienia nowego zabezpieczenia najpóźniej na 30 dni przed upływem terminu ważności dotychczasowego zabezpieczenia wniesionego w innej formie niż w pieniądzu, Zamawiający zmieni formę na zabezpieczenie w pieniądzu, poprzez wypłatę kwoty z dotychczasowego zabezpieczenia. Wypłata nastąpi nie później niż w ostatnim dniu ważności dotychczasowego zabezpieczenia.

10.7. Zamawiający zwraca 100% kwoty należytego zabezpieczenia umowy w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane.

§ 11. SIŁA WYŻSZA

11.1. Strony przewidują zmianę terminu realizacji umowy z powodu działania siły wyższej uniemożliwiającej realizację umowy w terminie określonym w ust. 2.1.

11.2. Zmiana terminu realizacji umowy dopuszczalna jest tylko o czas działania siły wyższej oraz o czas potrzebny do usunięcia skutków tego działania.

11.3. W przypadku stwierdzenia braku dostępności na rynku Systemu z przyczyn od Wykonawcy niezależnych, w szczególności wycofania oferowanego modelu z produkcji lub wprowadzenia zakazu importu lub eksportu danego modelu dopuszcza się, bez zmiany terminu realizacji, dostarczenie Systemu o cechach i parametrach nie gorszych niż zaproponowane w ofercie oraz zgodnych z parametrami technicznymi i użytkowymi określonymi w załączniku nr 1 do umowy. Zmiana nie wpływa na wysokość ceny należnej Wykonawcy z tytułu realizacji niniejszej umowy.

§ 12.PODWYKONAWCY

12.1. Wykonawca odpowiada wobec Zamawiającego za działania i zaniechania podwykonawców jak za swoje własne działania i zaniechania.

12.2. Wykonawca zapewnia, że podwykonawcy będą przestrzegać wszelkich postanowień umowy.

12.3. Wykonawca nie może powierzyć podwykonawcom do wykonania innych części przedmiotu umowy niż te, które wymienił w swojej ofercie, bez uprzedniej zmiany umowy.

[4] Należy uzupełnić zgodnie z wyborem przez Wykonawcę jednej lub kilku z następujących form zabezpieczenia:
1. pieniądz;
2. poręczenia bankowe lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
3. gwarancje bankowe;
4. gwarancje ubezpieczeniowe;
5. poręczenia udzielane przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

§ 13.ZMIANA UMOWY

13.1. Zmiana umowy możliwa jest w przypadkach wskazanych w ustawie z dnia 29 stycznia 2004 – Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 ze zm.).

13.2. Podstawą zmiany umowy może być w szczególności stworzenie przez producenta oprogramowania nowej wersji oprogramowania w stosunku do wskazanej w ofercie, stworzenie przez producenta oprogramowania wyższej wersji oprogramowania (o szerszych możliwościach) w stosunku do wskazanej w ofercie, zmiana sposobu dystrybucji oprogramowania lub modelu licencjonowania, potrzeba rozszerzenia zakresu licencji.

§ 14.POSTANOWIENIA KOŃCOWE

14.1. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.

14.2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy ustawy pzp, Kodeksu cywilnego oraz inne odpowiednie przepisy powszechnie obowiązującego prawa.

14.3. Ewentualne spory powstałe w związku z wykonywaniem przedmiotu umowy będą rozpatrywane przez sądy powszechne właściwe miejscowo dla siedziby Zamawiającego.

14.4. Wykonawca bez uprzedniej pisemnej zgody Zamawiającego nie może dokonać przeniesienia wierzytelności wynikających z niniejszej umowy na osoby trzecie.

14.5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

14.6. Następujące załączniki stanowią integralną część umowy:

Załącznik nr 1. – Szczegółowy opis przedmiotu zamówienia;

Załącznik nr 2. – Oferta Wykonawcy;

Załącznik nr 3. – Wzór protokołu odbioru końcowego;

Załącznik nr 4. – Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej;

Załącznik nr 5. – Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna;

Załącznik nr 6. – Umowa powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

Zamawiający **Wykonawca**

Załącznik nr 1

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

System kolekcji i korelacji logów - SIEM

1. **Wstęp.**
   Niniejszy dokument zawiera opis wymagań funkcjonalnych i technicznych wraz z dostawą i zakresem wdrożenia systemu kolekcji i korelacji logów (security information and event management - SIEM). W ramach realizacji przedmiotu zamówienia Wykonawca dostarczy kompletny system SIEM w formie maszyny wirtualnej w pełni zgodnej z posiadanym przez Zamawiającego rozwiązaniem wirtualizacyjnym. Realizując przedmiot zamówienia Wykonawca dostarczy i skonfiguruje wszelkie dostarczone oprogramowanie, tworząc działający system SIEM.
2. **Specyfikacja techniczna.**
   2.1. Wymagania dotyczące systemu SIEM:
   - 2.1.1. System musi być zainstalowany w formie maszyny wirtualnej na środowisku wirtualizacyjnym dostarczonym przez Zamawiającego,
   - 2.1.2. System musi zapewniać centralne monitorowanie wszystkich komponentów infrastruktury sieciowej,
   - 2.1.3. System musi posiadać wbudowaną obsługę normalizacji logów,
   - 2.1.4. System musi normalizować wspólne pola zdarzeń (tj. nazwy użytkowników, adresy IP, nazwy hostów i urządzenia będące źródłami logów) dla różnych urządzeń w sieci składającej się z systemów od wielu dostawców,
   - 2.1.5. System musi pozwalać na wyodrębnianie, normalizowanie i agregowanie pól zdarzeń, które nie są domyślnie normalizowane przez produkt,
   - 2.1.6. System musi nadawać odpowiednie wagi zgłaszanym powiadomieniom w celu określania dla nich priorytetów obsługi,
   - 2.1.7. System musi obsługiwać i normalizować znaczniki czasowe zdarzeń w wielu strefach czasowych,
   - 2.1.8. System musi analizować zdarzenia w czasie rzeczywistym,
   - 2.1.9. System musi umożliwiać przesyłanie alertów do innych systemów zarządzania,
   - 2.1.10. System musi oferować długoterminowe analizy trendów dotyczące zdarzeń,
   - 2.1.11. System musi oferować w ramach interfejsu użytkownika konfigurator i funkcje do minimalizowania liczby fałszywych alarmów,
   - 2.1.12. System musi oferować widok zdarzeń w czasie rzeczywistym, który może być dowolnie filtrowany,
   - 2.1.13. System musi zapewniać analitykę behawioralną i umożliwiać powiadamianie o anomaliach, zmianach w zachowaniu sieci i zdarzeniach bezpieczeństwa,
   - 2.1.14. W ramach analizy behawioralnej System musi dynamicznie uczyć się normalnego zachowania sieci i powiadamiać o pojawiających się zmianach,
   - 2.1.15. System musi zapewnić analizę i korelację ruchu w oparciu o obsługę protokołów: NetFlow, IPFIX, JFlow, SFlow,
   - 2.1.16. System musi mieć możliwość identyfikacji aplikacji w oparciu o przepływy oraz poprzez zasilenie danymi z systemów analizy ruchu sieciowego do warstwy 7. Identyfikacja aplikacji nie może zachodzić wyłącznie w oparciu o port komunikacyjny TCP/UDP, ale musi uwzględniać faktyczną zawartość ruchu,
   - 2.1.17. System musi integrować się z systemami typu NAC w celu zapewnienia widoczności użytkowników w sieci,
   - 2.1.18. System musi posiadać funkcję wykrywania zdarzeń typu „zero-day". Musi obsługiwać monitorowanie i wykrywanie aplikacji dla potrzeb rozpoznawania ruchu niezgodnego z politykami, w tym aplikacji P2P i strony portali społecznościowych,
   - 2.1.19. System musi zapewniać automatyczne wykrywanie wewnętrznych zasobów sieciowych w celu ograniczenia powstawania „false positives" (np. serwer DHCP),

2.1.20. System musi umożliwiać wizualizację geograficzną (czyli z jakiego kraju pochodzi dany ruch),
2.1.21. System musi oferować interfejs API dla potrzeb dostępu do danych przechowywanych w informacyjnej bazie danych,
2.1.22. System musi tworzyć i utrzymywać bazę danych zawierającą wszystkie wykryte zasoby sieciowe i zebrane o nich informacje (tj. atrybuty systemu, atrybuty sieciowe, stan zabezpieczeń, itp.) Baza danych musi umożliwiać edytowanie atrybutów, jeżeli nie mogą być one pozyskane automatycznie (tj. departament, lokalizacja, itp.). Użytkownik musi mieć możliwość przeszukiwania bazy danych,
2.1.23. System musi posiadać wbudowany korelator z możliwością jednoczesnej korelacji zdarzeń z różnych systemów oraz przepływów,
2.1.24. System musi umożliwiać wprowadzanie modyfikacji reguł korelacyjnych, oraz tworzenia własnych reguł,
2.1.25. System musi mieć możliwość efektywnego przechowywania zebranych logów (np. przez kompresję),
2.1.26. System musi obsługiwać powszechnie dostępne na rynku metody do zbierania logów (Syslog TCP/UDP/TLS, WMI, ODBC/JDBC, SNMP, OPSEC LEA),
2.1.27. System musi oferować możliwość dystrybucji przechowywania i przetwarzania zdarzeń w ramach całego systemu,
2.1.28. System musi umożliwiać szyfrowanie komunikacji pomiędzy komponentami,
2.1.29. System musi umożliwiać zbieranie informacji o sieci i zabezpieczeniach bez konieczności umieszczania agentów lub innych opartych na hoście mechanizmów w istniejących klientach lub serwerach,
2.1.30. System musie zapewnić przechwytywanie danych dla potrzeb analiz dochodzeniowych. Ilość przechwytywanych danych musi być konfigurowalna dla każdego przepływu,
2.1.31. System musi posiadać funkcję powiadamiania, bazującą na zaobserwowanych zagrożeniach bezpieczeństwa, anomaliach i zmianach w zachowaniu monitorowanych urządzeń,
2.1.32. System musi umożliwiać tworzenie przez użytkownika własnych profili i widoków, przy wykorzystaniu dowolnej cechy przepływu, zewnętrznego źródła danych lub już sprofilowanego ruchu,
2.1.33. System musi umożliwiać nadawanie odpowiedniej wagi powiadomieniom umożliwiając w ten sposób ich priorytetyzację. Wagi muszą być przypisywane w oparciu o wiele parametrów, takich jak typ zasobu, protokół, aplikacja, itp.,
2.1.34. System musi umożliwiać generowanie raportów zgodnych z ISO 27001 oraz musi posiadać konfigurowalny mechanizm raportowania dla potrzeb tworzenia własnych raportów,
2.1.35. System musi obsługiwać możliwość planowania raportów,
2.1.36. System musi obsługiwać automatyczną dystrybucję wygenerowanych automatycznie raportów,
2.1.37. System musi zapewniać scentralizowane zarządzanie wszystkimi elementami i dostęp do funkcji administracyjnych z poziomu jednego interfejsu użytkownika wykorzystującego przeglądarkę sieci Web. Panel zarządczy umożliwiający szybką wizualizację informacji o sieci i zabezpieczeniach,
2.1.38. System musi mieć możliwość definiowania opartego na rolach dostępu do systemu, wg urządzenia, grupy urządzeń lub zakresu sieci. Oznacza to możliwość ograniczania dostępu użytkownika tylko do informacji pochodzących z systemów należących do określonej grupy urządzeń lub zakresu sieci,
2.1.39. System musi mieć możliwość określenia opartego na rolach dostępu do różnych obszarów funkcjonalnych rozwiązania. Oznacza to możliwość ograniczenia dostępu użytkownika do określonych funkcji rozwiązania, które nie są związane z jego rolą, np. administracja, raportowanie, filtrowanie zdarzeń, korelacja i/lub podgląd paneli sterowania,
2.1.40. System musi integrować się z systemami katalogowymi od innych producentów stosowanymi jako metoda uwierzytelniania administratorów,

2.1.41. System musi oferować możliwość stosowania wielu paneli sterowania (dashboards), które mogą być dostosowane do określonych wymagań różnych użytkowników systemu,
2.1.42. System musi być wyposażony w funkcję wykrywania ataków DoS (Denial-of-Service) i DDoS (Distributed Denial-of-Service),
2.1.43. Rozwiązanie musi zapewniać integralność i niezaprzeczalność zebranych informacji,
2.1.44. System musi posiadać funkcję automatycznego wykrywania źródeł logów,
2.1.45. System musi posiadać funkcję automatycznego wykrywania aplikacji,
2.1.46. System musi posiadać funkcję automatycznego wykrywania zasobów sieciowych,
2.1.47. System musi posiadać funkcję automatycznego wykrywania luk w zabezpieczeniach,
2.1.48. System musi posiadać funkcję automatycznego grupowania zasobów,
2.1.49. System musi posiadać funkcję aktualizacji sygnatur zagrożeń, wsparcia urządzeń i aktualizacji oprogramowania z poziomu interfejsu użytkownika,
2.1.50. System musi posiadać funkcję automatycznej oceny poziomu zagrożenia zgłoszonych zdarzeń bezpieczeństwa, zależnej od stanu zabezpieczeń zaatakowanych zasobów,
2.1.51. System musi posiadać automatyczne wewnętrzne procedury do sprawdzania stanu systemu i powiadamiać użytkownika, gdy pojawiają się problemy,
2.1.52. System musi umożliwiać analizę minimum 1500 zdarzeń na sekundę (EPS) i minimum 75000 przepływów na minutę (FPM), z możliwością rozbudowy licencyjnej do minimum 5000 zdarzeń na sekundę i 200000 przepływów na minutę,
2.1.53. System musi zapewniać przechowywanie i dostęp do szczegółowych danych o zdarzeniach bezpieczeństwa i przepływach sieci przez czas do 60 miesięcy.

3. Zakres wdrożenia leżący po stronie Wykonawcy.

3.1. Zapewnienie Zamawiającemu udzielenia licencji (dostarczenie licencji).
3.2. Instalacja i uruchomienie systemu SIEM oraz konfiguracja po jednym ze źródeł logów i flow-ów wskazanych przez Zamawiającego.
3.3. Przeprowadzenie strojenia systemu SIEM w celu otrzymywania efektywnych monitów o zagrożeniach.
3.4. Backup konfiguracji systemu SIEM.
3.5. Przeprowadzenie instruktażu dla 2 osób.
3.6. Po uruchomieniu całości systemu Wykonawca sporządzi i przekaże dokumentację powykonawczą zawierającą m.in.:
3.6.1. Konfigurację systemu,
3.6.2. Pełną instrukcję odzyskiwania systemu z backupu.

4. Warunki gwarancji.

4.1. System SIEM musi być objęty gwarancją na następujących warunkach:
4.1.1. Gwarancja serwisowa udzielona przez producenta, a realizowana przez producenta lub autoryzowanego przedstawiciela producenta, przez okres minimum 1 rok. Po tym okresie Zamawiający zachowuje prawo do wieczystego korzystania z Systemu bez wsparcia i aktualizacji,
4.1.2. W okresie gwarancji wymagane jest usuwanie awarii, dostęp do wszystkich aktualizacji oraz nowych wersji oprogramowania,
4.1.3. W okresie gwarancji zapewniony dostęp do wsparcia przez e-mail i telefon przez 24 godziny, 7 dni w tygodniu,
4.1.4. Zgłoszenia krytyczne na skutek awarii uniemożliwiającej pracę systemu lub powodującej przerwę w bieżącej kolekcji logów – czas realizacji zgłoszenia i usunięcia problemu – do końca następnego dnia roboczego od momentu zgłoszenia,
4.1.5. Zgłoszenie na skutek awarii ograniczającej funkcjonalności systemu – czas realizacji zgłoszenia i usunięcia problemu – do końca drugiego dnia roboczego od momentu zgłoszenia.

Załącznik nr 2

OFERTA WYKONAWCY

Załącznik nr 3

WZÓR

PROTOKÓŁ ODBIORU KOŃCOWEGO

do umowy nr _____ z dnia _____

Odbierający:	**Przekazujący:**
Gmina Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1, 10-101 Olsztyn, NIP 739-384-70-26 (Zamawiający)	_____ _____ (Wykonawca)

Świadczenia polegające odbiorowi (przedmiot odbioru):

Lp.	Świadczenia polegające odbiorowi (przedmiot odbioru):	Data odbioru	Uwagi
1.	[Opis przedmiot odbioru zgodnie z umową]	[Data dostarczenia świadczenia zgodnego z umową]	[Zastrzeżenia lub stwierdzenie zgodności świadczenia z umową]
2.			
3.			

Przedmiot odbioru zostaje przyjęty bez zastrzeżeń ☐

Z uwagi na zgłoszone uwagi w tabeli Zamawiający odmawia odbioru przedmiotu odbioru[5] ☐

Dodatkowe uzasadnienie

[Dodatkowe uzasadnienie decyzji – jeśli dotyczy]

Dodatkowe ustalenia,

[Opis dodatkowych ustaleń – jeśli dotyczy]

Dodatkowe uwagi:

Przekazujący (Wykonawca):	
	podpis

Zamawiający:			
Imię i nazwisko		**Stanowisko**	
Data protokołu		**Podpis**	

[5] Należy zaznaczyć właściwy kwadrat

Załącznik nr 4

OŚWIADCZENIE WYKONAWCY O AKCEPTACJI PRZESYŁANIA FAKTUR DROGĄ ELEKTRONICZNĄ

Na podstawie art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174, z późn. zm.) **Zamawiający: Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna**; Pl. Jana Pawła II 1, 10-101 Olsztyn; NIP 739-384-70-26, akceptuje przesyłanie, w tym udostępniane faktur, ich korekt oraz duplikatów w formie PDF za pośrednictwem poczty elektronicznej.

Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna oświadcza, że:

1. Faktury VAT i korekty faktur należy przesyłać na adres email: sekretariat@ciuwo.olsztyn.eu,
2. Tytuł wiadomości email musi zawierać wyrażenie: faktura/faktury lub korekta/korekty lub korygująca/korygujące lub duplikat/duplikaty
3. Faktury VAT i korekty faktur, Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna wysyła z adresu e-mail: sekretariat@ciuwo.olsztyn.eu.

.....

Podpis Zamawiającego

Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej

Na podstawie art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174, z późn. zm.) akceptuję przesyłanie, w tym udostępnianie faktur, ich korekt oraz duplikatów w formie PDF za pośrednictwem poczty elektronicznej:

Nazwa firmy Wykonawcy: .....

Adres Wykonawcy: .....

Nr NIP Wykonawcy: ..... **Oświadczam, że:**

Faktury/korekty faktur/duplikaty faktur będę przesyłać do Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna z adresu e-mail:

Adres skrzynki nadawczej Wykonawcy: .....

Adresem właściwym do przesyłania faktur/ korekty faktur/duplikaty faktur przez Gminę Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna jest adres e-mail:

Adres skrzynki odbiorczej Wykonawcy: .....

.....

Podpis Wykonawcy

INFORMACJE DODATKOWE:

1. Faktury wraz ze wszystkimi załącznikami muszą być zapisane w formie PDF oraz załączone bezpośrednio do wiadomości e-mail.
2. Faktury i załączniki nie mogą być kompresowane i zaszyfrowane.
3. Skrzynka odbiorcza Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna – email: sekretariat@ciuwo.olsztyn.eu- jest obsługiwana automatycznie. Fakturę uważa się za doręczoną w momencie wpływu na skrzynkę odbiorczą Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna.
4. Wskazane powyżej adresy skrzynek pocztowych Zamawiającego i Wykonawcy są jedynymi właściwymi adresami stanowiącymi gwarancję pochodzenia faktury.

Załącznik nr 4

Załącznik nr 1 do Zarządzenia nr 24/2019 Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna z dnia 9 września 2019 r. w sprawie ustalenia regulaminu ochrony informacji dla Wykonawcy, wzoru umowy powierzenia przetwarzania danych oraz o zachowaniu poufności informacji, wzoru umowy o zachowaniu poufności informacji.

Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna

Spis treści

§1 CEL

1.1. Celem dokumentu w Centrum Informatycznych Usług Wspólnych Olsztyna jest:

1) Określenie minimalnych środków technicznych i organizacyjnych służących zabezpieczeniu danych.

2) Określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla podmiotów zewnętrznych.

3) Określenie minimalnych wymagań w zakresie zabezpieczeń systemów teleinformatycznych.

§2 ZAKRES

2.1. Niniejszy dokument stosują wszystkie podmioty zewnętrzne wykonujące prace na rzecz Centrum Informatycznych Usług Wspólnych Olsztyna (zwanego dalej CIUWO), związane z przetwarzaniem Aktywów informacyjnych Centrum Informatycznych Usług Wspólnych Olsztyna.

2.2. Niniejszy dokument należy stosować we wszystkich umowach z podmiotami zewnętrznymi, których przedmiot jest związany z ochroną informacji.

2.3. Stosowanie niniejszego dokumentu określającego minimalne środki techniczne i organizacyjne nie zwalnia podmiotów zewnętrznych ze stosowania środków adekwatnych, tj. dostosowanych do rodzaju przetwarzanych danych i sposobu ich przetwarzania tak, żeby zapewnić bezpieczeństwo przetwarzania stosownie do ryzyka naruszenia praw i wolności osób, których dane dotyczą, a które w konkretnych przypadkach mogą być dalej idące.

§3 TERMINOLOGIA

3.1. Pojęcia używane w Regulaminie:

1) **Aktywo i zasób informacyjny** – wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością CIUWO lub wykorzystywane bądź administrowane bądź zarządzane przez CIUWO.

2) **Główny Administrator Bezpieczeństwa Systemów (GABS)** – nadzoruje bezpieczeństwo wszystkich systemów teleinformatycznych. Jest odpowiedzialny za dopuszczanie systemów teleinformatycznych do eksploatacji.

3) **System informatyczny, System** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

4) **System Teleinformatyczny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

5) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia

bezpieczeństwa informacji.

§4 POSTANOWIENIA OGÓLNE

4.1. Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych 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 Centrum Informatycznych Usług Wspólnych Olsztyna.

4.2. Podmiot zewnętrzny spełnia wymagania niniejszego Regulaminu przed uzyskaniem dostępu do Systemu Teleinformatycznego CIUWO.

4.3. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych przetwarzanych przez CIUWO, podmiot zewnętrzny powinien spełnić następujące warunki:

1) w przypadku przetwarzania Informacji Poufnych – podpisać zobowiązanie do zachowania poufności przetwarzanych danych na wzorze obowiązującym w CIUWO, będącym załącznikiem nr 1 do Regulaminu.

2) w przypadku przetwarzania Informacji Poufnych i Danych – podpisać umowę powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji na wzorze obowiązującym w CIUWO, będącym załącznikiem nr 2 do Regulaminu.

§5 NADAWANIE, ZMIANA BĄDŹ ODEBRANIE UPRAWNIEŃ

5.1. W przypadku podmiotów zewnętrznych, zakres uprawnień w poszczególnych systemach i aplikacjach ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych danych osobowych.

5.2. Lista użytkowników podmiotu zewnętrznego powinna być dostarczona przez osoby ze strony podmiotu zewnętrznego wskazane w umowie jako odpowiedzialne za jej realizację.

5.3. Po każdej zmianie użytkowników ze strony podmiotu zewnętrznego, jest on zobowiązany do przekazania listy użytkowników ze wskazaniem zmian w ich zakresie uprawnień.

5.4. Rejestrowanie/wyrejestrowanie użytkowników zewnętrznych Systemu Teleinformatycznego CIUWO oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez pracowników CIUWO:

1) Podczas rejestracji użytkownika zewnętrznego nadawany jest przez administratora systemu unikalny identyfikator użytkownika oraz ustawiane jest hasło tymczasowe niezbędne do logowania po raz pierwszy do Systemu (zgodne z zasadami opisanymi w niniejszej procedurze) dla użytkownika zewnętrznego Systemu Teleinformatycznego.

2) O nadaniu/zmianie/odebraniu uprawnień właściwych identyfikatorów w odpowiednich systemach i aplikacjach i nadaniu właściwych uprawnień administrator systemu informuje GABS oraz przedstawiciela podmiotu zewnętrznego.

§6 METODY I ŚRODKI UWIERZYTELNIANIA

6.1. Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie

prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do Systemu Teleinformatycznego.

6.2. Hasła użytkowników do systemów powinny podlegać następującym zasadom:

1) hasło składa się z minimum 8 znaków,
2) hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),
3) hasło musi być zmieniane minimum co 30 dni,
4) kolejne hasła muszą być różne,
5) hasła należy przechowywać w sposób gwarantujący ich poufność,

6.3. Zabrania się udostępniania haseł innym osobom.

6.4. Zabrania się tworzenia haseł na podstawie:

1) cech i numerów osobistych (np. dat urodzenia, imion itp.),
2) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
3) identyfikatora użytkownika

6.5. Zabrania się tworzenia haseł łatwych do odgadnięcia.

6.6. Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.

6.7. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.

6.8. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko użytkownikowi.

6.9. 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 punktach poprzednich.

6.10. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.

6.11. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.

6.12. Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:

1) w plikach,
2) na kartkach papieru w miejscach dostępnych dla osób trzecich,
3) w skryptach,
4) w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.

6.13. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą zostać natychmiast zmienione przez użytkownika lub Administratora Systemu.

6.14. Hasło użytkownika sytemu umożliwiające dostęp do Systemu Teleinformatycznego utrzymuje się w tajemnicy również po upływie jego ważności.

6.15. Zmiany hasła dokonuje użytkownik. W przypadku gdy użytkownik zapomniał hasła, właściwy

Administrator Systemu ustawia hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania.

6.16. Hasła przez użytkowników nie powinny być przekazywane przesyłane za pomocą telefonu, faksu, bądź poczty e-mail w formie jawnej.

6.17. W przypadku grupowego tworzenia kont użytkowników generowane hasła powinny być unikalne.

§7 DOSTĘP ZDALNY

7.1. CIUWO prowadzi pisemny wykaz osób i podmiotów zewnętrznych posiadających dostęp zdalny do zasobów Systemu Teleinformatycznego CIUWO.

7.2. Dostęp zdalny podmiotów zewnętrznych możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym Regulaminie.

7.3. Dla każdej umowy z podmiotem zewnętrznym Dyrektor CIUWO wyznacza Koordynatora Prac Zdalnych CIUWO (dalej zwany KPZ) zgodnie z wzorem określonym w załączniku nr 4.

7.4. Podmiot zewnętrzny powierzając prace swoim pracownikom we własnym zakresie udziela im niezbędnych pełnomocnictw.

7.5. Dostępu udziela się na czas obowiązywania umowy na podstawie pisemnego wniosku przekazanego przez podmiot zewnętrzny do KPZ o podanie potrzebnych identyfikatorów i haseł dostępu.

7.6. 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.

7.7. W przypadku konieczności realizacji prac na środowisku produkcyjnym, podmiot zewnętrzny uzgadnia z KPZ termin prowadzenia prac obarczonych ryzykiem, o którym mowa w §8, 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:

1) Czas (moment) podjęcia planowanych prac, przewidywany czas trwania prac.
2) Zakres wykonywanych prac.
3) Informację, czy wymagana jest przerwa w pracy użytkowników.
4) Potencjalne ryzyka podejmowanych czynności.

7.8. Pracownik lub przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, co do których istnieje wysokie ryzyko utraty danych lub przerwy w działaniu systemu, informuje o ryzyku KPZ.

7.9. KPZ w przypadku otrzymania informacji o wysokim ryzyku utraty danych ustala możliwość rozpoczęcia prac z bezpośrednim przełożonym, Głównym Administratorem Bezpieczeństwa Systemów, a w przypadku takiej potrzeby – z innymi administratorami, w tym z administratorem systemu sesji zdalnych. Po akceptacji ryzyka przez KPZ w formie dokumentowej, pracownik

podmiotu zewnętrznego może rozpocząć realizację czynności objętej wskazanym ryzykiem. W przypadku braku akceptacji ryzyka, strony podejmują działania w celu usunięcia potencjalnych podatności dla ryzyka, a następnie przedstawiciel podmiotu zewnętrznego postępuje zgodnie z §7 i §8 powyżej.

7.10. 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.

7.11. Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci CIUWO.

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

7.13. Dostęp zdalny jest przez CIUWO monitorowany.

7.14. Monitorowanie odbywa się poprzez:

1) Logowanie ruchu w zakresie wszystkich sesji połączeń.
2) Nadzór nad wykonawcami za pomocą systemu monitorowania zdalnych sesji w zakresie prac wykonywanych zdalnie w sieci Urzędu,
3) Centralny system korelacji logów (SIEM) zbiera informacje ze wszystkich systemów i ocenia stopień zagrożenia sieci LAN.

7.15. W przypadku realizacji umowy głównej w trybie SaaS, IaaS lub DaaS, zapewnienie realizacji obowiązków określonych w §7 realizuje podmiot zewnętrzny.

§8 WYMAGANIA ZABEZPIECZEŃ

Zasady zabezpieczeń zasobów serwerowych i stacji roboczych

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

1) System antywirusowy jest zainstalowany w systemie operacyjnym i jego sygnatury są aktualne.
2) System operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń.
3) Firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera.
4) Zainstalowane na komputerze oprogramowanie pochodzi z godnych zaufania źródeł.
5) Oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.
6) Oprogramowanie nie łamie i nie narusza w żadnym stopniu przepisów ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. z późniejszymi zmianami.

8.2. W przypadku realizacji umowy głównej w trybie SaaS Podmiot zewnętrzny zobowiązuje się dodatkowo do:

1) W zakresie realizacji polityki Antywirusowej – do aktualizacji bazy definicji wirusów i przeprowadzania co najmniej cotygodniowego skanu Antywirusowego wszystkich serwerów, na których są zlokalizowane zasoby CIUWO. Skanowanie będzie przeprowadzane w godzinach nocnych/rannych. Ponadto Podmiot zewnętrzny zobowiązuje się do uruchomienia skanowania Antywirusowego na żądanie Zamawiającego w przypadku pozyskania przez niego informacji o zagrożeniu.

2) Celem potwierdzenia wywiązania się z realizacji zadań, przekazania do CIUWO pisemnego raportu 1 (jeden) raz na kwartał, zawierającego:

   i) planowaną ilość wykonanych kopii zapasowych i rzeczywistą ilość wykonanych kopii zapasowych,

   ii) potwierdzenie przeprowadzenia skanu Antywirusowego wszystkich serwerów, na których są zlokalizowane zasoby Zamawiającego wraz z wynikami skanu.

Stosowanie zabezpieczeń kryptograficznych

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

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.

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

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

8.6. Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES o długości klucza min. 256 bit.

§9 REAGOWANIE NA INCYDENTY

9.1. O ile zawarte między CIUWO a podmiotem zewnętrznym umowy nie przewidują dalej idących zobowiązań, każde naruszenie bezpieczeństwa informacji należy w ciągu [24] godziny od powzięcia informacji o jego wystąpieniu zgłaszać Inspektorowi Ochrony Danych telefonicznie pod numer 89 7525809 lub w formie e-mail za potwierdzeniem odbioru na adres iod@ciuwo.olsztyn.eu z tematem wiadomości „Naruszenie bezpieczeństwa informacji".

9.2. Inspektor Ochrony Danych w porozumieniu z Dyrektorem CIUWO, jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa, może zdecydować o natychmiastowym odebraniu uprawnień w systemach użytkownikom podmiotu zewnętrznego, przy czym w takiej sytuacji bez zbędnej zwłoki przekazuje on informację o blokadzie dostępu osobie upoważnionej ze strony podmiotu

zewnętrznego.

9.3. Upoważnione osoby z podmiotu zewnętrznego zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa.

9.4. W stosownych przypadkach Administrator Danych informuje o wystąpieniu incydentu bezpieczeństwa organ nadzorczy ds. ochrony danych osobowych oraz Podmiot danych.

9.5. W szczególnych przypadkach Administrator Danych informuje organy ścigania o zaistniałej sytuacji.

9.6. Sposób zgłaszania incydentów bezpieczeństwa przez Podmioty Zewnętrzne, postępowanie i odpowiedzialność dla naruszeń bezpieczeństwa określa umowa powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

§10 POSTANOWIENIA KOŃCOWE

10.1. Za nadzór nad przestrzeganiem postanowień Regulaminu odpowiada:

1) Ze strony podmiotu zewnętrznego – uprawniony przedstawiciel tego podmiotu.
2) Ze strony CIUWO – Inspektor Ochrony Danych oraz Główny Administrator Bezpieczeństwa Systemów.

10.2. Naruszając Regulamin, podmiot zewnętrzny może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów RODO.

§11 LISTA DOKUMENTÓW ZWIĄZANYCH

11.1. Wzór zobowiązania do zachowania poufności przetwarzanych danych;

11.2. Wzór umowy powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

§12 ZAŁĄCZNIKI

12.1. Wzór – wyznaczenie Koordynatora Prac Zdalnych CIUWO.

Załącznik nr 1 do Regulaminu Ochrony Informacji dla Wykonawcy CIUWO – Wzór – wyznaczenie Koordynatora Prac Zdalnych CIUWO

Wyznaczenie Koordynatora Prac Zdalnych
Centrum Informatycznych Usług Wspólnych Olsztyna

Na podstawnie zapisów zawartych w pkt. 8.3 Regulaminu, wyznaczam Panią /Pana*

Imię i nazwisko

na stanowisku

nazwa stanowiska

adres e'mail: tel.:

adres e'mail nr telefonu

po stronie Centrum Informatycznych Usług Wspólnych Olsztyna na Koordynatora Prac Zdalnych w ramach umowy zawartej pomiędzy Centrum Informatycznych Usług Wspólnych Olsztyna a:

Nazwa Wykonawcy

z siedzibą w

Siedziba Wykonawcy

adres:

Adres Wykonawcy

data Nr

Data zawarcia umowy powierzenia przetwarzania danych numer umowy

Dotyczącej

Przedmiot umowy

Obowiązującej w okresie od do

Początek obowiązywania umowy Koniec obowiązywania umowy

Dostęp zdalny odbywać się będzie na zasadach określonych w §7 wyżej powołanego Regulaminu, którego kopia została dostarczona Wykonawcy.

Wyznaczam:	Zatwierdzam:	Przyjąłem do stosowania:
data i podpis bezpośredniego przełożonego	data i podpis Dyrektora CIUWO	data podpis pracownika wyznaczonego na KPZ

Załącznik nr 4

Załącznik nr 2 do Zarządzenia nr 24/2019 Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna z dnia 9 września 2019 r. w sprawie ustalenia regulaminu ochrony informacji dla Wykonawcy, wzoru umowy powierzenia przetwarzania danych oraz o zachowaniu poufności informacji, wzoru umowy o zachowaniu poufności informacji.

/wzór/

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
ORAZ O ZACHOWANIU POUFNOŚCI INFORMACJI

dotycząca umowy: ……..

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

Centrum Informatycznych Usług Wspólnych Olsztyna oraz Gminą Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1; 10-101 Olsztyn, reprezentowaną przez

_____

(zwanym dalej **Powierzającym**)

a

…….. z siedzibą w **……**, przy ul. **……**, **……**, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, której akta rejestrowe są prowadzone przez Sąd Rejonowy w **……**, **……** Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr KRS: **……**, NIP: **……**, o kapitale zakładowym w wysokości **……** zł, wpłaconym w całości,

reprezentowaną przez

……..

(zwaną dalej **Przetwarzającym**),

zwanymi dalej łącznie **Stronami**, a każda z osobna **Stroną**,

Spis treści

§1 DEFINICJE

1.1. Dla potrzeb Umowy, Strony ustalają następujące znaczenie niżej wymienionych pojęć:

1) **Dane** – dane osobowe w rozumieniu art. 4 pkt 1) RODO.

2) **Dni Robocze** – dni w Pn 8:00 – 16:00, Wt-Pt 7:30 – 15:30, z wyłączeniem dni ustawowo wolnych od pracy w Polsce;

3) **Przetwarzanie Danych** – przetwarzanie Danych w rozumieniu art. 4 pkt 2) RODO;

4) **Umowa –** niniejsza umowa;

5) **Umowa Główna** – umowa …….. zawarta w dniu ……;

6) **RODO** – rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).

7) **Informacje Poufne** – oznaczają Dane oraz wszelkie inne materiały i/lub informacje dotyczące Powierzającego lub osób trzecich, zarówno handlowe, finansowe, techniczne, technologiczne i inne, ujawnione Przetwarzającemu w związku z realizacją przez Przetwarzającego dla Powierzającego Umowy Głównej, w tym stanowiące tajemnice przedsiębiorstwa, przekazane w postaci ustnej, pisemnej, elektronicznej lub w jakikolwiek inny sposób (w tym w formie dokumentów, prezentacji, rysunków, filmów, nagrań audio).

§2 PRZEDMIOT UMOWY

2.1. Przetwarzający oświadcza, że dysponuje odpowiednimi doświadczeniem, wiedzą oraz personelem, a także, że wdrożył i stosuje odpowiednie środki organizacyjne i techniczne w celu zapewnienia prawidłowego wykonywania Umowy oraz zapewnienia wystarczających gwarancji, aby Przetwarzanie Danych spełniało wymogi określone przepisami prawa, w tym regulacjami RODO.

2.2. Na podstawie art. 28 ust. 3 RODO oraz na zasadach określonych postanowieniami Umowy, Powierzający powierza Przetwarzającemu przetwarzanie Danych, a Przetwarzający zobowiązuje się przetwarzać Dane:

1) w zakresie obejmującym kategorie osób, których dane dotyczą, rodzaje informacji (Danych) oraz operacje lub zestawy operacji na Danych (czynności Przetwarzania Danych) wymienione w Załączniku nr [1] do Umowy oraz

2) wyłącznie w celu wykonania zobowiązań Przetwarzającego wynikających z Umowy Głównej.

2.3. Przetwarzający w zakresie realizacji celu określonego w ust. 2.2 pkt 2) jest uprawniony do wykonywania wyłącznie takich czynności Przetwarzania niezbędnych do realizacji tego celu.

2.4. Powierzenie Przetwarzania Danych następuje z chwilą zawarcia przez Strony Umowy.

2.5. Przetwarzanie Danych może odbywać się wyłącznie na terenie państwa członkowskiego Unii Europejskiej lub w innym państwie będącym sygnatariuszem Porozumienia o Europejskim Obszarze Gospodarczym (EOG), chyba że zachodzi wyjątek opisany w art. 49 RODO.

2.6. Z tytułu wykonywania świadczeń określonych w Umowie, Przetwarzającemu nie przysługuje

odrębne wynagrodzenie. Wykonywanie przez Przetwarzającego obowiązków określonych w Umowie następuje w ramach wynagrodzenia Przetwarzającego określonego w Umowie Głównej.

§3 POLECENIA POWIERZAJĄCEGO

3.1. W celu uniknięcia wątpliwości Strony postanawiają, że zawarcie Umowy stanowi udokumentowane polecenie Powierzającego, o którym mowa w art. 28 ust. 3 pkt a) RODO.

3.2. Dodatkowe polecenia dotyczące Przetwarzania Danych w trakcie realizacji Umowy będą przekazywane Przetwarzającemu przez Powierzającego w formie pisemnej, elektronicznej lub dokumentowej.

3.3. Przetwarzający jest zobowiązany zastosować się do poleceń Powierzającego, o których mowa w ust. 2 powyżej, w tym w szczególności dokonywać zmian w zakresie sposobu Przetwarzania Danych lub wdrożyć przewidziane w poleceniach środki techniczne lub organizacyjne niezwłocznie, nie później jednak niż w terminie [3] Dni Roboczych od dnia otrzymania polecenia, chyba że Strony w danym przypadku postanowią inaczej.

3.4. Jeżeli Przetwarzający uzna, że polecenie Powierzającego narusza przepisy o ochronie danych osobowych, Przetwarzający niezwłocznie informuje o tym Powierzającego i Przetwarzający ma prawo wstrzymać się z wykonaniem takiego polecenia do chwili potwierdzenia polecenia przez Powierzającego.

§4 ZOBOWIĄZANIA PRZETWARZAJĄCEGO

4.1. Przetwarzający zobowiązuje się do Przetwarzania Danych wyłącznie w zakresie i w ramach realizacji celu określonego w Umowie, z uwzględnieniem szczegółowych zasad Przetwarzania wynikających z postanowień Umowy, obowiązujących przepisów prawa, w tym regulacji dotyczących zasad przetwarzania danych osobowych, a w szczególności art. 32-36 RODO, a także wszelkich kodeksów postępowania, wytycznych oraz opisów dobrych praktyk, nawet jeśli nie stanowią powszechnie obowiązującego prawa, które powinny mieć zastosowanie do Umowy i Przetwarzania Danych realizowanego na jej podstawie.

4.2. Przetwarzający zobowiązuje się stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.

4.3. Przed rozpoczęciem Przetwarzania, Przetwarzający zobowiązuje się do wdrożenia, a przez cały okres obowiązywania Umowy do stosowania środków technicznych i organizacyjnych służących zabezpieczeniu Danych oraz realizowanych na podstawie umowy czynności Przetwarzania Danych, co najmniej w zakresie środków opisanych w Regulaminie Ochrony Informacji dla Wykonawcy.

4.4. Niezależnie od obowiązku wskazanego w ust. 4.3, Przetwarzający zobowiązuje się przez cały okres Przetwarzania Danych do zapewnienia bezpieczeństwa powierzonych do przetwarzania Danych poprzez wdrożenie, aktualizację i stosowanie odpowiednich środków organizacyjnych oraz technicznych w celu prawidłowego wykonania Umowy oraz zapewnienia wystarczających gwarancji, aby Przetwarzanie Danych spełniało wymogi określone przepisami prawa, w tym regulacjami RODO. W szczególności, Przetwarzający zobowiązuje się podjąć odpowiednie środki gwarantujące bezpieczeństwo Danych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą,

modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem, w szczególności wdrożyć, przy uwzględnieniu stanu wiedzy technicznej, charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, odpowiednie środki techniczne i organizacyjne, w celu zapewnienia stopnia bezpieczeństwa przetwarzania Danych odpowiadającego ryzyku określonemu przez Powierzającego, w tym między innymi w stosownym przypadku:

1) środki polegające na pseudonimizacji i szyfrowaniu danych osobowych,
2) środki gwarantujące zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
3) środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
4) środki zapewniające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

4.5. W przypadku stwierdzenia przez Przetwarzającego, że stosowane przez niego środki organizacyjne i techniczne mogą być nieadekwatne do rozpoznanych zagrożeń ochrony Danych, Przetwarzający ma obowiązek zastosować środki techniczne i organizacyjne odpowiednie do zapewnienia adekwatnego poziomu bezpieczeństwa Przetwarzania Danych oraz niezwłocznie poinformować o Powierzającego o podjętych działaniach, w tym o charakterze i terminie wdrożenia takich środków.

4.6. Przetwarzający zobowiązuje się przeszkolić pracowników oraz współpracowników uczestniczących w realizacji Umowy lub Umowy Głównej w zakresie regulacji prawnych dotyczących przetwarzania danych osobowych i ochrony informacji, a także stosowanych środków organizacyjnych i technicznych służących zapewnieniu bezpieczeństwa Przetwarzania Danych realizowanego na podstawie Umowy.

4.7. Przetwarzający zapewni, że każda osoba upoważniona przez Przetwarzającego do Przetwarzania, przetwarzała je wyłącznie na polecenie Powierzającego w celach i zakresie przewidzianym w Umowie, przy czym Powierzający upoważnia Przetwarzającego do udzielenia indywidualnych upoważnień do Przetwarzania Danych dla osób dokonujących Przetwarzania Danych w ramach realizacji Umowy.

4.8. Przetwarzający jest zobowiązany do poinformowania Powierzającego o wszelkich zmianach w zakresie osób upoważnionych do Przetwarzania Danych.

4.9. Przetwarzający zobowiązuje się prowadzić ewidencję osób upoważnionych do Przetwarzania Danych; na żądanie Powierzającego w terminie wskazanym w takim wezwaniu Przetwarzający przekaże Powierzającemu kopię lub, odpowiednio, wyciąg z takiej ewidencji.

4.10. Na żądanie Powierzającego wyrażone w formie dokumentowej, a w przypadku upoważnienia do Przetwarzania Danych za pośrednictwem zdalnego dostępu – bez żądania przed dopuszczeniem do Przetwarzania Danych – Przetwarzający zobowiązany jest do przekazania Powierzającemu kopii upoważnień do przetwarzania danych osobowych i oświadczeń o zachowaniu poufności.

4.11. Przetwarzający jest zobowiązany prowadzić rejestr kategorii czynności przetwarzania dokonywanych w imieniu Powierzającego, o którym mowa w art. 30 ust. 2 RODO.

4.12. Przetwarzający jest zobowiązany do prowadzenia rejestru naruszeń ochrony danych, w którym

dokumentowane są wszelkie naruszenia ochrony danych osobowych, dotyczące powierzonych danych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze przez Przetwarzającego.

4.13. Przetwarzający zobowiązuje się do niezwłocznego, jednak nie później niż w terminie [3] Dni Roboczych, informowania Powierzającego w formie pisemnej o:

1) każdym postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym Przetwarzania Danych przez Przetwarzającego;

2) każdej decyzji administracyjnej lub orzeczeniu dotyczącym Przetwarzania Danych, skierowanych do Przetwarzającego;

3) wszelkich kontrolach i inspekcjach dotyczących Przetwarzania Danych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy;

4) wszelkich skargach osób, których dane dotyczą, związanych z Przetwarzaniem dotyczących ich Danych;

5) każdym żądaniu udostępnienia powierzonych Przetwarzającemu Danych właściwemu organowi państwa, chyba że zakaz zawiadomienia Powierzającego wynika z bezwzględnie obowiązujących przepisów prawa;

6) każdym nieupoważnionym dostępie do Danych, których Przetwarzanie zostało powierzone Przetwarzającemu.

§5 WSPÓŁPRACA PRZETWARZAJĄCEGO Z POWIERZAJĄCYM

5.1. Przetwarzający zobowiązuje się współpracować z Powierzającym przez cały okres trwania powierzenia Przetwarzania Danych w zakresie umożliwiającym Powierzającemu wywiązanie się z wszelkich obowiązków związanych z przetwarzaniem Danych zgodnie obowiązującymi przepisami prawa.

5.2. Przetwarzający, w zakresie wskazanym przez Powierzającego, zobowiązuje się zapewnić Powierzającemu pomoc, w tym za pośrednictwem stosowanych przez siebie odpowiednich środków technicznych i organizacyjnych, w wywiązywaniu się przez Powierzającego z obowiązku odpowiadania na żądania osoby fizycznej, której przetwarzane Dane dotyczą, w zakresie wykonywania jej praw określonych w określonych w art. 15-22 RODO, w szczególności poprzez niezwłoczne przekazywanie Powierzającemu wszelkich otrzymanych żądań i wniosków osób, których Dane dotyczą, nie później jednak niż w terminie [2] Dni Roboczych od dnia ich wpłynięcia.

5.3. Przetwarzający nie jest upoważniony do udzielenia odpowiedzi na wniosek, o którym mowa w ust. 5.2, bez uprzedniej zgody lub wyraźnego polecenia Powierzającego. Powierzający uprawniony jest do wskazania sposobu realizacji żądania osoby, której dane dotyczą przez Przetwarzającego.

5.4. Przetwarzający zobowiązuje się współpracować z Powierzającym w zakresie niezbędnym do wywiązania się przez Powierzającego z obowiązku dokonania oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO oraz przeprowadzenia konsultacji Powierzającego z organem nadzorczym, o których mowa w art. 36 RODO; w szczególności Przetwarzający jest zobowiązany dostarczać Powierzającemu na jego żądanie, w terminie [3] Dni Roboczych od dnia sformułowania żądania, informacji niezbędnych do opisu planowanych operacji przetwarzania, a także jest zobowiązany do uczestniczenia w dokonywaniu oceny, czy te operacje są niezbędne oraz

proporcjonalne do celu przetwarzania oraz oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą.

5.5. Przetwarzający zobowiązuje się udostępniać Powierzającemu na każde jego żądanie, w formie określonej w treści żądania, niezwłocznie, nie później niż w terminie [2] Dni Roboczych od dnia sformułowania żądania (chyba że z uwagi na charakter lub zakres żądanej informacji strony uzgodnią dłuższy termin), wszelkie informacje niezbędne do wykazania spełnienia przez Powierzającego obowiązków w zakresie ochrony danych osobowych określonych w RODO oraz innych znajdujących zastosowanie przepisach prawa, w tym w celu należytego wykonania przez Powierzającego obowiązków w zakresie właściwego opisania zaistniałych naruszeń ochrony danych osobowych oraz podjętych środków w rejestrze prowadzonym przez powierzającego (art. 33 pkt 5 RODO) oraz w celu przygotowania dla organu nadzorczego lub osób, których dane dotyczą informacji o naruszeniach ochrony danych osobowych i podjętych środkach (art. 33 pkt 1 RODO i art. 34 RODO).

§6 NARUSZENIA

6.1. Przetwarzający jest zobowiązany do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony Danych oraz wdrażaniu właściwych środków naprawczych.

6.2. Przetwarzający jest zobowiązany do udzielania Powierzającemu informacji na temat procedur, o których mowa powyżej, na każde żądanie Powierzającego, w formie określonej w treści żądania, w terminie [2] Dni Roboczych od dnia sformułowania żądania.

6.3. Po stwierdzeniu naruszenia ochrony danych osobowych (także w przypadku poinformowania o naruszeniu przez Powierzającego), w rozumieniu art. 4 pkt 12) RODO, dotyczącego lub mogącego dotyczyć Danych powierzonych przez Powierzającego w tym w szczególności w zakresie stosowania art. 32-36 RODO, Przetwarzający niezwłocznie, jednak nie później niż w ciągu [24] godzin od chwili wykrycia naruszenia, zgłasza je Powierzającemu w formie dokumentowej, poprzez przesłanie wiadomości e-mail oraz w formie pisemnej.

6.4. Zgłoszenie, o którym mowa w ust. 6.3, zawiera co najmniej informacje o:

1) dacie, czasie trwania oraz lokalizacji naruszenia ochrony danych osobowych;
2) charakterze i skali naruszenia, tj. w szczególności o kategoriach i przybliżonej liczbie osób, których dane dotyczą, oraz kategoriach i przybliżonej liczbie wpisów danych osobowych, których dotyczy naruszenie, a w razie możliwości, także wskazania podmiotów danych, których dotyczyło naruszenie;
3) systemie informatycznym, w którym wystąpiło naruszenie (jeżeli naruszenie nastąpiło w związku z przetwarzaniem danych w systemie informatycznym);
4) przewidywanym czasie potrzebnym do naprawienia szkody spowodowanej naruszeniem;
5) charakterze i zakresie danych osobowych objętych naruszeniem;
6) możliwych konsekwencjach naruszenia, z uwzględnieniem konsekwencji dla osób, których dane dotyczą;
7) środkach podjętych w celu zminimalizowania konsekwencji naruszenia oraz proponowanych działaniach zapobiegawczych i naprawczych;
8) danych kontaktowych osoby mogącej udzielić dalszych informacji o naruszeniu.

6.5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w zgłoszeniu Przetwarzający jest zobowiązany poinformować Powierzającego o dokonaniu takiej oceny.

6.6. Do czasu uzyskania od Powierzającego wytycznych dotyczących wdrożenia odpowiednich środków naprawczych, Przetwarzający bez zbędnej zwłoki podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.

6.7. Przetwarzający jest zobowiązany do dokumentowania wszelkich naruszeń ochrony powierzonych mu danych osobowych, ich skutków oraz podjętych działań zaradczych w sposób i zakresie wskazanym w art. 33 ust 5 RODO; przetwarzający zobowiązuje się niezwłocznie udostępnić Powierzającemu dokumentację, o której mowa w zdaniu poprzedzającym, na każde żądanie Powierzającego niezwłocznie, nie później niż w terminie [2] dni od dnia otrzymania żądania przez Przetwarzającego, chyba że z uwagi na charakter lub zakres żądanej informacji strony uzgodnią dłuższy termin.

6.8. Przetwarzający zobowiązuje się nie powiadamiać o stwierdzonym naruszeniu bez wyraźnego polecenia Powierzającego w tym zakresie innych podmiotów, w tym osób, których dane dotyczą, ani organu nadzorczego, chyba że obowiązek taki wynika z przepisów prawa (w takim przypadku Przetwarzający jest zobowiązany do poinformowania o przekazaniu takiej informacji Powierzającego, chyba, że przekazanie takiej informacji stanowiłoby naruszenie obowiązujących przepisów prawa).

§7 POWIERZENIE DANYCH OSOBOWYCH INNEMU PODMIOTOWI PRZETWARZAJĄCEMU

7.1. Przetwarzający może powierzyć powierzone mu dane osobowe do przetwarzania innym podmiotom przetwarzającym jedynie w zakresie i celu zgodnym z Umową, wyłącznie po uzyskaniu pisemnej, pod rygorem nieważności, zgody Powierzającego. Przetwarzający zobowiązuje się do korzystania z usług wyłącznie takich innych podmiotów przetwarzających, które gwarantują wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia wystarczającego poziomu bezpieczeństwa przetwarzania danych osobowych.

7.2. W każdym przypadku korzystania z usług innego podmiotu przetwarzającego, Przetwarzający zawrze z innym podmiotem przetwarzającym umowę dalszego powierzenia przetwarzania danych osobowych i zobowiąże w niej inny podmiot przetwarzający do przestrzegania wszystkich obowiązków nałożonych na Przetwarzającego na podstawie niniejszej umowy, w tym w szczególności obowiązku zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO oraz zapewni możliwość przeprowadzenia przez Powierzającego bezpośredniej kontroli zgodności przetwarzania danych osobowych przez inny podmiot przetwarzający z umową oraz obowiązującymi przepisami prawa.

7.3. Na każde jego żądanie Powierzającego w celu wykazania spełnienia przez Przetwarzającego obowiązków wynikających z umowy Przetwarzający udostępni Powierzającemu wszelkie informacje dotyczące innych podmiotów przetwarzających oraz umowy zawarte z tymi podmiotami.

7.4. Powierzający może żądać od Przetwarzającego natychmiastowego rozwiązania umowy z innym podmiotem przetwarzającym w przypadku, gdy Przetwarzający zawarł z tym podmiotem umowę dalszego powierzenia przetwarzania danych osobowych bez uprzedniej pisemnej zgody

Powierzającego, jak również gdy dalszy podmiot przetwarzający nie daje gwarancji należytego zabezpieczenia danych osobowych, a także w każdym innym przypadku, gdy Powierzający będzie miał uzasadnione podstawy do stwierdzenia, że dalsze przetwarzanie danych przez taki podmiot ma negatywny wpływ na ochronę danych osobowych.

7.5. W przypadku niewywiązania się przez inny podmiot przetwarzający ze spoczywających na nim obowiązków ochrony danych osobowych, na Przetwarzającym spoczywa pełna odpowiedzialność wobec Powierzającego za wypełnienie obowiązków innego podmiotu przetwarzającego.

§8 OBOWIĄZEK ZACHOWANIA TAJEMNICY

8.1. Przetwarzający zobowiązany jest do zachowania w tajemnicy treści Danych oraz wszelkich innych Informacji Poufnych, w tym informacji o stosowanych środkach organizacyjnych i technicznych służących zabezpieczeniu Danych lub procesów Przetwarzania Danych – przez czas obowiązywania Umowy, jak również w okresie [15] lat po jej rozwiązaniu, chyba że dłuższy okres takiego obowiązku przewidują obowiązujące przepisy prawa.

8.2. Przetwarzający zobowiązuje się:

1) zachować w tajemnicy uzyskane Informacje Poufne;

2) nie przekazywać ani nie ujawniać bez każdorazowej uprzedniej pisemnej zgody Powierzającego, jakichkolwiek Informacji Poufnych żadnej osobie z wyjątkiem:

   i) pracowników Przetwarzającego wyznaczonych do realizacji Umowy Głównej, którzy potrzebują takich informacji w związku z realizacją Umowy Głównej, pod warunkiem podpisania przez nich oświadczenia stanowiącego Załącznik do Umowy, zawierającego zobowiązanie do zachowania w poufności oraz poinformowania takich osób o prawnych konsekwencjach naruszenia poufności Informacji Poufnych, w tym Danych;

   ii) przypadków, w których Przetwarzający jest zobowiązany do takiego ujawnienia przez sąd lub w przypadku ustawowego obowiązku takiego ujawnienia, z zastrzeżeniem, że Przetwarzający dołoży właściwych starań w celu uprzedniego pisemnego poinformowania Powierzającego przed dokonaniem takiego ujawnienia;

   iii) osób trzecich zaangażowanych przez Przetwarzającego do realizacji Umowy Głównej, pod warunkiem podpisania przez nich Oświadczenia stanowiącego Załącznik do Umowy, zawierającego zobowiązanie do zachowania w poufności informacji;

3) ponieść wobec Powierzającego 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 2) ppkt iii), za której działania Przetwarzający odpowiada, jak za działania własne;

4) nie wykorzystywać i nie rozpowszechniać Informacji Poufnych w ramach swojej działalności, z wyjątkiem wykorzystywania lub rozpowszechniania wyłącznie w zakresie koniecznym dla celów Umowy Głównej;

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

6) spowodować, na żądanie Powierzającego, aby którekolwiek z osób i organów, o których mowa

w pkt 2) ppkt 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.

8.3. Obowiązku zachowania poufności, o którym mowa w ust. 8.2, nie stosuje się do jakiejkolwiek części Informacji Poufnych, w stosunku, do których Przetwarzający może wykazać, że informacje takie są lub stały się publicznie znane z przyczyn, za które pozostają poza kontrolą Przetwarzającego; lub zostały zgodnie z prawem otrzymane od niezależnej osoby trzeciej bez naruszenia obowiązku zachowania poufności; lub w dacie ich ujawnienia przez Powierzającego lub otrzymania od Powierzającego były już znane Przetwarzającemu bez obowiązku zachowania poufności.

8.4. Przetwarzający może ujawnić Informacje Poufne otrzymane od drugiej Strony wyłącznie w celu wykorzystania w związku z realizacją Umowy Głównej, co nie uchybia ograniczeniom lub dodatkowym obowiązkom Przetwarzającego związanych z ujawnieniem Danych wynikającym z Umowy (w szczególności opisanym w §7 Umowy) oraz obowiązujących przepisów prawa.

8.5. Niezależnie od obowiązku wskazanego w ust. 8.2 pkt 2) ppkt i), Powierzający zobowiązuje się zapewnić, aby osoby upoważnione do Przetwarzania Danych dodatkowo zobowiązały się do zachowania tajemnicy, zarówno w trakcie trwania upoważnienia do Przetwarzania Danych, jak i po jego ustaniu.

8.6. Postanowienia powyższe nie uchybiają dalej idącym zobowiązaniom Przetwarzającego wynikającym z Umowy Głównej, innych umów zawartych z Powierzającym lub powszechnie obowiązujących przepisów prawa.

§9 KONTROLA I AUDYT

9.1. Powierzającemu przysługuje prawo przeprowadzenia w każdym momencie obowiązywania Umowy kontroli zgodności przetwarzania danych osobowych przez Przetwarzającego z Umową oraz obowiązującymi przepisami prawa, w szczególności zgodności i adekwatności stosowanych przez Przetwarzającego środków technicznych i organizacyjnych służących zapewnieniu bezpieczeństwa Przetwarzanych Danych, poprzez:

1) prawo żądania dostępu do posiadanej przez Przetwarzającego dokumentacji dotyczącej Przetwarzania Danych;

2) prawo żądania udzielenia wszelkich informacji dotyczących Przetwarzania Danych;

3) prawo przeprowadzania audytów lub inspekcji Przetwarzającego, w tym domagania się dostępu do pomieszczeń, infrastruktury, nośników oraz systemów informatycznych służących do przetwarzania powierzonych Danych, także prowadzonych przez osoby trzecie, działające na zlecenie i w imieniu Powierzającego.

9.2. Powierzający ma prawo żądać od Przetwarzającego w dowolnym momencie obowiązywania Umowy udzielenia informacji dotyczących Przetwarzania powierzonych mu Danych. Przetwarzający jest zobowiązany do udzielenia Powierzającemu stosownych informacji w formie określonej w treści żądania, niezwłocznie, nie później niż w terminie [2] dni od dnia otrzymania żądania przez Przetwarzającego, chyba że z uwagi na charakter lub zakres żądanej informacji strony uzgodnią dłuższy termin.

9.3. W przypadku zamiaru przeprowadzenia audytu w miejscach Przetwarzania Danych, Powierzający

poinformuje Przetwarzającego co najmniej [5] Dni Roboczych przed planowaną datą audytu o zamiarze jego przeprowadzenia. Jeżeli z ważnych powodów, w ocenie Przetwarzającego, audyt nie może zostać przeprowadzony we wskazanym terminie, Przetwarzający zobowiązany jest niezwłocznie poinformować o tym fakcie Powierzającego, drogą mailową, wskazując uzasadnienie dla takiej oceny. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.

9.4. Przetwarzający ma obowiązek współpracować z Powierzającym i upoważnionymi przez niego audytorami we wszelkim wymaganym czynnościami audytowymi zakresie, w szczególności zapewniać im dostęp do pomieszczeń i dokumentów obejmujących Dane oraz informacje o sposobie przetwarzania Danych, infrastrukturze teleinformatycznej oraz systemach IT, a także do osób mających wiedzę na temat procesów Przetwarzania Danych realizowanych przez Przetwarzającego.

9.5. Powierzający lub upoważnieni przez niego audytorzy po przeprowadzeniu audytu sporządzają protokół, zawierający wskazówki i zalecenia dotyczące w szczególności poprawy bezpieczeństwa Przetwarzania powierzonych Danych, który podpisują przedstawiciele obu Stron. Przetwarzający zobowiązuje się, w terminie uzgodnionym z Powierzającym, dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa Przetwarzania Danych.

§10 ODPOWIEDZIALNOŚĆ PRZETWARZAJĄCEGO

10.1. Strony zgodnie postanawiają, że jakiekolwiek ograniczenia odpowiedzialności Przetwarzającego przewidziane w Umowie Głównej nie będą miały zastosowania w odniesieniu do odpowiedzialności Przetwarzającego z tytułu niewykonania lub nienależytego wykonania Umowy, w szczególności naruszenia zasad Przetwarzania Danych.

10.2. Przetwarzający odpowiada za wszelkie szkody, jakie powstaną wobec Powierzającego, osób, których Dane dotyczą lub innych osób trzecich w wyniku niezgodnego z Umową lub obowiązującymi przepisami prawa przetwarzania Danych objętych powierzeniem, a w szczególności w związku z udostępnianiem Danych osobom nieupoważnionym.

10.3. Przetwarzający ponosi pełną odpowiedzialność za działania swoich pracowników, współpracowników, podwykonawców (w tym innych podmiotów przetwarzających) oraz innych osób, przy pomocy których Przetwarza powierzone Dane, jak za własne działania i zaniechania.

10.4. Przetwarzający zobowiązany jest pokryć każdą szkodę, a także wszelkie koszty, wydatki, w tym koszty obsługi prawnej oraz koszty kar finansowych, które Powierzający poniesie albo może ponieść lub za które może stać się odpowiedzialny w związku z jakimkolwiek pozwem, roszczeniem, bądź postępowaniem prowadzonym przeciwko niemu w związku z nienależytym wykonywaniem przez Przetwarzającego obowiązków wynikających z Umowy oraz obowiązków wynikających z RODO i innych właściwych przepisów.

10.5. Przetwarzający zobowiązany jest do niezwłocznego wezwania Powierzającego do przystąpienia do ewentualnego procesu, związanego z żądaniem odszkodowania za poniesioną przez osobę fizyczną szkodę majątkową lub niemajątkową związaną z Przetwarzaniem Danych naruszającym przepisy prawa i wytoczeniem powództwa w tym zakresie bezpośrednio przeciwko Przetwarzającemu, oraz prowadzenia procesu z udziałem Powierzającego jako interwenienta ubocznego albo w innym charakterze stosownie do obowiązujących przepisów procedury cywilnej.

10.6. W przypadku, gdy osoba fizyczna wytoczy powództwo bezpośrednio przeciwko Powierzającemu,

Powierzający zobowiązany jest do niezwłocznego wezwania Przetwarzającego do przystąpienia do ewentualnego procesu związanego z żądaniem odszkodowania za poniesioną przez osobę fizyczną szkodę majątkową lub niemajątkową związaną z Przetwarzaniem Danych naruszającym przepisy prawa i prowadzenia procesu z udziałem Przetwarzającego jako interwenienta ubocznego albo w innym charakterze stosownie do obowiązujących przepisów procedury cywilnej.

10.7. W każdym przypadku naruszenia przez Przetwarzającego zasad ochrony Danych lub obowiązku zachowania w tajemnicy treści Danych oraz wszelkich innych Informacji Poufnych, w szczególności niewykonania lub nienależytego wykonania Umowy, Powierzającemu przysługuje prawo dochodzenia zapłaty kary umownej w wysokości 10.000,00 złotych (słownie: dziesięć tysięcy 00/100) za każdy przypadek naruszenia, płatnej na podstawie noty obciążeniowej w terminie w niej wskazanym. Żądanie zapłaty kary umownej przysługuje niezależnie od obowiązku naprawienia szkody, o których mowa w ust. 10.2 - 10.6 i prawa do odszkodowania uzupełniającego, o którym mowa w ust. 10.11.

10.8. Przez nienależyte wykonanie Umowy Strony rozumieją w szczególności sytuację, gdy organ nadzorczy stwierdzi, że Przetwarzanie Danych w zakresie realizowanym przez Przetwarzającego nie jest zgodne z zasadami ochrony danych osobowych.

10.9. W razie rozwiązania Umowy, Powierzający może dochodzić kar umownych należnych do dnia jej rozwiązania, a w przypadku naruszenia obowiązku, o którym mowa w §12 ust. 12.2 Umowy, również kary umownej z tytułu naruszenia tego obowiązku.

10.10. W przypadku zawarcia przez Przetwarzającego umowy podpowierzenia z innym podmiotem przetwarzającym pomimo braku zgody Powierzającego, Powierzającemu przysługuje prawo dochodzenia zapłaty kary umownej w wysokości 10.000,00 złotych (słownie: dziesięć tysięcy 00/100), płatnej na podstawie noty obciążeniowej w terminie w niej wskazanym.

10.11. Powierzający jest uprawniony do żądania zapłaty przez Przetwarzającego odszkodowania uzupełniającego na zasadach ogólnych, przenoszącego wartość zastrzeżonych kar umownych.

10.12. Przetwarzający jest odpowiedzialny za naruszenie przepisów prawa podczas Przetwarzania Danych, ponosząc odpowiedzialność przed organem nadzorczym w postaci kar administracyjnych.

§11 OBOWIĄZYWANIE UMOWY

11.1. Umowa zostaje zawarta na czas wykonania zobowiązań wynikających z Umowy Głównej oraz obowiązków wynikających z Umowy.

11.2. Powierzający jest uprawniony do rozwiązania Umowy ze skutkiem natychmiastowym, jeżeli:

1) Przetwarzający nie stosuje odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z Przetwarzaniem powierzonych Danych,

2) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli, Przetwarzający nie usunie ich w wyznaczonym terminie,

3) Przetwarzający Przetwarza Dane w sposób niezgodny z Umową,

4) Przetwarzający Przetwarza Dane w sposób niezgodny z przepisami RODO lub innymi właściwymi przepisami prawa, bądź instrukcjami Powierzającego,

5) Przetwarzający powierzył Przetwarzanie Danych dalszemu podmiotowi przetwarzającemu bez zgody Powierzającego,

6) Przetwarzający utracił zdolność do realizacji Umowy, w szczególności utracił zdolność do zagwarantowania należytego zabezpieczenia powierzonych danych osobowych.

11.3. Niezależnie od przypadków wskazanych w ust. 11.2, Powierzający może rozwiązać Umowę bez wypowiedzenia z innych ważnych powodów, w szczególności gdy Powierzający będzie miał uzasadnione podstawy do stwierdzenia, że dalsze przetwarzanie danych przez Przetwarzającego lub inną osobę działającą w jego imieniu ma negatywny wpływ na ochronę danych osobowych.

11.4. W przypadku ograniczenia zakresu powierzenia przetwarzania przez Powierzającego, postanowienia o rozwiązaniu Umowy stosuje się odpowiednio do danych osobowych, które wskutek ograniczenia zakresu nie mogą już być przetwarzane przez Przetwarzającego.

11.5. W przypadku zawarcia przez Powierzającego umowy podpowierzenia przetwarzania danych osobowych Przetwarzający zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi postanowień, zgodnie z którymi umowy dalszego przetwarzania danych będą ulegały automatycznemu rozwiązaniu w razie zakończenia obowiązywania Umowy.

§12 USUNIĘCIE LUB ZWROT DANYCH

12.1. Stosownie do decyzji Powierzającego w tym zakresie, w terminie do [30] dni od dnia rozwiązania Umowy, niezależnie od sposobu i trybu jej rozwiązania, lub od dnia zakończenia Przetwarzania Danych (w zależności od tego, co nastąpiło wcześniej), Przetwarzający jest zobowiązany do usunięcia lub zwrotu Informacji Poufnych, w tym wszelkich powierzonych mu Danych oraz usunięcia wszelkich ich istniejących kopii zapisanych w jakimkolwiek urządzeniu lub na jakimkolwiek innym nośniku na którym są zapisane lub przechowywane, chyba że obowiązujące przepisy prawa nakazują przechowywanie tych Informacji Poufnych.

12.2. Przetwarzający zobowiązany jest przesłać Powierzającemu pisemne potwierdzenie zwrotu lub zniszczenia wszelkich Informacji Poufnych, w tym Danych w sposób i w terminie uzgodnionym z Powierzającym, nie dłuższym niż [7] dni.

12.3. W przypadku gdy Przetwarzanie Danych przez Przetwarzającego odbywało się wyłącznie w systemach informatycznych Powierzającego, Przetwarzający złoży po rozwiązaniu Umowy, niezależnie od sposobu i trybu jej rozwiązania (w zależności od tego, co nastąpiło wcześniej), pisemne oświadczenie o nieprzechowywaniu powierzonych na podstawie Umowy Danych.

§13 POSTANOWIENIA KOŃCOWE

13.1. Zmiana Umowy wymaga zachowania formy pisemnej pod rygorem nieważności, z zastrzeżeniem odmiennie brzmiących postanowień Umowy.

13.2. W sprawach nieuregulowanych Umową mają zastosowanie przepisy prawa polskiego, w tym przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2019 r. poz. 1145), ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2019 r., poz. 1010) oraz przepisy RODO.

13.3. Przetwarzający nie może przenieść praw lub obowiązków wynikających z Umowy bez pisemnej zgody Powierzającego.

13.4. Osobami upoważnionymi do kontaktu w sprawach związanych z realizacją Umowy, w tym do przekazywania informacji o stwierdzonych naruszeniach ochrony Danych (§ 6 ust 3 Umowy), są:

1) ze strony Powierzającego – Inspektor Ochrony Danych:

iv) e-mail: iod@ciuwo.olsztyn.eu

v) tel: 89 752 58 09

2) ze strony Przetwarzającego – ……:

i) e-mail: ……

ii) tel: ……

13.5. Spory związane z wykonywaniem Umowy rozstrzygane będą przez sąd właściwy dla siedziby Powierzającego.

13.6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Powierzającego i jeden dla Przetwarzającego.

§14 ZAŁĄCZNIKI:

14.1. Załącznik nr 1 – zakres powierzenia Danych.

14.2. Załącznik nr 2 – wzór oświadczenia.

POWIERZAJĄCY	**PRZETWARZAJĄCY**
.....	.....

Załącznik nr 1 umowy powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji

ZAKRES POWIERZENIA DANYCH

Zbiór pod nazwą ___

(Jeżeli dane przetwarzane w systemie, dodać nazwę systemu)

Charakter oraz cele przetwarzania:	
Operacje wykonywane na danych osobowych:	
Kategorie osób, których dane dotyczą:	
Rodzaj danych osobowych:	
Obszar, na którym przetwarzane będą dane osobowe:	

Załącznik nr 2 umowy powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji

/WZÓR/

OŚWIADCZENIE

……, dnia …… r.

Niniejszym oświadczam, że znana mi jest treść Umowy przetwarzania danych osobowych oraz o zachowaniu poufności informacji, zawarta pomiędzy Centrum Informatycznych Usług Wspólnych Olsztyna oraz Gminą Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1; 10-101 Olsztyn a:

Nazwa Wykonawcy

z siedzibą w

Siedziba Wykonawcy

adres:

Adres Wykonawcy

data

Data zawarcia umowy powierzenia przetwarzania danych

oraz wynikające z niej zobowiązania do utrzymywania w tajemnicy ujawnionych Informacji Poufnych.

Niniejszym zobowiązuję się jako pracownik/ współpracownik/ zleceniobiorca/ podwykonawca* ww. Wykonawcy do zachowania w tajemnicy wszelkich Informacji Poufnych, które zostały mi ujawnione w związku z moim uczestnictwem w realizacji prac na rzecz Centrum Informatycznych Usług Wspólnych Olsztyna, na warunkach określonych w umowie przetwarzania danych osobowych oraz o zachowaniu poufności. Jestem świadomy, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

Imię i nazwisko oświadczającego

podpis

* niepotrzebne skreślić