

**WARUNKI  
ZAMÓWIENIA  
(WZ)**

**oznaczenie sprawy: 1400/DW00/ZT/KZ/2024/0000101045**



**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage  
Engine**

**Zatwierdzam**

podpis Kierownika Zamawiającego  
(osoby upoważnionej)

Poznań, dnia 21 listopada 2024 r.

## SPIS TREŚCI

<b>Rozdział I – INFORMACJA DLA WYKONAWCÓW .....</b>	<b>3</b>
<b>1. Informacje wstępne.....</b>	<b>3</b>
<b>3. Tryb udzielenia zamówienia.....</b>	<b>4</b>
<b>4. Przedmiot zamówienia .....</b>	<b>5</b>
<b>5. Termin realizacji zamówienia.....</b>	<b>5</b>
<b>6. Warunki udziału w postępowaniu oraz brak podstaw wykluczenia udziału w postępowaniu.....</b>	<b>5</b>
<b>7. Wymagane dokumenty i oświadczenia .....</b>	<b>7</b>
<b>8. Wadium.....</b>	<b>9</b>
<b>9. Sposób przygotowania oferty .....</b>	<b>9</b>
<b>10. Oferty wspólne .....</b>	<b>10</b>
<b>11. Sposób obliczenia ceny oferty .....</b>	<b>10</b>
<b>12. Miejsce i termin składania ofert .....</b>	<b>10</b>
<b>13. Termin związania ofertą .....</b>	<b>11</b>
<b>14. Kryteria oceny ofert .....</b>	<b>11</b>
<b>15. Otwarcie ofert i przebieg postępowania .....</b>	<b>11</b>
<b>16. Odrzucenie oferty.....</b>	<b>13</b>
<b>17. Unieważnienie postępowania .....</b>	<b>13</b>
<b>18. Zabezpieczenie należytego wykonania umowy .....</b>	<b>14</b>
<b>19. Zawarcie Umowy.....</b>	<b>14</b>
<b>ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA.....</b>	<b>15</b>
<b>ROZDZIAŁ III – WYKAZ ZAŁĄCZNIKÓW .....</b>	<b>15</b>

**ROZDZIAŁ I – INFORMACJA DLA WYKONAWCÓW****1. INFORMACJE WSTĘPNE**

- 1.1. Zamawiającym w niniejszym postępowaniu jest:

**ENEA Centrum sp. z o.o.**

**Pl. Władysława Andersa 7, 61-894 Poznań, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000477231, NIP: 777-000-28-43; numer statystyczny (REGON): 630770227, kapitał zakładowy: 103.929.000,00 PLN**

- 1.2. Numer postępowania: Postępowanie, którego dotyczy niniejszy dokument oznaczone jest znakiem:

**1400/DW00/ZT/KZ/2024/0000101045**

Wykonawcy we wszystkich kontaktach z Zamawiającym powinni powoływać się na ten znak.

- 1.3. Wszelkie informacje dotyczące postępowania Zamawiający udostępnia na swojej stronie internetowej [www.enea.pl/bip/zamowienia](http://www.enea.pl/bip/zamowienia), która jest główną stroną prowadzonego postępowania. Zamawiający informuje, iż Platforma Zakupowa Logintrade.NET dostępna na stronie internetowej GK ENEA pod adresem <https://www.enea.pl/bip/zamowienia/zamowienia-logintrade> służy wyłącznie do składania ofert i zadawania pytań do treści Warunków Zamówienia.
- 1.4. Postępowanie prowadzone jest w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie Wykonawców. Czynności związane z przygotowaniem i przeprowadzeniem niniejszego postępowania wykonują osoby zapewniające bezstronność i obiektywizm
- 1.5. Postępowanie jest prowadzone w języku polskim w związku z tym wszelkie oświadczenia, zawiadomienia, zapytania do treści WZ, oferty itp. muszą być składane w języku polskim. Zawarte w ofercie dokumenty i oświadczenia sporządzone w języku obcym, muszą być złożone wraz z **tłumaczeniami na język polski**. Zamawiający dopuszcza możliwość przedstawienia tłumaczenia zwykłego. W przypadku wątpliwości Zamawiający może zażądać uzupełnienia oferty o tłumaczenie sporządzone przez tłumacza przysięgłego.
- 1.6. W postępowaniu obowiązuje zasada pisemności.
- 1.7. Zamawiający informuje, że postępowanie, w tym otwarcie ofert jest niejawne i nie zamierza zwoływać zebrania Wykonawców.
- 1.8. **W niniejszym postępowaniu Wykonawcom nie przysługują środki odwoławcze.**
- 1.9. Wykonawca ponosi wszelkie koszty związane z uczestnictwem w niniejszym postępowaniu, w tym także z przygotowaniem i złożeniem oferty.
- 1.10. Żadne materiały dotyczące postępowania, dostarczone przez Wykonawców, nie podlegają zwrotowi.

**2. KOMUNIKACJA, KORESPONDENCJA I DOKUMENTACJA POSTĘPOWANIA**

- 2.1. **Składanie ofert następuje poprzez Platformę Zakupową Logintrade**, dostępną na stronie internetowej GK ENEA pod adresem <https://www.enea.pl/bip/zamowienia/zamowienia-logintrade>, z zastrzeżeniem **pkt 9.4. lit. c) WZ**. Wszelka komunikacja z Zamawiającym odbywa się wyłącznie za pośrednictwem poczty e-mail osób uprawnionych do bezpośredniego kontaktowania się z Wykonawcami wskazanymi w pkt 2.12 (konieczne jest wysłanie na oba adresy e-mail). **W przypadku pytań Wykonawców do treści WZ**, dopuszcza się możliwość ich składania poprzez Platformę Zakupową Logintrade dostępną na stronie internetowej GK ENEA pod adresem <https://www.enea.pl/bip/zamowienia/zamowienia-logintrade>.
- 2.2. **Formularz oferty (Załącznik nr 1 do WZ) i pełnomocnictwa należy podpisać** w sposób umożliwiający identyfikację osoby podpisującej tj. :
- podpisem własnoręcznym,
  - podpisem epuap,
  - elektronicznym podpisem kwalifikowanym,
  - elektronicznym podpisem niekwalifikowanym,
- w formie nieedytowalnej np. plik PDF, skan, zdjęcie dokumentu.

- 2.3. **Pozostałe dokumenty i oświadczenia składane są w formie wskazanej w pkt. 2.2. Dopuszcza się podpisanie pozostałych dokumentów i oświadczeń również poprzez wskazanie imienia i nazwiska.**
- 2.4. Dokumenty składane przez Wykonawcę uważa się za złożone skutecznie, jeżeli zostały zarejestrowane **w wymaganej formie** przed upływem określonego przez Zamawiającego terminu na:
- a) Platformie Zakupowej Logintrade – dotyczy ofert składanych zgodnie z pkt 12.1 WZ;
  - b) serwerze poczty e-mail osób uprawnionych do bezpośredniego kontaktowania się z Wykonawcami – w pozostałym zakresie.
- 2.5. Zamawiający wymaga złożenia oferty Wykonawcy w postaci dokumentu elektronicznego (dopuszczalne jest skompresowanie do formatu **zip**). Maksymalny rozmiar pojedynczego pliku przesyłanego do platformy zakupowej to **20 MB**. W przypadku dokumentu podpisanego profilem zaufany rozmiar pliku **nie może** przekroczyć 10 MB.
- 2.6. Wszelkie dokumenty, w tym oferta powinny być podpisane przez osoby upoważnione do reprezentacji Wykonawcy. **Jeżeli umocowanie do reprezentowania Wykonawcy nie wynika z odpisu z właściwego rejestru - należy wykazać dokumentami ciąg umocowania do reprezentacji.**
- 2.7. Zamawiający żąda niezwłocznego potwierdzenia faktu otrzymania dokumentów, informacji, zawiadomień przekazanych za pomocą poczty elektronicznej (w przypadku prowadzenia Postępowań na platformie zakupowej potwierdzenia dostarczenia wiadomości na serwer odbiorcy).
- 2.8. **Zamawiający zastrzega sobie prawo do modyfikacji Warunków Zamówienia** do upływu terminu składania ofert. Zmiana może dotyczyć m.in. kryteriów oceny ofert, a także warunków udziału w postępowaniu oraz sposobu oceny ich spełnienia.
- 2.9. Zamawiający może przedłużyć termin składania ofert – z uwzględnieniem czasu niezbędnego do wprowadzenia w ofertach zmian wynikających z modyfikacji treści WZ. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie dokumentacji postępowania.
- 2.10. **Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie dokumentacji postępowania, a także o wyjaśnienie / modyfikację treści Projektu umowy.** Zamawiający zobowiązany jest udzielić wyjaśnień treści dokumentacji postępowania nie później niż na 1 dzień roboczy przed upływem terminu składania ofert – pod warunkiem, że wniosek o wyjaśnienie treści dokumentacji postępowania wpłynął do Zamawiającego nie później, niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
- 2.11. Treść zapytań bez ujawniania źródła zapytania wraz z wyjaśnieniami Zamawiający udostępni na stronie internetowej.
- 2.12. Osobami uprawnionymi do bezpośredniego kontaktowania się z Wykonawcami są:

**Pani Natalia Burzmińska**

ENEA Centrum Sp. z o.o., Departament Zakupów

Plac Władysława Andersa 7, 61-894 Poznań

e-mail: [natalia.burzminska@enea.pl](mailto:natalia.burzminska@enea.pl)

**Pan Karol Olejnik**

ENEA Centrum Sp. z o.o. Departament Zakupów

Plac Władysława Andersa 7, 61-894 Poznań

e-mail: [karol.olejnik@enea.pl](mailto:karol.olejnik@enea.pl)

### **3. TRYB UDZIELENIA ZAMÓWIENIA**

- 3.1. Postępowanie o udzielenie zamówienia prowadzone jest zgodnie z wewnętrznymi regulacjami obowiązującymi u Zamawiającego oraz w oparciu o niniejsze Warunki Zamówienia.
- 3.2. **Do postępowania nie znajdują zastosowania przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.**

- 3.3. Zamawiający informuje, iż w prowadzonym postępowaniu, Zamawiający najpierw dokona badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej Wykonawcy, którego oferta została najwyżej oceniona, w zakresie braku podstaw wykluczenia oraz spełnienia warunków udziału w postępowaniu.

#### 4. PRZEDMIOT ZAMÓWIENIA

- 4.1. Przedmiotem zamówienia jest:

##### **Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine**

Szczegółowy Opis Przedmiotu Zamówienia zawarty jest w Rozdziale II Warunków Zamówienia „Opis Przedmiotu Zamówienia”.

- 4.2. Wykonawca może złożyć tylko jedną ofertę. Alternatywy zawarte w treści oferty spowodują jej odrzucenie.
- 4.3. Nie dopuszcza się składania ofert częściowych ani wariantowych. Złożona oferta musi dokładnie odpowiadać Szczegółowemu Opisowi Przedmiotu Zamówienia zawartemu w Rozdziale II Warunków Zamówienia, zostać przedstawiona zgodnie z formularzem ofertowym stanowiącym **Załącznik nr 1 do Warunków Zamówienia** i obejmować swoim zakresem całość zamówienia.
- 4.4. Zamawiający nie dopuszcza możliwość wykonania zamówienia z udziałem podwykonawców.
- 4.5. Zamawiający w wyniku postępowania zamierza zawrzeć Umowę z jednym Wykonawcą.

#### 5. TERMIN REALIZACJI ZAMÓWIENIA

- 5.1. Umowa zostanie zawarta na okres: zgodnie z par. 2 ust 1-3 Projektu Umowy stanowiącego załącznik nr 9 do Warunków Zamówienia.

#### 6. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW WYKLUCZENIA UDZIAŁU W POSTĘPOWANIU

- 6.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełnią warunki dotyczące:

- 6.1.1. zdolności technicznej lub zawodowej;

Warunek ten zostanie uznany za spełniony, jeżeli Wykonawca wykaże, że:

- a) w okresie ostatnich 3 lat przed upływem terminu składania Ofert zrealizował (zakończył) oraz w trakcie realizacji (trwające) co najmniej 2 (dwie) usługi, których przedmiotem była usługa wsparcia serwisowego wraz z wdrożeniem dla systemu Service Desk Plus Manage Engine, o wartości co najmniej 100 000,00 zł netto każda.

**UWAGA!** Jeżeli Wykonawca w terminie składania oferty wykonuje zamówienie, wskazany warunek uznaje się za spełniony, jeżeli do upływu terminu składania ofert Wykonawca wykonał zamówienia o wartości nie mniejszej niż określona powyżej.

Wykazane przez Wykonawcę usługi muszą zostać potwierdzone dokumentami poświadczającymi należyte wykonanie usług (takimi jak: referencje, oświadczenie Klienta Wykonawcy, z tym zastrzeżeniem, że Zamawiający nie dopuszcza przedstawienia referencji własnych przez Wykonawcę oraz faktur); dokumenty potwierdzające należyte wykonanie usług powinny być sporządzone i oznaczone w taki sposób, aby nie było wątpliwości, których usług wykazanych przez Wykonawcę dotyczą.

W przypadku przedstawienia usług nadal realizowanych, dowód potwierdzający należyte wykonywanie usług musi być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

**UWAGA!** W przypadku dostaw realizowanych na rzecz Zamawiającego (ENEA Centrum Sp. z o.o.), zamiast dokumentu potwierdzającego należyte wykonanie dostawy, Zamawiający dopuszcza wskazanie nr umowy oraz Koordynatora Umowy ze Strony Zamawiającego.

- b) posiada status Partnera producenta oprogramowania

- 6.2. Wykonawca podlega wykluczeniu z udziału w postępowaniu jeżeli:

- a) w ciągu ostatnich 3 lat przed upływem terminu składania ofert uniemożliwił lub odmówił zawarcia Umowy w sprawie Zamówienia po wyborze jego oferty przez Zamawiającego lub nie wniósł wymaganego

- zabezpieczenia należytego wykonania Umowy;
- b) w ciągu ostatnich 3 lat przed upływem terminu składania ofert, nie wykonał przedmiotu Zamówienia na rzecz Zamawiającego lub wykonał go nienależycie, a w ramach działań naprawczych nie doprowadził przedmiotu Zamówienia stanu zgodności z Umową lub nie naprawił powstałej w ten sposób szkody, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które Wykonawca nie ponosi odpowiedzialności;
  - c) w ciągu ostatnich 3 lat przed upływem terminu składania ofert doprowadził do wypowiedzenia albo odstąpienia od Umowy w sprawie Zamówienia wykonywanego na rzecz Zamawiającego z przyczyn leżących po stronie Wykonawcy;
  - d) w ciągu ostatnich 3 lat przed upływem terminu składania ofert dopuścił się poważnych naruszeń Kodeksu Kontrahentów Grupy ENEA albo dopuścił się innych naruszeń postanowień Kodeksu Kontrahentów Grupy ENEA a w ramach działań naprawczych nie doprowadził do ich usunięcia;
  - e) w ciągu ostatnich 3 lat przed upływem terminu składania ofert w sposób inny niż wskazany w lit. a) – d) wyrządził Zamawiającemu szkodę w związku z realizacją Zamówienia, której to szkody nie naprawił w ramach podjętych działań naprawczych;
  - f) został wpisany do Rejestru Wykonawców Wykluczonych zgodnie z „Zasadami dokonywania oceny Wykonawców w Obszarze Zakupowym Zakupy Ogólne w Grupie ENEA”;
  - g) otwarto jego likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
  - h) doradzał lub w inny sposób był zaangażowany w przygotowanie Postępowania o udzielenie tego Zamówienia, a spowodowane tym zaangażowaniem zakłócenie konkurencji nie może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w tym Postępowaniu. Przed wykluczeniem Wykonawcy Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego zaangażowanie w przygotowanie Postępowania o udzielenie Zamówienia nie zakłóci konkurencji;
  - i) Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, , chyba że wykażą, przygotowali te oferty niezależnie od siebie;
  - j) naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne chyba że Wykonawca przed upływem terminu składania Ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
  - k) złożył nieprawdziwe informacje mające lub mogące mieć wpływ na wynik Postępowania;
  - l) nie wykazał spełnienia warunków udziału w Postępowaniu;
  - m) został wpisany na listy sankcyjne<sup>1</sup>;
  - n) jego beneficjentem rzeczywistym<sup>2</sup> :

---

#### <sup>1</sup> Listy Sankcyjne

- I. wykazy osób lub podmiotów określone w:
  - rozporządzeniu Rady (WE) 765/2006 z dnia 18 maja 2006 r. dotyczącym środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy,
  - rozporządzeniu Rady (UE) 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających oraz
- II. lista osób lub podmiotów określona w ustawie z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego; prowadzona przez ministra właściwego do spraw wewnętrznych, publikowana w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw wewnętrznych, wobec których stosuje się sankcję wykluczenia z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych.

<sup>2</sup> w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,

- i. jest osoba wpisana na Listy Sankcyjne lub
  - ii. była od dnia 24 lutego 2022 r. osoba wpisana na Listy Sankcyjne
- o) jego jednostką dominującą<sup>3</sup>:
  - i. jest osoba wpisana na Listy Sankcyjne lub
  - ii. była od dnia 24 lutego 2022 r. osoba wpisana na Listy Sankcyjne
- 6.3. Zamawiający informuje, iż Wykonawca podlegający wykluczeniu z postępowania o udzielenie zamówienia na podstawie ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, który w okresie tego wykluczenia ubiega się o udzielenie zamówienia, podlega karze pieniężnej na warunkach określonych w tej ustawie.
- 6.4. W celu potwierdzenia, iż Wykonawca spełnia warunki udziału w postępowaniu oraz nie podlega wykluczeniu z postępowania, **Zamawiający żąda złożenia wraz z ofertą Załącznika nr 2 do WZ – tj. Oświadczenia o niepodleganiu wykluczeniu z postępowania oraz spełnianiu warunków udziału w postępowaniu.** Dokument ten tymczasowo zastępuje dokumenty potwierdzające spełnienie warunków udziału w postępowaniu oraz dokumenty potwierdzające brak podstaw wykluczenia Wykonawcy z postępowania, do złożenia których Zamawiający wezwie Wykonawcę, którego oferta została najwyżej oceniona. Zamawiający zastrzega możliwość wezwania do złożenia dokumentów wymienionych w pkt. 7.2 – 7.3. WZ również pozostałych Wykonawców, których oferty są w rankingu ofert.
- 6.5. Zamawiający może na każdym etapie postępowania, wezwać Wykonawców do złożenia wszystkich lub niektórych dokumentów potwierdzających brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu, aktualnych na dzień ich złożenia, jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie Zamówienia.
- 6.6. Wykonawca musi wykazać spełnianie warunków udziału w postępowaniu nie później niż na dzień składania ofert.
- 6.7. Zamawiający dokona oceny spełniania warunków udziału w postępowaniu wskazanych w pkt 6.1 WZ oraz braku podstaw wykluczenia wskazanych w pkt 6.2. WZ, na zasadzie „spełnia – nie spełnia”, w oparciu o:
  - a) informacje zawarte w Oświadczeniu, o którym mowa w pkt 6.4 WZ oraz
  - b) dokumenty i oświadczenia złożone przez Wykonawcę, którego oferta zostanie najwyżej oceniona, o których mowa w pkt 7.2-7.3 WZ.
- 6.8. Oferta Wykonawcy, który został wykluczony z postępowania podlega odrzuceniu.
- 6.9. Wykonawcę wykluczonego z postępowania Zamawiający niezwłocznie poinformuje o wykluczeniu wraz z podaniem uzasadnienia.
- 6.10. **Zamawiający nie dopuszcza posługiwania się zasobami podmiotów trzecich w celu wykazania spełniania warunków udziału w postępowaniu.**

## **7. WYMAGANE DOKUMENTY I OŚWIADCZENIA**

- 7.1. Wykonawca zobowiązany jest do złożenia oferty, na którą składają się następujące dokumenty:
  - a) formularz oferty obejmujący oświadczenie o zaakceptowaniu Warunków Zamówienia (**Załącznik nr 1 do Warunków Zamówienia**),
  - b) klauzula informacyjna Wykonawcy dotycząca przetwarzania danych osobowych reprezentantów i pracowników Zamawiającego, o której mowa w pkt. 3 lit. I) Formularza Oferty, **(Uwaga nie należy utożsamiać z załącznikiem nr 5 do Warunków Zamówienia)**
  - c) oświadczenie wstępne Wykonawcy o niepodleganiu wykluczeniu z postępowania oraz spełnianiu warunków udziału w Postępowaniu (**Załącznik nr 2 do Warunków Zamówienia**),
  - d) podpisane upoważnienie do podpisania oferty i załączników do niej, o ile nie wynika ono z innych dokumentów załączonych przez Wykonawcę (Zamawiający udostępnia wzór, który Wykonawca może wykorzystać – **Załącznik nr 3 do Warunków Zamówienia**),
  - e) oświadczenie Wykonawcy o zachowaniu poufności (**Załącznik nr 4 do Warunków Zamówienia**),

---

<sup>3</sup> w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości.

- f) informacja o Administratorze Danych Osobowych (**Załącznik nr 5 do Warunków Zamówienia**),
- g) oświadczenie o spełnieniu minimalnych wymagań w zakresie stosowanych zabezpieczeń technicznych i organizacyjnych dotyczących ochrony danych osobowych osób fizycznych (załącznik nr 8 do Warunków Zamówienia)
- 7.2. W celu potwierdzenia spełniania warunków udziału w postępowaniu, określonych w **pkt 6.1. WZ**, Zamawiający żąda przedstawienia następujących oświadczeń i dokumentów aktualnych na dzień ich złożenia:
- a) wykazu usług (**Załącznik nr 6 do Warunków Zamówienia**), wraz z dokumentami potwierdzającymi ich należyte wykonanie/wykonywanie takimi jak: referencje, oświadczenie Klienta Wykonawcy, z tym zastrzeżeniem, że Zamawiający nie dopuszcza przedstawienia referencji własnych przez Wykonawcę; dokumenty potwierdzające należyte wykonanie dostaw powinny być sporządzone i oznaczone w taki sposób, aby nie było wątpliwości, których dostaw wykazanych przez Wykonawcę dotyczą
- b) dokument/certyfikat/zaświadczenie potwierdzające, że Wykonawca posiada aktualny status Partnera producenta oprogramowania, z zastrzeżeniem, że dokument powinien być wystawiony przez podmiot niepowiązany kapitałowo czy osobowo z Wykonawcą
- UWAGA w przypadku gdy Wykonawca składa dokument w języku obcym, zgodnie z pkt 1.5. WZ zobowiązany jest złożyć tłumaczenie na język polski.**
- 7.3. W celu potwierdzenia braku podstaw wykluczenia z udziału w postępowaniu, określonych w **pkt 6.2. WZ**, Zamawiający żąda przedstawienia następujących oświadczeń i dokumentów aktualnych na dzień ich złożenia:
- a) oświadczenie Wykonawcy o uczestnictwie w grupie kapitałowej (**Załącznik nr 7 do Warunków Zamówienia**),
- b) odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie **pkt 6.2. lit. g WZ**, sporządzonych nie wcześniej niż 3 miesiące przed upływem terminu składania Ofert, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji
- w przypadku zaświadczenia o wpisie do Centralnej Ewidencji i Informacji o Działalności Gospodarczej - Zamawiający dopuszcza przedstawienie wydruku ze strony internetowej Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej ([www.firma.gov.pl](http://www.firma.gov.pl));
  - w przypadku odpisu z Krajowego Rejestru Sądowego, Zamawiający dopuszcza przedstawienie wydruku pobranego ze strony internetowej Ministerstwa Sprawiedliwości (<https://ems.ms.gov.pl/krs/wyszukiwaniepodmiotu>),
- 7.4. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej zamiast odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w **pkt 7.3. lit. b)** – składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury, dokument powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania Ofert;
- 7.5. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w **pkt 7.4. WZ** lub gdy dokumenty te nie odnoszą się do wymienionego tam zakresu, zastępuje się je w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy.
- 7.6. **Wykonawca nie jest zobowiązany do złożenia Podmiotowych środków dowodowych, o których mowa w pkt 7.2 lub 7.3 WZ, które Zamawiający posiada (np. zostały one złożone w innym, wcześniej prowadzonym postępowaniu lub zawierają informacje, które dotyczą zamówień wcześniej realizowanych na rzecz tego**



Zamawiającego lub zostały dostarczone z ofertą), jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

## 8. WADIUM

8.1. W niniejszym postępowaniu wadium nie jest wymagane.

## 9. SPOSÓB PRZYGOTOWANIA OFERTY

9.1. **Wraz z ofertą Wykonawca składa dokumenty określone w pkt 7.1.-7.4. WZ.** Zamawiający wymaga złożenia dokumentów zgodnie z załączonymi wzorami dokumentów jeśli takie udostępniono (z wyjątkiem upoważnienia do podpisania oferty i załączników tj. **Załącznika nr 3 do Warunków Zamówienia**).

9.2. **Dokumenty i oświadczenia, o których mowa w pkt 7.1.-7.4. WZ należy złożyć zgodnie z postanowieniami pkt. 2.1-2.6 WZ.**

9.3. Oferta oraz wszelkie oświadczenia i zaświadczenia składane w trakcie postępowania są jawne w ramach przedsiębiorstwa Zamawiającego; nie są natomiast dostępne publicznie, chyba że obowiązek taki wynika z przepisów prawa powszechnie obowiązującego.

9.4. **Wykonawca może wprowadzić zmiany oraz wycofać złożoną przez siebie ofertę przed terminem składania ofert:**

- a) w przypadku **wycofania oferty**, Wykonawca składa oświadczenie o wycofaniu swojej oferty (zgodnie z formą określoną w **pkt. 2.2 WZ**) oraz przesyła je na adresy email osób uprawnionych do bezpośredniego kontaktowania się z Wykonawcami;
- b) w przypadku **zmiany oferty** złożonej za pośrednictwem platformy zakupowej należy:
  - i. zalogować się na Platformę Zakupową <https://grupaenea.logintrade.net> ;
  - ii. wejść w zakładkę „Twoje aukcje i zapytania”, a następnie wybrać „Twoje oferty”;
  - iii. następnie należy wejść w szczegóły oferty, która ma zostać zmieniona;
  - iv. na samym dole szczegółów oferty znajduje się przycisk „Aktualizuj ofertę”;
  - v. po kliknięciu w „Aktualizuj ofertę” zostanie uruchomiony „Kreator oferty”, który pozwoli na zmianę wcześniej wysłanej oferty;
  - vi. po wprowadzeniu wszystkich zmian należy kliknąć w „Wyślij ofertę”.

**UWAGA!** Zmiana zostaje dokonana poprzez nadpisanie pierwotnie złożonej przez Wykonawcę Oferty i nie ma możliwości powrotu do oferty sprzed dokonania zmiany.

- c) w przypadku podjęcia decyzji o **ponownym złożeniu oferty** po jej wycofaniu, zgodnie z **lit. a)**, Wykonawca przesyła nową ofertę na adresy wskazane w **pkt. 2.12 WZ**. **UWAGA!** Powyższa sytuacja dotyczy wyłącznie ponownego złożenia oferty po dokonaniu jej wycofania. W przypadku zmiany oferty należy dokonać tego zgodnie z **lit. b)**. **Zamawiający nie dopuszcza zmiany oferty za pośrednictwem poczty elektronicznej.**
- d) Oferta, która zostanie złożona w przypadku opisanym w **lit. c)**:
  - i. musi zostać zaszyfrowana, tzn. opatrzona hasłem dostępowym uniemożliwiającym otwarcie plików bez jego posiadania. W tym celu wykonawca może posłużyć się narzędziami oferowanymi przez oprogramowanie, w którym przygotowuje dokument.
  - ii. Hasło dostępu do pliku (plików) ze złożoną ofertą, Wykonawca przesyła Zamawiającemu na adresy *email osób* uprawnionych do bezpośredniego kontaktowania się z Wykonawcami (konieczne jest wysłanie korespondencji na oba wymienione wyżej adresy) **PO TERMINIE SKŁADANIA OFERT, JEDNAK NIE PÓŹNIEJ NIŻ W CIĄGU 2 GODZIN OD UPŁYWU TEGO TERMINU**. Wiadomość, o której mowa w zdaniu poprzednim może zawierać, również inne informacje niezbędne dla prawidłowego dostępu do dokumentu, w szczególności informacje o wykorzystanym programie szyfrującym lub procedurze odszyfrowania danych.

**UWAGA! PRZESŁANIE HASŁA DOSTĘPU W TERMINIE INNYM NIŻ WSKAZANY POWYŻEJ, SPOWODUJE ODRZUCENIE OFERTY JAKO NIEODPOWIADAJĄCEJ WYMAGANIOM OKREŚLONYM W WARUNKACH ZAMÓWIENIA.**

- iii. W treści wiadomości z przesłaną ofertą oraz hasłem do oferty należy wskazać oznaczenie i nazwę postępowania, którego powyższe dotyczą oraz nazwę Wykonawcy albo dowolne oznaczenie pozwalające na prawidłową identyfikację Wykonawcy oraz postępowania.
  - iv. Maksymalny rozmiar wiadomości email to 20 MB. Zamawiający dopuszcza przesłanie oferty w kilku wiadomościach email, co powinno być wyraźnie zaznaczone przez Wykonawcę w treści tych wiadomości.
- 9.5. Wykonawca nie może wprowadzić zmian do oferty, ani wycofać jej po upływie terminu do składania ofert.
- 9.6. Zamawiający informuje, że w przypadku wystąpienia w ofercie informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity Dz.U. z 2022 r., poz. 1233), Zamawiający nie jest upoważniony do ich ujawnienia, jeżeli Wykonawca nie później niż w terminie składania ofert zastrzegł, że nie mogą być one udostępnione oraz wykazał, że stanowią one tajemnicę przedsiębiorstwa. Informacje, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa powinny zostać złożone w osobnym pliku wraz z oznaczeniem „Załącznik stanowiący tajemnicę przedsiębiorstwa”, a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku w formacie zip– zgodnie z pkt 9.4. Warunków Zamówienia lub w przypadku opisanym w pkt. 9.4. lit. c) Warunków Zamówienia – skompresowane do jednego pliku i opatrzone hasłem. Zamawiający nie ponosi odpowiedzialności za ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa, które nie zostały oznaczone i złożone w wymagany sposób. Brak stosownego zastrzeżenia będzie traktowany jako jednoznaczny ze zgodą na ujawnienie całości przekazanych informacji. Zamawiający nie ponosi odpowiedzialności za ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa, które nie zostały oznaczone i złożone w wymagany sposób.
- 9.7. Oferta nie może zawierać poprawek czy elementów charakterystycznych dla trybu śledzenia zmian, tj. komentarzy poprawek, przekreśleń, powtórzeń i innych. Wszelkie niezaakceptowane przez Wykonawcę zmiany nie będą uwzględniane.

## **10. OFERTY WSPÓLNE**

- 10.1. Zamawiający nie dopuszcza składania ofert wspólnych. Nie dotyczy to przedsiębiorców prowadzących działalność gospodarczą zarejestrowaną w CEIDG w formie spółek cywilnych, które w takiej formie składają ofertę. Przedsiębiorcy ci są traktowani przez Zamawiającego jako jeden podmiot. składających ofertę jako spółka cywilna.

## **11. SPOSÓB OBLICZENIA CENY OFERTY**

- 11.1. Cena podana w ofercie powinna obejmować wszystkie koszty związane z realizacją Przedmiotu Zamówienia.
- 11.2. Cena powinna być skonstruowana w sposób podany w formularzu oferty. Podana cena jest obowiązująca w całym okresie ważności oferty i w trakcie realizacji umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia.
- 11.3. Cena oferty musi być podana w złotych polskich, z dokładnością do dwóch miejsc po przecinku.
- 11.4. Rozliczenie między Zamawiającym a Wykonawcą będzie prowadzone w walucie złoty polski.

## **12. MIEJSCE I TERMIN SKŁADANIA OFERT**

- 12.1. Ofertę należy złożyć w postaci elektronicznej, za pośrednictwem środków komunikacji elektronicznej, tj. poprzez elektroniczną platformę zakupową <https://grupaenea.logintrade.net> W przypadku opisanym w **pkt 9.4. lit. c)** WZ, Ofertę należy przesłać na adresy email wskazane w **pkt 2.12.** Warunków Zamówienia.

**Ofertę złożyć należy w terminie do dnia 29.11.2024 r. do godz. 10:00.**

- 12.2. Za termin złożenia Oferty uważa się termin jej zamieszczenia na Platformie Zakupowej.  
Za termin wycofania oferty lub ponownego złożeniu oferty po jej wycofaniu uważa się moment dostarczenia wiadomości zawierającej wycofanie / ponownie składaną ofertę na serwer pocztowy Zamawiającego.
- 12.3. Utrzymywanie dobrej reputacji serwerów pocztowych wykorzystywanych przez Wykonawcę do przysyłania korespondencji elektronicznej z Zamawiającym, leży po stronie usługodawcy poczty elektronicznej / działu IT Wykonawcy. Zamawiający weryfikuje kondycję serwerów pocztowych poprzez portal <https://mxtoolbox.com/emailhealth>.  
Zamawiający informuje, że jeżeli serwer pocztowy Wykonawcy nie zostanie pozytywnie zweryfikowany, korespondencja nie dotrze do Zamawiającego.
- 12.4. **Zamawiający informuje, iż Platforma Zakupowa nie przyjmuje ofert po terminie składania. W przypadku przesłania Ofert za pośrednictwem poczty elektronicznej (przypadek określony w pkt 9.4. lit. c) po terminie składania ofert, oferty zostaną odrzucone na podstawie pkt. 16.1. lit. a).**

### 13. TERMIN ZWIĄZANIA OFERTA

- 13.1. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
- 13.2. Wykonawca pozostaje związany ofertą przez okres **90 dni** od upływu terminu składania ofert.
- 13.3. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z zastrzeżeniem zdania następnego. Zamawiający może jednokrotnie, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na wydłużenie terminu o oznaczony okres.

### 14. KRYTERIA OCENY OFERT

- 14.1. Zamawiający dokona wyboru oferty najkorzystniejszej dla Zamówienia na podstawie poniższego kryterium oceny ofert:

	Kryterium	Waga kryterium
1.	<b>ŁĄCZNA CENA OFERTY NETTO</b>	<b>100%</b>

#### Kryterium 1 – ŁĄCZNA CENA OFERTY NETTO (A)

Liczba punktów, którą można uzyskać w ramach tego kryterium obliczona wg poniższego wzoru:

$$\text{ŁĄCZNA CENA OFERTY NETTO} = \frac{\text{cena netto oferty najtańszej}}{\text{cena netto oferty badanej}} \times 100\% \times 100 \text{ pkt.}$$

- 14.2. Za Ofertę najkorzystniejszą będzie uznana Oferta, która uzyska największą liczbę punktów w ww. kryterium oceny ofert.
- 14.3. Punktacja będzie liczona z dokładnością do dziewiątego miejsca po przecinku.
- 14.4. Jeżeli nie będzie można dokonać wyboru najkorzystniejszej Oferty z uwagi na to, że złożono dwie oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te Oferty do złożenia dodatkowych Ofert cenowych w wyznaczonym terminie. Wykonawcy składając Oferty dodatkowe nie mogą zaoferować cen wyższych niż zaoferowane w złożonych Ofertach.

### 15. OTWARCIE OFERT I PRZEBIEG POSTĘPOWANIA

- 15.1. Po otwarciu ofert Zamawiający dokonuje weryfikacji i oceny ofert złożonych przez Wykonawców, w wyznaczonym terminie wzywa Wykonawców do:
- a) uzupełnienia lub wyjaśnienia, dokumentów, oświadczeń (w tym oświadczenia, o którym mowa w pkt. 6.4 WZ) lub pełnomocnictw wymaganych przez Zamawiającego w dokumentacji postępowania dotyczących spełnienia warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania (chyba, że

- mimo ich uzupełnienia lub wyjaśnienia, oferta Wykonawcy podlega odrzuceniu lub postępowanie podlega unieważnieniu),
- b) wyjaśnienia treści oferty oraz dokumentów dotyczących przedmiotu Zamówienia wpływających na ocenę oferty,
  - c) złożenia dokumentów określonych przez Zamawiającego dotyczących spełnienia warunków udziału w postępowaniu oraz potwierdzenia braku podstaw do wykluczenia z postępowania.
- 15.2. Zamawiający wzywa Wykonawcę, którego Oferta została najwyżej oceniona do złożenia dokumentów określonych przez Zamawiającego dotyczących spełnienia warunków udziału w postępowaniu oraz potwierdzenia braku podstaw do wykluczenia z postępowania w wyznaczonym terminie.
- 15.3. Dokumenty uzupełnione na wezwanie o którym mowa w **pkt 15.1. WZ**, powinny potwierdzać stan faktyczny, aktualny na dzień składania Ofert. Wykonawca, na wezwanie o którym mowa w pkt 15.2 WZ, składa podmiotowe środki dowodowe aktualne na dzień ich złożenia.
- 15.4. Zamawiający poprawia w Ofercie:
- a. oczywiste omyłki pisarskie,
  - b. oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek;
  - c. inne omyłki polegające na niezgodności Oferty z Warunkami Zamówienia, niepowodujące istotnych zmian w treści Oferty.
- 15.5. Zamawiający niezwłocznie informuje Wykonawcę, którego Oferta została poprawiona, o tym fakcie.
- 15.6. Jeżeli cena wskazana w ofercie wydaje się Zamawiającemu **rażąco niska** w stosunku do przedmiotu zamówienia, Zamawiający może zwrócić się do Wykonawcy o udzielenie w określonym terminie wyjaśnień dotyczących elementów oferty mających wpływ na wysokość ceny.
- 15.7. Zamawiający przeprowadzi negocjacje z Wykonawcami, których oferty przed negocjacjami zostały najwyżej ocenione.
- 15.8. Przedmiotem negocjacji będzie cena.
- 15.8.1. W ramach negocjacji, o których mowa w punkcie **15.7**. Zamawiający może przeprowadzić:
- a) aukcję elektroniczną z zastosowaniem kryteriów oceny ofert określonych w **pkt 14.1. Warunków Zamówienia**,
  - b) negocjacje indywidualne (tj. odrębnie z każdym Wykonawcą) w formie telekonferencji zgodnie z terminem złożenia Ofert – począwszy od najwcześniej złożonej, decyduje data zamieszczenia oferty na platformie zakupowej lub wpływu na serwer pocztowy Zamawiającego (wyłącznie w sytuacji opisanej w pkt 9.4. lit c) WZ.
- 15.8.2. Wymagania techniczne platformy, za pośrednictwem której przeprowadzona zostanie aukcja, są następujące:  
<https://grupaenea.logintrade.net/PlatformaZakupowa,wymaganiatechniczne.html>
- 15.8.3. Zamawiający zastrzega, iż przed przeprowadzeniem aukcji elektronicznej poinformuje Wykonawców:
- o danych, które zostaną udostępnione Wykonawcom podczas aukcji elektronicznej,
  - o minimalnym postąpieniu aukcji elektronicznej,
  - o przebiegu procedury aukcji elektronicznej.
- 15.8.4. Zamawiający może po przeprowadzeniu aukcji elektronicznej przeprowadzić dalsze negocjacje w formie określonej w **pkt 15.8.1**, w 4 rundach negocjacyjnych, z **Wykonawcami**, którzy złożyli najwyżej ocenione oferty w toku aukcji elektronicznej.
- 15.8.5. Zamawiający może po przeprowadzeniu negocjacji indywidualnych, przeprowadzić dalsze negocjacje w formie określonej w **pkt 15.8.1**, w 4 rundach negocjacyjnych, z **Wykonawcami**, którzy złożyli najwyżej ocenione oferty w toku negocjacji.
- 15.8.6. Ustalenia zawarte w raporcie (raportach) z aukcji / protokole (protokołach) z negocjacji są wiążące dla Wykonawców.
- 15.9. Zakończenie aukcji / negocjacji nie jest równoznaczne z wyborem oferty Wykonawcy ani z przyjęciem oferty złożonej przez Wykonawcę.
- 15.10. Treść Umowy, której projekt stanowi **Załączniki nr 9 do Warunków Zamówienia obowiązujący w terminie składania ofert**, nie podlega negocjacom. Treść Umowy, której projekt stanowi **Załączniki nr 9 do**

**Warunków Zamówienia** może ulec zmianie po upływie terminu składania ofert jedynie w szczególnie uzasadnionych przypadkach, za które uznaje się wprowadzenie zapisów techniczno-organizacyjnych zapewniających sprawne wykonywanie umów. Powyższe nie dotyczy postanowień Umowy, w których pozostawiono miejsce do uzupełnienia.

**Jednocześnie Zamawiający przypomina o możliwości składania propozycji modyfikacji projektów Warunków Zamówienia, w tym Projektu Umowy, zgodnie z pkt 2.10. Warunków Zamówienia.**

15.11. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.

15.12. Niezwłocznie po rozstrzygnięciu postępowania Zamawiający zawiadamia wszystkich Wykonawców, którzy złożyli oferty, o wyniku postępowania.

## **16. ODRZUCENIE OFERTY**

16.1. Oferta podlega odrzuceniu, w przypadkach gdy:

- a) nie odpowiada wymaganiom określonym w Warunkach Zamówienia,
- b) Wykonawca, pomimo wezwania nie złożył w przewidzianym terminie oświadczenia, o którym mowa w **pkt. 6.4 WZ** lub dokumentów potwierdzających spełnianie warunków udziału w postępowaniu lub brak podstaw wykluczenia z udziału z postępowania lub innych dokumentów lub oświadczeń;
- c) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
- d) zawiera rażąco niską cenę w stosunku do przedmiotu Zamówienia a Wykonawca nie przedstawił w wyznaczonym terminie wyjaśnień potwierdzających, że oferta nie zawiera rażąco niskiej ceny;
- e) została złożona przez Wykonawcę wykluczonego z udziału w postępowaniu lub w trybie innym niż otwarty, została złożona przez Wykonawcę niezaproszonego do składania ofert;
- f) narusza przepisy prawa powszechnie obowiązującego;
- g) jest nieważna na podstawie odrębnych przepisów;
- h) wadium nie zostało wniesione lub zostało wniesione w sposób nieprawidłowy, jeżeli zażądano jego wniesienia;
- i) Wykonawca w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa **pkt 15.4. lit. c WZ**;
- j) Wykonawca nie wyraził pisemnej zgody na przedłużenie terminu związania ofertą po otrzymaniu wniosku Zamawiającego o przedłużenie tego terminu;
- k) Wykonawca nie wyraził pisemnej zgody na wybór jego oferty po upływie terminu związania ofertą.

16.2. Zamawiający niezwłocznie informuje Wykonawcę, którego Oferta została odrzucona w Postępowaniu o udzielenie Zamówienia, o odrzuceniu Oferty wraz z podaniem uzasadnienia.

## **17. UNIEWAŻNIENIE POSTĘPOWANIA**

17.1. Postępowanie unieważnia się, w przypadku gdy:

- a) nie złożono żadnej oferty lub nie złożono żadnej oferty niepodlegającej odrzuceniu;
- b) cena najkorzystniejszej oferty, pomimo przeprowadzenia negocjacji lub aukcji elektronicznej, przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na finansowanie Zamówienia, chyba że Zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty;
- c) Kierownik Zamawiającego nie zatwierdził przedstawionej mu rekomendacji wyboru najkorzystniejszej oferty;
- d) wystąpiły inne istotne okoliczności powodujące, że prowadzenie postępowania lub realizacja Zamówienia nie leży w interesie Zamawiającego;
- e) w trakcie postępowania nastąpiło istotne naruszenie przepisów Regulaminu, które miało wpływ na wynik Postępowania;
- f) Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie Zamówienia lub nie przedłożył dokumentów wymaganych do zawarcia umowy (w tym nie wniósł wymaganego zabezpieczenia należytego wykonania umowy), a Zamawiający nie dokonał wyboru najkorzystniejszej oferty spośród ofert pozostałych w postępowaniu Wykonawców;

- g) wystąpiły inne uzasadnione przyczyny.
- 17.2. O unieważnieniu postępowania o udzielenie Zamówienia Zamawiający zawiadomi wszystkich Wykonawców, którzy złożyli oferty w postępowaniu.
- 17.3. Zamawiający dopuszcza możliwość rozstrzygnięcia postępowania również w przypadku złożenia jednej ważnej oferty.

**18. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY**

- 18.1. Zabezpieczenie należytego wykonania umowy **nie jest wymagane.**

**19. ZAWARCIE UMOWY**

- 19.1. Z Wykonawcą, którego oferta zostanie uznana za najkorzystniejszą, zostanie zawarta Umowa w formie pisemnej, w terminie i w miejscu wskazanym przez Zamawiającego. Strony mogą zawrzeć Umowę po upływie terminu związania ofertą, o ile wyrażą na to zgodę. Projekty Umowy stanowi **Załącznik nr 9 do Warunków Zamówienia.**
- 19.2. Jeżeli okaże się, że Wykonawca, którego oferta została wybrana:
- będzie uchylał się od zawarcia Umowy w sprawie zamówienia
  - przedstawił nieprawdziwe dane
- Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.
- 19.3. Jeżeli w związku z zaistnieniem przesłanek, o których mowa w pkt 19.2. WZ, Zamawiający zamierza zawrzeć Umowę z kolejnym Wykonawcą, stosuje się w tym względzie odpowiednio zapisy o zawarciu Umowy z Wykonawcą, który złożył najkorzystniejszą Ofertę.

**ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA****1. Przedmiotem zamówienia jest:**

- 1.1. świadczenie usług wsparcia technicznego systemu Service Desk Plus Manage Engine Enterprise wdrożonego u Zamawiającego dla 656 techników i 13000 zasobów (wieczysty model licencji), przez okres 12 miesięcy począwszy od dnia 31.12.2024.
- 1.2. świadczenie usług wsparcia technicznego systemu Service Desk Plus Manage Engine Professional wdrożonego u Zamawiającego dla 257 techników (wieczysty model licencji) wraz z modułem katalog usług. przez okres 12 miesięcy począwszy od dnia 31.12.2024.
- 1.3. Subskrypcja licencji ze wsparciem OpManager Professional dla 50 urządzeń, 15 adresów url i 15 techników przez okres 12 miesięcy począwszy od dnia 22.12.2024.
- 1.4. Subskrypcja ze wsparciem Application Manager Plugin dla 50 monitorów wraz z dodatkiem Microsoft SharePoint monitoring przez okres 12 miesięcy począwszy od dnia 22.12.2024.

**2. Opis działania usług wsparcia technicznego.**

- 2.1. Po stronie producenta oprogramowania – ZOHO Corporation B.V. działająca pod marką ManageEngine, z siedzibą w Hoogoorddreef 15, 1101 BA Amsterdam, Holandia (dalej: „Producent”):

- a) nielimitowane wsparcie techniczne drogą mailową przez cały rok w trybie 24x5,
- b) telefoniczne wsparcie techniczne,
- c) darmowy dostęp do podstawowych uaktualnień i poprawek w systemie,
- d) główne aktualizacje takie jak zmiana wersji,
- e) dostęp do dokumentacji on-line.

- 2.2. Po stronie partnera Producenta bez dodatkowych opłat:

- a) nielimitowane wsparcie techniczne drogą mailową i systemem zdalnej pomocy,
- b) dostęp do portalu pomocy technicznej i bazy rozwiązań,
- c) telefoniczne wsparcie.

**ROZDZIAŁ III – WYKAZ ZAŁĄCZNIKÓW**

1. ZAŁĄCZNIK NR 1 - FORMULARZ OFERTY
2. ZAŁĄCZNIK NR 2 - OŚWIADCZENIE WSTĘPNE WYKONAWCY O BRAKU PODSTAW DO WYKLUCZENIA Z UDZIAŁU W POSTĘPOWANIU ORAZ SPEŁNIENIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU
3. ZAŁĄCZNIK NR 3 - UPOWAŻNIENIE UDZIELONE PRZEZ WYKONAWCĘ – WZÓR
4. ZAŁĄCZNIK NR 4- OŚWIADCZENIE WYKONAWCY O ZACHOWANIU POUFNOŚCI.
5. ZAŁĄCZNIK NR 5 - OŚWIADCZENIE WYKONAWCY W ZAKRESIE WYPEŁNIANIA OBOWIĄZKÓW INFORMACYJNYCH PRZEWIDZIANYCH W ART. 13 LUB ART. 14 RODO
6. ZAŁĄCZNIK NR 6 – WYKAZ USŁUG PODOBNYCH (SKŁADANE NA WEZWANIE PRZEZ WYKONAWCĘ KTÓREGO OFERTA ZOSTANIE NAJWYŻEJ OCENIONA)
7. ZAŁĄCZNIK NR 7 – OŚWIADCZENIE O UCZESTNICTWIE W GRUPIE KAPITAŁOWEJ (SKŁADANE NA WEZWANIE PRZEZ WYKONAWCĘ KTÓREGO OFERTA ZOSTANIE NAJWYŻEJ OCENIONA)
8. ZAŁĄCZNIK NR 8 – OŚWIADCZENIE O SPEŁNIENIU MINIMALNYCH WYMAGAŃ W ZAKRESIE STOSOWANYCH ZABEZPIECZEŃ TECHNICZNYCH I ORGANIZACYJNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH OSÓB FIZYCZNYCH.
9. ZAŁĄCZNIK NR 9 - PROJEKT UMOWY



**ZAŁĄCZNIK NR 1 – FORMULARZ OFERTY (SKŁADANE WRAZ Z OFERTĄ)**(nazwa Wykonawcy)**Oferta w postępowaniu**

Ja, niżej podpisany (My niżej podpisani):

działając w imieniu i na rzecz:Składa(m)y ofertę na wykonanie zamówienia, którego przedmiotem jest:

Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine

1. **Oferujemy wykonanie zamówienia w sposób i na warunkach określonych w Warunkach Zamówienia, zgodnie z Opisem Przedmiotu Zamówienia (Rozdział II Warunków Zamówienia), i na zasadach określonych w umowie za cenę (PLN) :**

ŁĄCZNA CENA OFERTY NETTO: ..... PLN

**W tym:**

Lp.	Opis	Ilość	Cena jednostkowa w PLN	Wartość w PLN
1.	Wsparcie techniczne dla licencji ServiceDesk Plus Enterprise Multi-language do 31.12	656		
2.	Wsparcie techniczne dla licencji ServiceDesk Plus Professional Multi-language do 31.12	257		
3.	OpManager ManageEngine dla 50 urządzeń, 15 adresów URL i 15 techników wraz z pluginem Application Manager dla 50 monitorów i modułu MicrosoftSharePoint Monitoring	1		
RAZEM				

2. Wykonamy przedmiot zamówienia zgodnie z terminami wskazanymi w rozdz. I pkt 5 WZ.
3. Oświadczam(y), że:
- a) jestem(śmy) związany(i) niniejszą ofertą przez okres **90 dni** od upływu terminu składania ofert,
  - b) zamówienie wykonam(y):  
☐ **samodzielnie**
  - c) otrzymałem(liśmy) wszelkie informacje konieczne do przygotowania oferty,
  - d) wyrażamy zgodę na wprowadzenie skanu naszej oferty do Platformy Zakupowej Zamawiającego,
  - e) akceptuję(emy) treść Warunków Zamówienia i w razie wybrania mojej (naszej) oferty zobowiązuję(emy) się do podpisania Umowy, zgodnej z projektem stanowiącym **Załącznik nr 9 do Warunków Zamówienia**,
  - f) wszelkie informacje zawarte w formularzu oferty wraz z załącznikami są zgodne ze stanem faktycznym,
  - g) zapoznałem(liśmy) się z postanowieniami kodeksu postępowania dla dostawców i partnerów biznesowych Grupy ENEA dostępnymi pod adresem <https://www.enea.pl/pl/grupaenea/compliance/kodeks-kontrahentow> oraz zobowiązuję(emy) się do ich przestrzegania,

- h) jesteśmy podmiotem, w którym Skarb Państwa posiada bezpośrednio lub pośrednio udziały [dodatkowa informacja do celów statystycznych]:  
☐ tak / ☐ nie
- i) osobą uprawnioną do udzielania wyjaśnień Zamawiającemu w imieniu Wykonawcy jest:  
Pan(i) ..... , tel.: ..... e-mail: .....
- j) informacje o aukcji elektronicznej należy przesłać na adres e-mail: .....
- (Proszę o wskazanie wyłącznie jednego adresu e-mail w celu przekazania informacji o aukcji elektronicznej)**
- k) **Dane osobowe reprezentantów, koordynatorów i personelu Zamawiającego oraz innych osób biorących udział w postępowaniu lub realizacji zamówienia, które zostały przekazane Wykonawcy w ramach niniejszego postępowania lub realizacji przedmiotowego zamówienia, przetwarzane będą zgodnie z klauzulą informacyjną Wykonawcy załączoną (wskazaną) do oferty, której treść:**  
☐ dostępna jest na stronach internetowych Wykonawcy - link do klauzul; <http://www. ....>  
(uzupełnić - jeśli dotyczy)  
☐ przekazana została jako załącznik do oferty (odrębny dokument)  
**(Uwaga nie należy utożsamiać z załącznikiem nr 5 do Warunków Zamówienia)**
4. W przypadku wybrania naszej oferty jako najkorzystniejszej podajemy dane, niezbędne do zawarcia Umowy: [należy uzupełnić, o ile dane są znane na etapie składania oferty]
- a) W moim(naszym) imieniu umowę zawrze Pan(i)..... Pełniący(a) funkcję.....
- b) W celu realizacji przedmiotu Umowy, wyznaczam(y) osobę odpowiedzialną za prawidłową realizację Umowy – Koordynatorów Umowy:  
Imię i nazwisko:  
e-mail – .....  
nr tel. ....
- c) Dane osobowe osób reprezentujących, pracowników, współpracowników oraz innych osób, których dane osobowe zostały lub zostaną przekazane drugiej Stronie w celu zawarcia, realizacji i monitorowania wykonywania Umowy, przetwarzane będą zgodnie z klauzulą informacyjną, której treść:  
☐ dostępna jest na stronach internetowych Wykonawcy - link do klauzul; <http://www. ....> **(uzupełnić - jeśli dotyczy)**  
☐ przekazana zostanie jako załącznik do umowy w wersji papierowej w momencie jej podpisania.

Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy

**ZAŁĄCZNIK NR 2 – OŚWIADCZENIE WYKONAWCY O BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA ORAZ SPEŁNIENIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU (SKŁADANE WRAZ Z OFERTA)**

(nazwa Wykonawcy)

**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine**

<b>I. Informacja dotycząca podstaw wykluczenia z postępowania:</b>	
1. Wykonawca w ciągu ostatnich 3 lat przed upływem terminu składania Ofert uniemożliwił lub odmówił zawarcia Umowy w sprawie Zamówienia po wyborze jego Oferty przez Zamawiającego lub nie wniósł wymaganego zabezpieczenia należytego wykonania Umowy;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
2. Wykonawca w ciągu ostatnich 3 lat przed upływem terminu składania Ofert, nie wykonał przedmiotu Zamówienia na rzecz Zamawiającego lub wykonał go nienależycie, a w ramach działań naprawczych nie doprowadził przedmiotu Zamówienia do stanu zgodności z Umową lub nie naprawił powstałej w ten sposób szkody, , chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które Wykonawca nie ponosi odpowiedzialności;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
3. Wykonawca w ciągu ostatnich 3 lat przed upływem terminu składania Ofert z przyczyn leżących po stronie Wykonawcy doprowadził do wypowiedzenia albo odstąpienia od Umowy w sprawie Zamówienia wykonywanego na rzecz Zamawiającego;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
4. Wykonawca w ciągu ostatnich 3 lat przed upływem terminu składania Ofert dopuścił się poważnych naruszeń Kodeksu Kontrahentów Grupy ENEA albo dopuścił się innych naruszeń postanowień Kodeksu Kontrahentów Grupy ENEA, a w ramach działań naprawczych nie doprowadził do ich usunięcia;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
5. Wykonawca w ciągu ostatnich 3 lat przed upływem terminu składania Ofert w sposób inny niż wskazany w pkt.1-4 wyrządził Zamawiającemu szkodę w związku z realizacją Zamówienia, której to szkody nie naprawił w ramach podjętych działań naprawczych	<input type="checkbox"/> tak / <input type="checkbox"/> nie
6. Wykonawca został wpisany do Rejestru Wykonawców Wykluczonych zgodnie z „Zasadami dokonywania oceny Wykonawców w Obszarze Zakupowym Zakupy Ogólne w Grupie ENEA”	<input type="checkbox"/> tak / <input type="checkbox"/> nie
7. Otwarto likwidację Wykonawcy, ogłoszono jego upadłość, jego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, jego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
8. Wykonawca doradzał lub w inny sposób był zaangażowany w przygotowanie Postępowania o udzielenie tego Zamówienia, a spowodowane tym zaangażowaniem zakłócenie konkurencji nie może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w tym Postępowaniu;	<input type="checkbox"/> tak / <input type="checkbox"/> nie

Jeżeli „tak” Wykonawca ma możliwość udowodnienia, że jego zaangażowanie w przygotowanie Postępowania o udzielenie zamówienia nie zakłóci konkurencji	...
9. Jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne Oferty, chyba że wykażą, że przygotowali te Oferty niezależnie od siebie;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
10. Wykonawca naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że Wykonawca przed upływem terminu składania Ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
11. Wykonawca złożył nieprawdziwe informacje mające lub mogące mieć wpływ na wynik Postępowania;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
12. Wykonawca nie wykazał spełnienia warunków udziału w Postępowaniu;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
13. Wykonawca został wpisany na Listy Sankcyjne <sup>4</sup> ;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
14. Beneficjentem rzeczywistym <sup>5</sup> Wykonawcy jest: i. jest osoba wpisana na Listy Sankcyjne lub ii. była od dnia 24 lutego 2022 r. osoba wpisana na Listy Sankcyjne	<input type="checkbox"/> tak / <input type="checkbox"/> nie
15. Wykonawca <b>podlega wyłączeniu</b> od obowiązku zgłaszania informacji o beneficjentach rzeczywistych do Centralnego Rejestru Beneficjentów Rzeczywistych na podstawie ..... (wskazać podstawę prawną na podstawie której podlega wyłączeniu )	<input type="checkbox"/> tak / <input type="checkbox"/> nie
16. Jednostką dominującą <sup>6</sup> Wykonawcy jest: i. jest osoba wpisana na Listy Sankcyjne lub ii. była od dnia 24 lutego 2022 r. osoba wpisana na Listy Sankcyjne	<input type="checkbox"/> tak / <input type="checkbox"/> nie
17. Wykonawca w rozumieniu art. 3 ust. 1 pkt 37 ustawy z 29 września 1994 r. o rachunkowości jest jednostką zależną, nad którą kontrolę sprawuje jednostka dominująca ..... (wskazać jednostkę dominującą, jeśli istnieje)	<input type="checkbox"/> tak / <input type="checkbox"/> nie

**<sup>4</sup> Listy Sankcyjne**

i. wykazy osób lub podmiotów określone w:

- rozporządzeniu Rady (WE) 765/2006 z dnia 18 maja 2006 r. dotyczącym środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy,
- rozporządzeniu Rady (UE) 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających oraz
- ii. lista osób lub podmiotów określona w ustawie z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego; prowadzona przez ministra właściwego do spraw wewnętrznych, publikowana w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw wewnętrznych, wobec których stosuje się sankcję wykluczenia z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych.

<sup>5</sup> w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,<sup>6</sup> w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości.

II. Informacja dotycząca warunków udziału w postępowaniu	
1. Wykonawca spełnia określone w WZ warunki udziału w postępowaniu dotyczące posiadania niezbędnej wiedzy i doświadczenia oraz dysponowania odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania Zamówienia i posiada wymagane zgodnie z WZ dokumenty:	
a. wykaz Usług Podobnych wykonanych w okresie ostatnich 3 lat przed upływem terminu składania Ofert, z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których Usługi zostały wykonane – zgodnie z pkt 6.1.1 a) WZ;	<input type="checkbox"/> tak / <input type="checkbox"/> nie
b. dokumenty potwierdzające należyte wykonanie Usług Podobnych	<input type="checkbox"/> tak / <input type="checkbox"/> nie
c. posiada aktualny status Partnera producenta oprogramowania – zgodnie z pkt 6.1.1. b) WZ;	<input type="checkbox"/> tak / <input type="checkbox"/> nie

**Oświadczenie:**

Niżej podpisany(-a)(-i) oficjalnie oświadcza(-ją), że informacje podane powyżej w częściach I–II są dokładne i prawidłowe oraz że zostały przedstawione z pełną świadomością konsekwencji poważnego wprowadzenia w błąd.

Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy

**ZAŁĄCZNIK NR 3 – UPOWAŻNIENIE UDZIELONE PRZEZ WYKONAWCĘ (SKŁADANE WRAZ Z OFERTĄ – JEŻELI DOTYCZY)**

(nazwa Wykonawcy)

**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine****Upoważnienie udzielone przez Wykonawcę do podpisania oferty i załączników oraz składania i przyjmowania innych oświadczeń woli w imieniu Wykonawcy w przedmiotowym postępowaniu**

W imieniu .....  
upoważniam Pana/Panią ..... urodzonego/ą dnia .....  
..... w ..... legitymującego się dowodem osobistym numer: .....  
..... seria: ....., PESEL: ..... do:

- a) podpisania oferty,
- b) podpisania wszystkich załączników do Warunków Zamówienia stanowiących integralną część oferty,
- c) składania i przyjmowania innych oświadczeń woli w imieniu Wykonawcy w przedmiotowym postępowaniu,
- d) zawarcia umowy w przedmiotowym postępowaniu.

**Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy**

**ZAŁĄCZNIK NR 4 – OŚWIADCZENIE WYKONAWCY O ZACHOWANIU POUFNOŚCI (SKŁADANE WRAZ Z OFERTA)**

(nazwa Wykonawcy)

**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine**

Niniejszym oświadczam(-y) że, zobowiązuję (-emy) się wszelkie informacje handlowe, przekazane lub udostępnione przez Zamawiającego w ramach prowadzonego postępowania o udzielenie zamówienia, wykorzystywać jedynie do celów uczestniczenia w niniejszym postępowaniu, nie udostępniać osobom trzecim, nie publikować w jakiegokolwiek formie w całości ani w części, lecz je zabezpieczać i chronić przed ujawnieniem. Ponadto zobowiązujemy się je zniszczyć, wraz z koniecznością trwałego usunięcia z systemów informatycznych, natychmiast po zakończeniu niniejszego postępowania, chyba, że nasza oferta zostanie wybrana i Zamawiający pisemnie zwolni nas z tego obowiązku.

Obowiązki te mają charakter bezterminowy.

Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy

**ZAŁĄCZNIK NR 5 – INFORMACJA O ADMINISTRATORZE DANYCH OSOBOWYCH (SKŁADANA WRAZ Z OFERTA)**

(nazwa Wykonawcy)

**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine****INFORMACJA O ADMINISTRATORZE DANYCH OSOBOWYCH**

Oświadczam, że dopełniłem poniższego obowiązku informacyjnego wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia w postępowaniu nr **1400/DW00/ZT/KZ/2024/0000101045**

1. **[dane administratora danych]** Administratorem Pana/Pani danych osobowych jest **ENEA Centrum sp. z o.o. z siedzibą w Poznaniu, Plac Andersa 7; 61-894 Poznań, NIP: 777-000-28-43; REGON: 630770227** (dalej: Administrator).

Dane kontaktowe Inspektora Ochrony Danych: [ecn.iod@enea.pl](mailto:ecn.iod@enea.pl)

**[cele i podstawy przetwarzania danych]** Pana/Pani dane osobowe przetwarzane będą w celu uczestniczenia w postępowaniu nr **1400/DW00/ZT/KZ/2024/0000101045** oraz po jego zakończeniu w celu realizacji usługi na podstawie art. 6 ust. 1 lit. b, f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. tzw. ogólnego rozporządzenia o ochronie danych osobowych, dalej: **RODO**).

2. Podanie przez Pana/Panią danych osobowych jest dobrowolne, ale niezbędne do udziału w postępowaniu oraz realizacji usługi.
3. **[odbiorcy danych]** Administrator może ujawnić Pana/Pani dane osobowe podmiotom z grupy kapitałowej ENEA. Administrator może również powierzyć przetwarzanie Pana/Pani danych osobowych dostawcom usług lub produktów działającym na jego rzecz, w szczególności podmiotom świadczącym Administratorowi usługi IT, serwisowe.

Zgodnie z zawartymi z takimi podmiotami umowami powierzenia przetwarzania danych osobowych, Administrator wymaga od tych dostawców usług zgodnego z przepisami prawa, wysokiego stopnia ochrony prywatności i bezpieczeństwa Pana/Pani danych osobowych przetwarzanych przez nich w imieniu Administratora.

4. **[okres przechowywania danych]** Pani/Pana dane osobowe będą przechowywane do czasu wyboru wykonawcy w postępowaniu nr **1400/DW00/ZT/KZ/2024/0000101045**. Po zakończeniu postępowania przez czas trwania umowy oraz czas niezbędny do dochodzenia ewentualnych roszczeń, zgodnie z obowiązującymi przepisami.
5. **[Pana/Pani prawa]** Posiada Pan/Pani prawo żądania:
  - a) dostępu do treści swoich danych - w granicach art. 15 RODO,
  - b) ich sprostowania – w granicach art. 16 RODO,
  - c) ich usunięcia - w granicach art. 17 RODO,
  - d) ograniczenia przetwarzania - w granicach art. 18 RODO,
  - e) przenoszenia danych - w granicach art. 20 RODO,
  - f) prawo wniesienia sprzeciwu (w przypadku przetwarzania na podstawie art. 6 ust. 1 lit. f) RODO – w granicach art. 21 RODO,

6. Realizacja praw, o których mowa powyżej może odbywać się poprzez wskazanie swoich żądań przesłane Inspektorowi Ochrony Danych na adres e-mail: [ecn.iod@enea.pl](mailto:ecn.iod@enea.pl)
7. Przysługuje Panu/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pan/Pani, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

*Potwierdzam zapoznanie się zamieszczoną powyżej informacją Enei Centrum, dotyczącą przetwarzania danych osobowych.*

Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy



**ZAŁĄCZNIK NR 6 – WYKAZ USŁUG PODOBNYCH (SKŁADANY NA WEZWANIE PRZEZ WYKONAWCĘ KTÓREGO OFERTA ZOSTANIE NAJWYŻEJ OCENIONA)**

(nazwa Wykonawcy)

**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine**

Lp.	Nazwa podmiotu, dla którego wykonywano Usługę Podobną	Przedmiotem jest/była usługa wsparcia serwisowego wraz z wdrożeniem dla systemu Service Desk Plus Manage Engine (TAK/NIE)	Usługa zrealizowana/w trakcie realizacji w okresie ostatnich 3 lat przed upływem terminu składania Ofert (TAK / NIE)	Usługa o wartości minimum 100 000,00 zł netto (TAK/NIE)	Dowód należytego wykonania Usługi (nazwa i oznaczenie dokumentu)
1					
2					
3					

**Załącznikiem do niniejszego formularza, muszą być dokumenty potwierdzające należyte wykonanie/wykonywanie Usługi Podobne przez Wykonawcę. Zamawiający nie dopuszcza przedstawienia referencji własnych tj. wystawionych przez Wykonawcę.**

**DOKUMENTY POTWIERDZAJĄCE NALEŻYTE WYKONANIE USŁUG POWINNY BYĆ SPORZĄDZONE I OZNACZONE W TAKI SPOSÓB, ABY NIE BYŁO WĄTPLIWOŚCI, KTÓRYCH USŁUG WYKAZANYCH PRZEZ WYKONAWCĘ DOTYCZA.**  
Przykład: „Referencje do usługi nr 1”

**UWAGA:** w przypadku Usług trwających Zamawiający akceptuje jedynie referencje, które winny być wystawione w okresie **ostatnich 3 miesięcy od dnia składania ofert;**

*W przypadku Usług realizowanych na rzecz Zamawiającego tj. ENEA Centrum sp. z o.o. brak jest konieczności załączania do Oferty dokumentów potwierdzających wykonanie ze względu na fakt, iż Zamawiający jest w ich posiadaniu oraz ma możliwość ich weryfikacji wewnątrz organizacji. W celu umożliwienia weryfikacji wykonania Usługi Podobnej **konieczne** jest podanie niniejszych danych:*

- *W przypadku realizacji Usługi na podstawie umowy: nr umowy, daty zawarcia umowy oraz danych koordynatora umowy.*
- *W przypadku braku zamieszczenia danych jak powyżej, Zamawiający nie uzna Usługi Podobnej.*

**Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy**

**ZAŁĄCZNIK NR 7 – OŚWIADCZENIE O UCZESTNICTWIE W GRUPIE KAPITAŁOWEJ (SKŁADANE NA WEZWANIE PRZEZ WYKONAWCĘ KTÓREGO OFERTA ZOSTANIE NAJWYŻEJ OCENIONA)**

(nazwa Wykonawcy)

**Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine**

Działając w imieniu i na rzecz (nazwa/firma/adres Wykonawcy)

.....

.....

1. **\*\*** oświadczam, że przynależę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007r. o ochronie konkurencji i konsumentów z wymienionymi poniżej Podmiotami:

lp	Nazwa podmiotu	Adres
1		
2		

Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy

2. **\*** oświadczam, że nie przynależę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007r. o ochronie konkurencji i konsumentów.

Imię i nazwisko/podpis przedstawiciela(i)  
Wykonawcy

**\* niepotrzebne skreślić**

**\*\*wypełnić w przypadku, gdy Wykonawca należy do grupy kapitałowej**

**ZAŁĄCZNIK NR 8 - OŚWIADCZENIE O SPEŁNIENIU MINIMALNYCH WYMAGAŃ W ZAKRESIE STOSOWANYCH ZABEZPIECZEŃ TECHNICZNYCH I ORGANIZACYJNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH OSÓB FIZYCZNYCH.**  
(nazwa Wykonawcy)

Niniejszym oświadczam(y), że reprezentowany przeze mnie (przez nas) podmiot spełnia następujące minimalne wymagania w zakresie stosowanych zabezpieczeń technicznych i organizacyjnych dotyczących ochrony danych osobowych osób fizycznych:

X - oznacza wymagania konieczne do wystartowania w postępowaniu

Pole puste w kolumnie *minimalne wymagania, które Wykonawca zobowiązany jest spełnić* oznacza wymagania których spełnienie jest mile widziane ale ich brak nie dyskwalifikuje z udziału w postępowaniu

Obszary wymagań		Rodzaje zabezpieczeń	Minimalne wymagania, które Wykonawca zobowiązany jest spełnić <sup>7</sup>	W przypadku spełnienia warunków proszę wpisać V
środki organizacyjne	zabezpieczenia proceduralne i osobowe	polityki, procedury, instrukcje,	x	
		stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO,	x	
		zapewnia, aby dane przetwarzane były zgodnie z prawem – art. 6 – 11 RODO,	x	
		zapewnia, aby przestrzegane były prawa osób, których dane są przetwarzane – art. 12-23 RODO	x	
		zapewnia wypełnianie ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym – art. 24 – 31 RODO,	x	
		zapewnia bezpieczeństwo przetwarzania danych uwzględniając charakter zakres, kontekst i cele przetwarzania danych – art. 32- 36 RODO,	x	
		zapewnia kontrolę nad przetwarzaniem danych w postaci monitorowania przestrzegania przepisów i przyjętych procedur przetwarzania przez Inspektora Ochrony Danych lub podmioty certyfikujące, czy monitorujące przestrzeganie przyjętych kodeksów postępowania – art. 27- 43 RODO,	x	
		certyfikacja RODO		
		oświadczenia o zachowaniu bezpieczeństwa ,		
		procedury dotyczące zgłaszanie naruszeń ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO;	x	

<sup>7</sup> Minimalne wymagania, które jest zobowiązany spełnić Wykonawca zostały oznaczone w następujący sposób: X

		procedury dotyczące prowadzenia wewnętrznego rejestru naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;	x	
		wyznaczono IOD zgodnie z art. 37RODO	x	
		raporty dokumentujące wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7.		
		kodeksy branżowe/ stowarzyszenia branżowe		
		upoważnienia do przetwarzania danych osobowych oraz ewidencja upoważnień	x	
		umowy powierzenia z podwykonawcami oraz ewidencja umów powierzenia przetwarzania	x	
		zarządzanie aktywami (przetwarzanymi zbiorami danych),	x	
		w ciągu ostatnich 24 miesięcy działalność podmiotu została skontrolowana przez właściwe, ze względu na przedmiot działalności danego podmiotu, instytucje zewnętrzne, np. inspekcja pracy, UODO		
		wdrożono zalecenia z w/w kontroli w całości		
		wdrożono zalecenia z w/w kontroli częściowo		
		nie wdrożono zalecenia z w/w kontroli		
		zaimplementowano klasyfikację informacji.	x	
		zaimplementowano postępowanie z informacją.	x	
		zaimplementowano obsługę incydentów dot. ochrony danych osobowych.	x	
		zarządzanie ryzykiem przetwarzania danych osobowych	x	
środki techniczne	zabezpieczenia teleinformatyczne	stosowanie oprogramowania zabezpieczającego typu antywirus, antyspam, antymalware i firewall w systemach wykorzystywanych do realizacji usług wykonywanych dla Zamawiającego	X	
		posiadanie wymaganych licencji na wykorzystywane oprogramowanie	X	
		korzystanie z oprogramowania / bibliotek / kodów źródłowych / repozytoriów, które posiadają wszystkie aktualne poprawki bezpieczeństwa IT	X	
		autoryzacja (nadawanie dostępu) i uwierzytelnianie (potwierdzenie zadeklarowanej tożsamości)	X	
		kontrole dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych)	X	
		szyfrowanie informacji/plików zawierających wrażliwe dane (np. dane osobowe, logi, pliki konfiguracyjne, informacje zarządcze) w przypadku ich przesyłania/ wymiany - wykonane poprzez spakowanie i zahasłowanie pliku/plików silnym hasłem o długości min. 17 znaków lub skorzystanie z mechanizmu PKI. Hasła do archiwum są przysyłane innym kanałem niż plik archiwum.	X	

		nie będą wykorzystywane chmury publiczne (np. AWS, GCP, Azure) i publiczne zasoby plikowe (np. DropBox, Google Drive, OneDrive) do wykonywania zadań powierzonych przez Zamawiającego (dla informacji wrażliwych, np. danych osobowych, logów, plików konfiguracyjnych, informacji zarządczych), jedynie za zgodą strony biznesowej Zamawiającego	X	
		zabezpieczenie logów systemów (np. stacji roboczych, serwerów) Wykonawcy,	X	
		segmentacja i separacja sieci,	X	
		informowanie Zamawiającego o incydencie naruszenia bezpieczeństwa teleinformatycznego, jeśli dotyczy on usług wykonywanych dla Zamawiającego	X	
		zapewnienie, że zdalny dostęp do Wykonawcy (jeśli będzie wykorzystywany) jest możliwy tylko przez bezpieczne połączenia (np. VPN, TLS, szyfrowanie)	X	
		nie podłączanie niedozwolonych urządzeń (bez zgody Zamawiającego) do sieci LAN Zamawiającego (za wyjątkiem dostępu jako gość)	X	
		Wykonawca stosuje w swoich sieciach (np. LAN, wifi) standard 802.1x (gdy nie korzysta z VPN Zamawiającego) dla zabezpieczenia przed podłączeniem obcych urządzeń do sieci.	X	
	zabezpieczenia fizyczne	monitoring wizyjny,		
		monitoring wizyjny w trybie ciągłym		
		monitoring wizyjny w trybie okresowym		
		bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie		
		monitoring elektroniczny kontrola dostępu,		
		ochrona fizyczna obiektów,		
		systemy antywłamaniowe,		
		działanie grup interwencyjnych,		

--	--

Miejscowość i data

podpis przedstawiciela(i) Wykonawcy

**ZAŁĄCZNIK NR 9 – PROJEKT UMOWY****UMOWA Nr ..... - projekt**

zawarta w dniu \_\_\_\_\_ roku w Poznaniu pomiędzy:

ENEA Centrum Sp. z o.o. z siedzibą przy pl. Władysława Andersa 7; 61-894 Poznań, zarejestrowaną w Sądzie Rejonowym Poznań Nowe Miasto i Wilda w Poznaniu VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS: 0000477231, posiadającą nr REGON: 630770227, NIP: 777-00-02-843; kapitał zakładowy: 103 929 000 PLN, posiadającą status dużego przedsiębiorcy, reprezentowaną przez:...(należy wskazać imię, nazwisko, funkcję)

zwanym dalej „Zamawiającym”

..... z siedzibą przy ul. ...., -/-....., zarejestrowaną w Sądzie ... w ..... Wydział Gospodarczy pod nr KRS: ..., posiadającą nr REGON: ..., NIP: ..., kapitał zakładowy: ... zł, kapitał wpłacony: ... zł (należy wpisać tylko w przypadku Spółki Akcyjnej lub Spółki Komandytowo-Akcyjnej), reprezentowaną przez: ..... (należy wskazać imię, nazwisko, funkcję)

zwanym dalej „Wykonawcą”

**PREAMBUŁA**

Niniejsza umowa zostaje zawarta w wyniku zakończenia postępowania o udzielenie zamówienia pn. „Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine, subskrypcja licencji OpManager ManageEngine ze wsparciem technicznym oraz plugin Application Manager” znak sprawy 1400/DW00/ZT/KZ/2024/0000101045 prowadzonego w trybie przetargu otwartego na podstawie regulaminu obowiązującego u Zamawiającego.

**§ 1 PRZEDMIOT UMOWY**

1. Zamawiający zleca a Wykonawca przyjmuje do wykonania usługę pn.: „Świadczenie usług wsparcia technicznego dla systemu Service Desk Plus Manage Engine, subskrypcja licencji OpManager ManageEngine ze wsparciem technicznym oraz plugin Application Manager” (zwaną dalej „Przedmiotem umowy” lub „Przedmiotem zamówienia”). Wsparcie techniczne dla Service Desk Plus odbywać się będzie na czterech instancjach systemu Service Desk Plus Manage Engine zainstalowanych na osobnych serwerach.
2. Wykonawca zobowiązuje się do wykonania Przedmiotu umowy zgodnie ze złożoną ofertą oraz Załącznikami do Umowy. W razie rozbieżności między postanowieniami niniejszej Umowy lub innych załączników do niej, zastosowanie mieć będą postanowienia korzystniejsze dla Zamawiającego. Wykonawca przyjmuje do wiadomości, iż cel niniejszej Umowy w zakresie zapewnienia prawidłowego funkcjonowania systemów i infrastruktury określany jest przez Zamawiającego przy uwzględnieniu interesu Spółek Grupy Kapitałowej ENEA (tj. zgodnie z art. 3 ust. 1 pkt. 44 Ustawy o Rachunkowości, ENEA S.A. z siedzibą w Poznaniu oraz podmioty, wobec których jest ona jednostką dominującą, zgodnie z definicją w art. 3 ust. 1 pkt. 37 Ustawy o Rachunkowości).
3. Przez zawarcie Umowy Zamawiający zawiera jednocześnie umowy licencyjne z Producentem, zwane dalej „Umowami Licencyjnymi” (End User License Agreement, EULA), na mocy których Producent udziela Zamawiającemu licencji niewyłącznych na korzystanie z Oprogramowania w zakresie, o którym mowa w postanowieniu §2 ust. 2 Umowy. Udzielenie licencji następuje na czas wskazany w Umowie Licencyjnej.
4. Warunki i zasady udzielenia Licencji określa Umowa Licencyjna, której egzemplarz sporządzony w języku angielskim oraz języku polskim stanowi Załącznik numer 4 i 5 do Umowy.
5. Dla Stron wiążącą jest Umowa Licencyjna w języku angielskim.
6. Zamawiający oświadcza, że zapoznał się z treścią Umowy Licencyjnej, rozumie jej postanowienia i w pełni je akceptuje.

7. Zamawiającemu przysługuje na zasadach określonych Umową Licencyjną prawo do korzystania z podstawowego wsparcia technicznego świadczonego przez Producenta oraz do korzystania z wszelkich wydanych przez Producenta Aktualizacji i Poprawek Oprogramowania.
8. Wykonawca zrealizuje przedmiot zamówienia zgodnie z Warunkami Zamówienia z dnia: ... i treścią złożonej oferty z dnia: ... roku oraz protokołem z negocjacji (jeżeli dotyczy) z dnia: ...
9. Wykonawca zapewnia, że przedmiot zamówienia jest zgodny ze wszelkimi dotyczącymi go normami i przepisami prawa.
10. Wykonawca nie może przenieść praw, w tym wierzytelności wobec Zamawiającego lub obowiązków wynikających z niniejszej Umowy na osoby trzecie bez uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności.

## § 2 TERMINY REALIZACJI

1. Wykonawca przedstawi Zamawiającemu protokół potwierdzający uruchomienie usług: wsparcia technicznego AMS Manage Engine dla systemu Service Desk Plus w terminie maksymalnie 5 dni roboczych od dnia 31 grudnia 2024 r., subskrypcja licencji OpManager ze wsparciem technicznym oraz plugin Application Manager w terminie maksymalnie 5 dni roboczych od dnia 22 grudnia 2024 r.
2. Usługa wsparcia technicznego AMS Manage Engine dla systemu Service Desk Plus będzie świadczona przez okres 12 miesięcy od dnia 31 grudnia 2024 r., subskrypcja licencji OpManager ze wsparciem technicznym oraz pluginem Application Manager będą obowiązywać przez okres 12 miesięcy od dnia 22 grudnia 2024 r.
3. Każdorazowa zmiana terminów, o których mowa w ust. 1 powyżej, wymaga zawarcia przez Strony aneksu do umowy.
4. Wykonawca zobowiązany jest do informowania Zamawiającego o wszystkich okolicznościach mogących mieć wpływ na prawidłową i terminową realizację Przedmiotu umowy nie później niż następnego dnia po dniu zaistnienia danej okoliczności.

## § 3 OŚWIADCZENIA WYKONAWCY

1. Wykonawca gwarantuje, że usługi wsparcia technicznego świadczone będą w sposób profesjonalny zgodnie z parametrami określonymi w Rozdziale II Warunków Zamówienia oraz Szczegółową specyfikacją warunków i terminy wsparcia technicznego określonymi w Załączniku nr 1 do niniejszej umowy.
2. Wykonawca oświadcza, że uzyskał od Zamawiającego wszystkie niezbędne informacje i ma pełną wiedzę co do zakresu prac, trudności, ryzyka oraz wszelkich innych okoliczności, jakie mogą mieć wpływ na realizację umowy.
3. Wykonawca oświadcza, że posiada wiedzę, doświadczenie, wymagane uprawnienia oraz potencjał techniczny, ekonomiczny i kadrowy niezbędny do wykonania prac stanowiących Przedmiot umowy.
4. Wykonawca zapewnia, że przedmiot zamówienia jest zgodny ze wszelkimi dotyczącymi go normami i przepisami prawa.
5. Wykonawca oświadcza i zapewnia, że zapoznał się i będzie przestrzegał postanowień Kodeksu Kontrahentów Grupy ENEA dostępnego na stronie: [https://10.125.13.101/grupaenea/o\\_grupie/enea-polaniec/zamowienia/dokumenty-dla-wykonawcow/zalacznik-nr-1-kodeks-kontrahentow-grupy-enea-informacja-dla-kontrahentow.pdf?t=1588858520](https://10.125.13.101/grupaenea/o_grupie/enea-polaniec/zamowienia/dokumenty-dla-wykonawcow/zalacznik-nr-1-kodeks-kontrahentow-grupy-enea-informacja-dla-kontrahentow.pdf?t=1588858520)
6. W terminie 3 dni od zawarcia umowy, Wykonawca ma obowiązek przekazania Zamawiającemu kodów PKWiU, które dotyczą przedmiotu umowy i będą następnie wskazywane na wystawianych przez niego FV.

## § 4 WYNAGRODZENIE

1. Za prawidłowe i terminowe wykonanie Przedmiotu umowy Wykonawca otrzyma wynagrodzenie ryczałtowe w wysokości: ..... (słownie: ..... ) złotych netto,
2. Do kwoty Wynagrodzenia zostanie doliczony podatek od towarów i usług w wysokości określonej przepisami prawa obowiązującymi w chwili wystawienia faktury.
3. Wykonawca pokrywa wszelkie koszty bankowe swojego banku, koszty instytucji go kredytujących i transferujących środki płatnicze na jego zlecenie w związku z realizacją niniejszej umowy.
4. ENEA Centrum Sp. z o.o. pokrywa wszelkie koszty bankowe swojego banku, koszty instytucji go kredytujących i transferujących środki płatnicze na jego zlecenie w związku z realizacją niniejszej umowy.

**§ 5 WARUNKI PŁATNOŚCI**

1. Podstawą dokonania zapłaty wynagrodzenia będzie faktura wystawiona przez Wykonawcę zgodnie z postanowieniami niniejszej Umowy.
2. Wykonawca wystawi fakturę w terminie 7 dni od daty podpisania przez Zamawiającego protokołu potwierdzającego uruchomienie przez Wykonawcę usług wsparcia technicznego, którego data podpisania przez Zamawiającego jest datą potwierdzającą rozpoczęcie realizacji przedmiotu umowy.
3. W przypadku gdy termin płatności przypada w sobotę lub dzień ustawowo wolny od pracy, płatność nastąpi w pierwszy dzień roboczy przypadający po tych dniach. Za termin dokonania zapłaty rozumie się dzień obciążenia rachunku Zamawiającego.
4. Za nieterminową zapłatę faktury Wykonawca może naliczyć odsetki ustawowe za opóźnienie od transakcji handlowych, na podstawie obowiązujących przepisów.
5. Faktura wystawiona przedwcześnie, bezpodstawnie lub bez protokołu potwierdzającego odbiór prac przez Zamawiającego „bez zastrzeżeń”, nie rodzi obowiązku zapłaty.
6. Wykonawca oświadcza, że rachunek bankowy Wykonawcy, służący do rozliczenia wynagrodzenia spełnia wymogi na potrzeby mechanizmu podzielonej płatności (split payment), tzn. że do ww. rachunku bankowego jest przypisany rachunek VAT, a faktura będzie zawierać numery ww. rachunków oraz specjalne oznaczenie w postaci zapisu: „mechanizm podzielonej płatności”, a także, że faktura spełniać będzie inne warunki określone w powszechnie obowiązujących przepisach w tym zakresie.
7. Zamawiający oświadcza, że płatności za wszystkie faktury realizuje z zastosowaniem mechanizmu podzielonej płatności (split payment).
8. Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności (split payment).
9. Płatności za faktury będą realizowane wyłącznie na numery rachunków rozliczeniowych, o których mowa w art. 49 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe, lub imiennych rachunków w spółdzielczej kasie oszczędnościowo-kredytowej, której Wykonawca jest członkiem, otwartych w związku z prowadzoną przez Wykonawcę działalnością gospodarczą – wskazanych w zgłoszeniu identyfikacyjnym lub zgłoszeniu aktualizacyjnym i potwierdzonych przy wykorzystaniu STIR w rozumieniu art. 119zg pkt 6 Ordynacji podatkowej („Rachunek”).
10. Płatność za prawidłową realizację przedmiotu Umowy będzie dokonana przez Zamawiającego przelewem na Rachunek wskazany przez Wykonawcę na fakturze w terminie 30 dni od daty doręczenia na adres wskazany w ust. 16 prawidłowo wystawionej faktury. Wykonawca oświadcza, że Rachunek wskazany na fakturze został wskazany w zgłoszeniu identyfikacyjnym lub zgłoszeniu aktualizacyjnym złożonym przez Wykonawcę do naczelnika właściwego urzędu skarbowego i znajduje się na tzw. „białej liście podatników VAT”, o której mowa w art. 96 b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.
11. Jeżeli Zamawiający stwierdzi, że Rachunek wskazany przez Wykonawcę na fakturze nie znajduje się na tzw. „białej liście podatników VAT” lub rachunek wskazany przez Wykonawcę nie spełnia wymogów określonych w ust. 6 niniejszego paragrafu, Zamawiający wstrzyma się z dokonaniem zapłaty za prawidłową realizację Przedmiotu Umowy do czasu wskazania innego rachunku przez Wykonawcę, który będzie umieszczony na przedmiotowej liście oraz będzie spełniał warunki określone w ust.10. W takim przypadku Wykonawca zrzeka się prawa do żądania odsetek za opóźnienie w płatności za okres od pierwszego dnia po upływie terminu płatności wskazanego w ust. 10 do 7-go dnia od daty powiadomienia Zamawiającego o numerze rachunku spełniającego wymogi, o których mowa w zdaniu poprzednim.
12. Wykonawca ponosi wyłączną odpowiedzialność za wszelkie szkody poniesione przez Zamawiającego w przypadku, jeżeli oświadczenia i zapewnienia zawarte w ust. 6 oraz 10 okażą się niezgodne z prawdą. Wykonawca zobowiązuje się zwrócić Zamawiającemu wszelkie obciążenia nałożone z tego tytułu na Zamawiającego przez organy administracji skarbowej oraz zrekompensować szkodę, jaka powstała u Zamawiającego, wynikającą w szczególności, ale nie wyłącznie, z zakwestionowania przez organy administracji skarbowej prawidłowości odliczeń podatku VAT na podstawie wystawionych przez Wykonawcę faktur dokumentujących realizację Przedmiotu Umowy, jak również braku możliwości zaliczenia przez Zamawiającego wydatków poniesionych z realizacją Przedmiotu Umowy w koszty uzyskania przychodu.



13. Zamawiający oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.
14. Zamawiający akceptuje odbiór faktur ustrukturyzowanych oraz korekt faktur ustrukturyzowanych za pośrednictwem Krajowego Systemu eFaktur. Wystawienie faktury za pośrednictwem Krajowego Systemu eFaktur nie wymaga przesyłania faktury drogą elektroniczną lub papierową.  
Faktura ustrukturyzowana w polu przeznaczonym na informacje dodatkowe powinna zawierać ww. oznaczenia, w szczególności:
  - numer zamówienia podany przez Zamawiającego,
  - nazwę komórki organizacyjnej – jeśli dotyczy
15. Załączniki do faktury ustrukturyzowanej Wykonawca przesyła na adres e-mail koordynatora Umowy ze strony Zamawiającego podając w tytule wiadomości numer faktury.
16. W przypadku gdy przeszkody techniczne uniemożliwią przesłanie faktur za pośrednictwem Krajowego Systemu eFaktur Wykonawca zobowiązuje się do wystawienia Zamawiającemu faktury w formie elektronicznej w formacie nieedytowalnym (np. pdf) oraz przesłania jej na adres: faktury.elektroniczne@enea.pl. Wykonawca nie przesyła w takim przypadku wersji papierowej dokumentu.
17. W sytuacji braku możliwości wystawienia faktury w formie elektronicznej Zamawiający dopuszcza dostarczenie faktury w wersji papierowej oraz przesłanie jej na adres: ENEA Centrum sp. z o.o. Centrum Zarządzania Dokumentami, ul. Zacisze 28, 65-792 Zielona Góra
18. Faktura winna zawierać dodatkowe oznaczenia, w szczególności:
  - numer zamówienia podany przez Zamawiającego,
  - nazwę komórki organizacyjnej – jeśli dotyczy,
19. Każda faktura powinna być zapisana, jako odrębny plik – nie może być przesłany jeden zbiorczy plik (np. pdf) kilku faktur.
20. Faktury, które posiadają załącznik w formie odrębnego pliku (pdf) należy wysłać, jako pojedyncze wiadomości e-mail (faktura + załącznik).

#### § 6 KARY UMOWNE

1. Wykonawca zapłaci na rzecz Zamawiającego karę umowną za każdy rozpoczęty dzień zwłoki lub opóźnienia w dostarczeniu protokołu potwierdzającego uruchomienie usług wsparcia technicznego – w wysokości 0,5% ustalonego wynagrodzenia netto określonego w §4 ust. 1 liczony od upływu terminu określonego w §2 ust. 1,
2. Wykonawca zapłaci na rzecz Zamawiającego karę umowną za rozwiązanie umowy ze skutkiem natychmiastowym przez Zamawiającego z przyczyn leżących po stronie Wykonawcy – w wysokości 10% ustalonego wynagrodzenia netto określonego w §4 ust. 1.
3. W przypadku, gdy szkody u Zamawiającego spowodowane działaniem lub zaniechaniem Wykonawcy lub osoby, za którą ponosi on odpowiedzialność przekraczają wysokość kar umownych określonych w ust. 1, niezależnie od kar umownych oraz w sytuacjach, w których nie zostały one zastrzeżone Zamawiający może dochodzić, na zasadach ogólnych od Wykonawcy odszkodowania w kwocie przewyższającej wartość kar umownych – do wysokości rzeczywiście poniesionej szkody.
4. Wykonawca jest zobowiązany do zapłaty Zamawiającemu kary umownej w kwocie 50.000,00 PLN (słownie pięćdziesiąt tysięcy złotych) za każdy przypadek:
  - a) naruszenie obowiązków ochrony informacji dotyczących bądź udostępnionych przez Zamawiającego oraz zachowania poufności,
  - b) naruszenia ochrony danych osobowych dotyczących bądź udostępnionych przez Zamawiającego
5. Zamawiający uprawniony jest do potrącenia naliczonych kar umownych z należności Wykonawcy.
6. Zapłata kar umownych nastąpi w terminie 7 dni od dnia wezwania skierowanego przez Zamawiającego do Wykonawcy.

**§ 7 ROZWIĄZANIE UMOWY**

1. Zamawiający może rozwiązać umowę ze skutkiem natychmiastowym w przypadku rażącego naruszenia przez Wykonawcę postanowień niniejszej umowy, w szczególności zrealizowania przedmiotu umowy niezgodnie z dokumentami wskazanymi w § 1 ust. 2.
2. Oświadczenie o rozwiązaniu Umowy wymaga zachowania formy pisemnej pod rygorem nieważności.
3. W przypadku rozwiązania umowy ze skutkiem natychmiastowym, bez względu na to, która strona rozwiązała umowę, Wykonawca wstrzyma dalszą realizację umowy poza dostawami określonymi przez Zamawiającego, koniecznymi dla zabezpieczenia już zrealizowanych prac.
4. W przypadku rozwiązania umowy ze skutkiem natychmiastowym Zamawiający zapłaci Wykonawcy wynagrodzenie za zrealizowany zakres umowy wykonany do dnia jej rozwiązania ze skutkiem natychmiastowym.
5. Mimo rozwiązania Umowy, Wykonawca pozostaje zobowiązany wobec Zamawiającego do zachowania obowiązku poufności i ochrony danych osobowych na zasadach i pod rygoremi określonymi w niniejszej Umowie.
6. Rozwiązanie przez Zamawiającego Umowy w trybie natychmiastowym nie pozbawia go prawa do podnoszenia względem Wykonawcy roszczeń odszkodowawczych, w tym żądania zapłaty kar umownych, wskazanych w Umowie.

**§ 8 KLAUZULA POUFNOŚCI**

1. Każda ze Stron oświadcza, że wszelkie informacje uzyskane w związku z zawarciem lub wykonywaniem Umowy albo przy okazji tych zdarzeń, stanowią tajemnicę przedsiębiorstwa drugiej Strony w rozumieniu art. 11 ustawy o zwalczaniu nieuczciwej konkurencji, chyba że informacje te są lub staną się informacjami dostępnymi publicznie na skutek zdarzeń zgodnych z prawem (Informacje Poufne). Za tajemnicę przedsiębiorstwa każdej ze Stron uznaje w szczególności informacje dotyczące działalności gospodarczej, informacje organizacyjne, finansowe, prawne, handlowe, marketingowe, produkcyjne, operacyjne, techniczne oraz technologiczne.
2. Wykonawca przyjmuje do wiadomości, że uzyskane przez Wykonawcę w związku z zawarciem lub wykonywaniem niniejszej Umowy albo przy okazji tych zdarzeń, mogą stanowić ponadto Informacje Poufne *ENEA S.A. i/lub/albo\* LWB Bogdanka S.A.* w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE (rozporządzenie MAR), wobec czego wykorzystanie lub ujawnienie informacji poufnej, jak też udzielenie rekomendacji lub nakłonienie innej osoby na podstawie informacji poufnej do nabycia lub zbycia instrumentów finansowych, których dotyczy ta informacja, wiąże się z odpowiedzialnością przewidzianą w powszechnie obowiązujących przepisach prawa. Wykonawca oświadcza, że zapewnia zachowanie poufności tych informacji oraz zobowiązuje się przestrzegać obowiązku zachowania poufności.
3. W pozostałym zakresie, nieokreślonym w ust. 1 i 2 Informacje Poufne każdej ze Stron definiowane są jako wszelkie informacje, dane lub dokumenty, które każda ze Stron otrzyma lub wytworzy w związku z realizacją Przedmiotu Umowy, z wyjątkiem informacji, które:
  - 1) są lub staną się ogólnie dostępne w inny sposób niż na skutek złamania zobowiązań określonych w niniejszej klauzuli poufności, lub
  - 2) będą znane Stronom przed rozpoczęciem realizacji Przedmiotu Umowy, a nie zostały otrzymane jako poufne w ramach innego zlecenia, lub
  - 3) zostaną otrzymane od osoby trzeciej, która, zgodnie z wiedzą stron, nie jest zobowiązana do zachowania poufności w odniesieniu do tych informacji.
4. Każda ze Stron zobowiązuje się do ochrony informacji określonych w ust. 1, 2 i 3 powyżej, w tym w szczególności:
  - 1) zachować informacje w poufności,
  - 2) zapewnić w pełnym zakresie ochronę przed ujawnieniem informacji, z zachowaniem staranności wymagane w stosunkach danego rodzaju,
  - 3) wykorzystywać informacje wyłącznie w celu wykonania Umowy,
  - 4) przekazywać informacje wyłącznie podmiotom uprawnionym z mocy ustawy do uzyskania tych informacji, w niezbędnym wymaganym zakresie; o każdym przypadku przekazania informacji strona przekazująca jest zobowiązany powiadomić drugą Stronę na piśmie, chyba że powiadomienie jest sprzeczne z obowiązującymi przepisami,

- 5) niezwłocznie zawiadomić drugą Stronę na piśmie o każdym przypadku nieuprawnionego dostępu do informacji,
- 6) po wykonaniu Umowy usunąć wszystkie informacje, chyba że Strony zażądają na piśmie innego sposobu wykonania tego obowiązku, w szczególności zwrotu nośników, na których przechowywane są informacje.
5. Każda ze Stron jest zobowiązana do ochrony informacji określonych w ust. 1, 2 i 3 powyżej przez okres od uzyskania pierwszego dostępu do informacji do upływu pięciu lat od dnia zakończenia wykonywania Umowy.
6. Niezależnie od obowiązków związanych z ochroną informacji określonych w ust. 1, 2 i 3 powyżej, każda ze Stron zobowiązuje się zachować w poufności wszelkie informacje, które uzyskała w związku z zawarciem lub wykonywaniem Umowy, jeżeli ich ujawnienie mogłoby w jakikolwiek sposób naruszać renomę drugiej Strony. Powyższy obowiązek ma charakter bezterminowy.
7. W trakcie obowiązywania Umowy oraz przez okres 5 lat od dnia zakończenia jej wykonywania każda ze Stron jest uprawniona zwrócić się z wnioskiem o złożenie przez drugą Stronę oświadczenia dotyczącego wypełniania obowiązku ochrony Informacji Poufnych. Strony są zobowiązane złożyć oświadczenie w terminie 21 (dwudziestu jeden) dni kalendarzowych.

#### § 9 NADZÓR NAD REALIZACJĄ PRZEDMIOTU UMOWY

1. Obowiązki koordynującego (sprawy związane z realizacją niniejszej umowy) ze strony Zamawiającego pełnić będzie: Pan(i) ....., tel.: +48 ....., e-mail: .....
2. Obowiązki koordynującego (sprawy związane z realizacją niniejszej umowy) ze strony Wykonawcy pełnić będzie: Pan(i) ....., tel.: +48 ....., e-mail: .....
3. Zmiana osób koordynujących, jak również zmiana środków komunikacji wskazanych w niniejszej Umowie (nr. telefonów, adresy email) nie stanowią zmiany Umowy i nie wymagają zawierania dodatkowych aneksów. O powyższych zmianach Strony powiadamiają się wzajemnie w formie pisemnej lub drogą elektroniczną.

#### § 10 PODWYKONAWSTWO

1. Wykonawca nie może powierzyć realizacji całości lub części zamówienia podwykonawcy bez pisemnej zgody Zamawiającego na powierzenie realizacji określonej części bądź całości zamówienia podwykonawcy wskazanemu przez Wykonawcę. Jednakże, jeżeli Zamawiający w terminie 14 dni nie zgłosi na piśmie sprzeciwu lub zastrzeżeń, uważa się, że Zamawiający zgody udzielił. Powyższe nie dotyczy podwykonawców wskazanych w ofercie złożonej przez Wykonawcę w ramach postępowania.
2. Wykonanie całości lub części zamówienia nie może być w żadnym przypadku powierzone podwykonawcy lub dalszemu podwykonawcy będącemu jednocześnie pracownikiem Zamawiającego, chyba, że Zamawiający wyrazi na to zgodę, a przy wykonywaniu powierzonej mu części zamówienia podwykonawca lub dalszy podwykonawca będzie występował, jako przedsiębiorca prowadzący we własnym imieniu działalność gospodarczą na zasadach określonych w przepisach ustawy o swobodzie działalności gospodarczej.

#### § 11 OCHRONA DANYCH OSOBOWYCH

1. Zamawiający powierza oraz podpowierza Wykonawcy do przetwarzania Dane osobowe w zakresie i na zasadach określonych w Umowie powierzenia przetwarzania danych osobowych, która stanowi załącznik nr ..... do Umowy. Powierzenie Wykonawcy przetwarzania danych osobowych wymaga zawarcia odrębnej umowy powierzenia danych osobowych na piśmie. Jeżeli w ocenie Wykonawcy w okresie obowiązywania Umowy pojawi się obowiązek zawarcia takiej umowy, Wykonawca jest zobowiązany zawiadomić o tym fakcie Zamawiającego na piśmie lub za pośrednictwem koordynatorów Umowy.
2. Zamawiający oświadcza, iż w rozumieniu RODO, administratorem danych (dalej: Administrator) w odniesieniu do powierzonych zgodnie z Umową danych osobowych, pozostają Spółki (każda z osobna):....., a wszelkie prawa do powierzonych danych osobowych przez cały czas trwania Umowy należą do Administratorów.
3. Umowa wraz z Umową DPA stanowią łącznie udokumentowanie polecenia Administratora, o którym mowa w art. 28 ust. 3 lit. a) RODO.

**§ 12 SIŁA WYŻSZA**

1. Strony będą zwolnione od odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy, o ile niewykonanie lub nienależyte wykonanie zobowiązania nastąpiło wskutek siły wyższej w rozumieniu Kodeksu cywilnego.
2. Strona, która zamierza żądać zwolnienia z odpowiedzialności z powodu siły wyższej zobowiązana jest powiadomić drugą Stronę na piśmie, bez zbędnej zwłoki, o jej zajściu i ustaniu.
3. Zaistnienie siły wyższej powinno być udokumentowane przez Stronę powołującą się na nią.

**§ 13 POSTANOWIENIA KOŃCOWE**

1. Umowa główna oraz DPA podlegają prawu polskiemu, natomiast umowa EULA podlega prawu holenderskiemu.
2. Ewentualne spory mogące wynikać z realizacji niniejszej umowy strony będą starały się rozwiązać polubownie.
3. W przypadku gdyby rozwiązania polubownego nie dało się wypracować, sądem właściwym do rozstrzygania wszelkich sporów będzie sąd powszechny właściwy ze względu na siedzibę Zamawiającego.
4. Gdyby któreś z postanowień niniejszej umowy były lub stały się bezskutecznymi, Strony dążyć będą do ich zastąpienia takimi postanowieniami, które będą skuteczne i możliwie najpełniej zrealizują cel postanowień bezskutecznych. To samo obowiązuje w przypadku luki w umowie.
5. Zapisy § 8 obowiązują Strony przez czas nieoznaczony.
6. Wszelkie zmiany i uzupełnienia w treści umowy wymagają formy pisemnej pod rygorem nieważności.
7. Zmiany adresu Stron, numeru rachunku bankowego, wykazu osób do kontaktu i danych kontaktowych nie stanowią zmiany umowy i nie wymagają zawierania dodatkowych aneksów. O powyższych zmianach Strony powiadamiają się wzajemnie w formie pisemnej, ze skutkiem od chwili doręczenia.
8. W sprawach nieuregulowanych niniejszą umową obowiązują w szczególności przepisy Kodeksu Cywilnego.
9. Treść umowy stanowi tajemnicę przedsiębiorstwa ENEA Centrum Sp. z o.o. i nie może być ujawniona stronie trzeciej bez pisemnej zgody Zamawiającego.
10. Wykonawca oświadcza, że zapoznał się z postanowieniami „Kodeksu Kontrahentów Grupy ENEA” dostępnego pod adresem <https://www.enea.pl/pl/grupaenea/compliance/kodeks-kontrahentow>, akceptuje je oraz zobowiązuje się do przestrzegania zawartych w nim zasad.
11. Umowę sporządzono w ... jednobrzmiących egzemplarzach, po jednym dla każdej ze stron, chyba, że którakolwiek ze Stron podpisze umowę kwalifikowanym podpisem elektronicznym. Wówczas druga strona otrzyma egzemplarz Umowy podpisanej elektronicznie za pośrednictwem poczty elektronicznej.
12. Za datę zawarcia Umowy poczytuje się datę złożenia przez ostatnią ze Stron podpisu odręcznego albo kwalifikowanego podpisu elektronicznego weryfikowanego przy pomocy kwalifikowanego certyfikatu, zgodnie z warunkami określonymi ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (tj.: Dz. U. z 2021 r., poz. 1797 z późn. zm.). W sytuacji, gdy Umowa podpisywana jest przez więcej niż jedną osobę działającą w imieniu Strony datą zawarcia jest data, którą opatrzone jest ostatni z podpisów składanych przez osoby działające w imieniu Strony. W przypadku złożenia podpisu odręcznego przez którąkolwiek ze Stron przyjmuje się, że umowa została zawarta w dniu wskazanym w preambule umowy.
13. Załączniki do umowy stanowią jej integralną część, do których zalicza się:
  - a) Załącznik nr 1 - Szczegółową specyfikacją warunków i terminy wsparcia technicznego AMS Manage Engine
  - b) Załącznik nr 2 – Protokół z negocjacji (jeżeli dotyczy).
  - c) Załącznik nr 3 - Umowa DPA
  - d) Załącznik nr 4 - Umowa EULA w języku angielskim
  - e) Załącznik nr 5 - Umowa EULA w języku polskim

**ZA ZAMAWIAJĄCEGO:****ZA WYKONAWCĘ:**

**Projekt Umowy o powierzenie przetwarzania danych osobowych do postępowania nr 1400/DW00/ZT/KZ/2024/0000101045**

**UMOWA  
O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH („UMOWA DPA”)**

zawarta w dniu ..... pomiędzy:

<b>ENEA Centrum Sp. z o.o. z siedzibą w Poznaniu, pl. Władysława Andersa 7, 61-894 Poznań</b>	..... <b>z siedzibą w .....</b>
wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu VIII Wydział Gospodarczy – Krajowy Rejestr Sądowy pod numerem KRS 477231, NIP 7770002843, REGON 630770227, wysokość kapitału zakładowego: 103.929.000,00 zł;	wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy w ..... pod numerem KRS ....., NIP ....., REGON ....., wysokość kapitału zakładowego: .....zł,
zwana dalej „ <b>EC</b> ”	zwana dalej „ <b>Przetwarzającym Dane</b> ”
reprezentowana przez: ..... ..... .....	reprezentowana przez: ..... ..... .....

zwane dalej łącznie „**Stronami**” a każda z osobna „**Stroną**”

**Preambuła**

**a. EC przetwarza dane osobowe powierzone jej przez**

- Enea Wytwarzanie Sp. z o.o. z siedzibą w Świerże Górne, 26-900 Kozienice, ul. Aleja Józefa Zielińskiego 1
- ENEA Badania i Rozwój Sp. z o.o. z siedzibą w Świerżach Górnych ul. Aleja Józefa Zielińskiego 1, 26 - 900 Kozienice
- Enea Bioenergia Sp. z o.o. z siedzibą w Zawadzie 26, 28-230 Połaniec,
- Enea Ciepło Serwis Sp. z o.o. z siedzibą w Białymstoku, ul. Starosielce 2/1, 15-670 Białystok
- Enea Ciepło Sp. z o.o. z siedzibą w Białymstoku, ul. Warszawska 27, 15-062 Białystok
- Enea Operator Sp. z o.o. z siedzibą w Poznaniu, ul. Strzeszyńska 58, 60-479 Poznań
- Enea S.A. z siedzibą w Poznaniu, ul. Górecka 1, 60-21 Poznań
- Enea Innowacje Sp. z o.o. z siedzibą w Warszawie kod pocztowy 00-124 Warszawa Al. Jana Pawła II 12
- Enea Logistyka Sp. z o.o. z siedzibą w Poznaniu, ul. Strzeszyńska 58, 60-479 Poznań
- Enea Oświetlenie Sp. z o.o. z siedzibą w Szczecinie, ul. Ku Słońcu 34, 71-080 Szczecin
- Enea Elektrownia Połaniec S.A. z siedzibą w Zawadzie 26, 28-230 Połaniec
- Enea Pomiary Sp. z o.o. z siedzibą w Poznaniu, ul. Strzeszyńska 58, 60-479 Poznań
- Enea Serwis sp. z o.o. z siedzibą w Gronówko 30, 64-111 Lipno
- Enea Trading Sp. z o.o. z siedzibą w Świerżach Górnych, Świerże Górne, gm. Kozienice, 26-900 Kozienice 1
- Enea Połaniec Serwis Sp. z o.o. z siedzibą w Zawadzie 26, 28-230 Połaniec
- Enea Nowa Energia Sp. z o.o. z siedzibą w Radomiu, ul. Kaszubska 2, 26-603 Radom
- Enea Elkogaz Sp. z o.o. z siedzibą w Warszawie, Aleja Jana Pawła II 12, 00-124 Warszawa
- Enea EKO Sp. z o.o. z siedzibą w Warszawie, Aleja Jana Pawła II 12, 00-124 Warszawa
- PV Genowefa Sp. z o.o. z siedzibą w Poznaniu, ul. Pastelowa 8, 60-198 Poznań

*Na podstawie Umowy Powierzenia Przetwarzania Danych Osobowych z dnia ..... zawartej między wyżej wymienionymi Spółkami jako Administratorami Danych a EC jako podmiotem przetwarzającym te Dane. Na podstawie tej umowy EC może podpowierzyć przetwarzanie tych danych.*

- b. Jednocześnie EC jest również samodzielnym Administratorem Danych.
- c. Strony oświadczają, że Przetwarzający Dane świadczy na rzecz EC usługi, w ramach których ma miejsce przetwarzanie danych osobowych.
- d. Strony mają świadomość spoczywających na nich obowiązków wynikających z obowiązującego prawa dotyczącego ochrony danych.
- e. Najważniejszym celem niniejszej Umowy DPA jest zapewnienie wysokiego poziomu ochrony danych osobowych zgodnie z obowiązującymi przepisami prawa oraz ustalenie wysokiego standardu ochrony danych jak również środków osobowych, technicznych i organizacyjnych służących temu celowi.
- f. Niniejsza Umowa DPA określa wzajemne prawa i obowiązki Stron w zakresie realizacji wzajemnej współpracy w odniesieniu do powierzenia przetwarzania danych.

## **§1. Przedmiot Umowy DPA**

1. Strony łączy Umowa ..... z dnia ..... na Zakup licencji Service, zwana dalej „Umową Główną”. Przewiduje się w trakcie obowiązywania niniejszej Umowy DPA zawarcie innych stosunków cywilnoprawnych, dotyczących infrastruktury informatycznej EC.
2. Wykonywanie Umowy Głównej wiąże się z czynnościami Przetwarzania Danych Osobowych – zarówno tych, co do których EC jest Administratorem Danych jak i Danych Osobowych Spółek, co do których EC jest podmiotem przetwarzającym Dane.
3. Przetwarzający Dane zobowiązuje się, że będzie przetwarzał Dane Osobowe na podstawie niniejszej Umowy DPA zgodnie z postanowieniami Rozporządzenia Parlamentu Europejskiego i Rady nr 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 (Dz. Urz. UE z 4.05.2016, nr L 119/1) („GDPR”), prawa krajowego dotyczącego ochrony danych osobowych oraz jakichkolwiek innych obowiązujących przepisów prawa regulujących ochronę danych osobowych.
4. W przypadku jakichkolwiek rozbieżności pomiędzy prawem krajowym dotyczącym ochrony danych a GDPR po dniu 25 maja 2018 r. moc wiążącą należy przyznać GDPR.
5. Terminy używane w niniejszej Umowie DPA, które nie zostały konkretnie zdefiniowane w jej treści mają znaczenie nadane im przez GDPR.

## **§2. Definicje**

Dla celów niniejszej Umowy DPA, w tym Preambuły, stosuje się następujące definicje:

<b>Podmiot Danych</b>	każda osoba fizyczna, której dotyczą Dane Osobowe;
<b>Umowa Główna</b>	umowa regulująca współpracę pomiędzy Stronami, o której mowa w § 1 niniejszej Umowy DPA, wskazana w ust 1 ;
<b>Dane Osobowe</b>	wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (Podmiotu Danych), które stanowią przedmiot niniejszej Umowy DPA – zarówno dane osobowe, co do których EC jest Administratorem Danych jak i dane osobowe przetwarzane przez Spółki, co do których EC jest podmiotem przetwarzającym Dane;
<b>Naruszenie Ochrony Danych Osobowych</b>	każde zdarzenie mające miejsce u Przetwarzającego Dane lub Podprzetwarzającego Dane, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, nieuprawnionego dostępu lub dostępności Danych Osobowych dla których EC lub Spółki są Administratorami;

<b>Przetwarzanie Danych Osobowych</b>	operacja lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub nieautomatyzowany, jaką jest zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
<b>Prawo Ochrony Danych Osobowych</b>	GDPR oraz inne znajdujące zastosowanie akty i regulacje Unii Europejskiej lub prawa krajowego;
<b>Podprzetwarzający Dane</b>	umowny partner Przetwarzającego Dane, który przetwarza Dane Osobowe dla których EC lub Spółki są Administratorami , będąc włączonym do procesu przetwarzania przez Przetwarzającego Dane;
<b>Spółki</b>	Spółki wskazane w pkt a) preambuły wraz z EC
<b>Administrator Danych</b>	Osoba fizyczna lub prawna lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Pojęcia zdefiniowane powyżej zachowują nadane im niniejszą Umową DPA znaczenie niezależnie od tego, czy występują w liczbie pojedynczej czy liczbie mnogiej.

### **§3. Postanowienia dotyczące Przetwarzania Danych Osobowych**

1. EC powierza Dane Osobowe do przetwarzania Przetwarzającemu Dane na czas i w celu wykonania Umowy Głównej.
2. Dla celów realizacji przedmiotu niniejszej Umowy DPA określonego powyżej, Przetwarzający Dane przetwarza Dane Osobowe powierzone mu przez EC w zakresie określonym w Załączniku II pkt 1 do niniejszej Umowy DPA.
3. Dane Osobowe będą przetwarzane w sposób określony w Załączniku II pkt 2 do niniejszej Umowy DPA.

### **§4. Cel przetwarzania**

Przetwarzający Dane może przetwarzać Dane Osobowe, w celu realizacji Umowy Głównej wskazanej w § 1 niniejszej Umowy DPA wyłącznie dla celów określonych w Załączniku I pkt 4 do niniejszej Umowy DPA.

### **§5. Prawa i obowiązki EC**

1. Jeżeli w trakcie obowiązywania Umowy zajdzie konieczność przekazania Przetwarzającemu Dane dodatkowych informacji o prawnych, technicznych lub organizacyjnych wymogach, które Przetwarzający Dane powinien znać, aby Przetwarzanie Danych odbywało się zgodnie z obowiązującym prawem, EC przekaze te informacje niezwłocznie.
2. EC może wydawać polecenia co do rodzaju, zakresu i sposobu Przetwarzania Danych Osobowych. Polecenia te mogą być wydawane pisemnie lub za pośrednictwem poczty elektronicznej.
3. EC może kontrolować przestrzeganie niniejszej Umowy DPA oraz Prawa Ochrony Danych Osobowych. EC jest uprawniona do przeprowadzania kontroli w miejscu przetwarzania jak również w lokalach Przetwarzającego Dane mających na celu uzyskanie potrzebnych informacji lub wglądu w przechowywane Dane Osobowe, a także kontroli programów służących przetwarzaniu Danych Osobowych, w każdym czasie i bez zbędnej zwłoki. W tym celu Przetwarzający Dane udostępni wskazane powyżej miejsca osobom kontaktowym lub, w zależności od konkretnego przypadku, innej osobie trzeciej upoważnionej przez EC do przeprowadzenia czynności kontrolnych. W celu przeprowadzenia kontroli EC poinformuje Przetwarzającego Dane co najmniej 5 dni roboczych przed planowaną datą kontroli o zamiarze jego przeprowadzenia. Jeżeli z ważnych

powodów, w ocenie Przetwarzającego Dane, kontrola nie może zostać przeprowadzona we wskazanym terminie Przetwarzający Dane powinien poinformować o tym fakcie EC drogą elektroniczną, wskazując uzasadnienie dla takiej oceny. W takim przypadku Strony wspólnie ustalają późniejszy termin kontroli.

4. Kontrole mogą być przeprowadzane w dni robocze w trakcie normalnych godzin pracy u Przetwarzającego Dane. Kontrola będzie przeprowadzana w sposób niezakłócający bieżącej działalności Przetwarzającego Dane, przy zachowaniu dobrej woli obu Stron i w racjonalnym czasie. EC może dokumentować wyniki kontroli. Przetwarzający Dane jest zobowiązany do udzielania EC pomocy, również w przypadku kontroli ochrony danych osobowych prowadzonych przez właściwe organy nadzorcze, w zakresie w jakim dotyczą one Przetwarzania Danych Osobowych wynikającego z niniejszej umowy DPA. Przetwarzający Dane zobowiązany jest do bezzwłocznego wdrożenia wymogów wskazanych przez organ nadzorczy w porozumieniu z EC.
5. Prawa EC określone w niniejszym paragrafie przysługują również Spółkom wymienionym w preambule, w zakresie przetwarzania Danych Osobowych, co do których są one Administratorem Danych. Spółki mogą wykonywać kontrole samodzielnie lub w porozumieniu z EC., na warunkach wskazanych w ust. 3 i 4 powyżej.

#### **§6. Prawa i obowiązki Przetwarzającego Dane**

1. Przetwarzający Dane ma obowiązek Przetwarzania Danych Osobowych wyłącznie na podstawie postanowień niniejszej Umowy DPA oraz udokumentowanych poleceń EC.
2. Przetwarzający Dane nie może wykorzystywać Danych Osobowych dla innych celów niż wskazane w niniejszej Umowie DPA, w szczególności Przetwarzający Dane nie może bez zgody EC udzielonej na piśmie przekazać Danych Osobowych osobom trzecim. Bez uprzedniej zgody EC Przetwarzający Dane nie może tworzyć kopii i duplikatów Danych Osobowych, z tym że zastrzeżenie powyższe nie obejmuje tworzenia kopii zapasowych w celu zapewnienia właściwego Przetwarzania Danych Osobowych.
3. Przetwarzający Dane zapewni, aby osoby upoważnione przez niego do Przetwarzania Danych Osobowych zobowiązały się do zachowania tajemnicy oraz przestrzegania właściwych sposobów zabezpieczenia Danych Osobowych lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Przetwarzający Dane zapewni, aby osoby upoważnione przez niego do Przetwarzania Danych Osobowych uczestniczyły szkoleniach z zakresu ochrony danych osobowych. Przetwarzający Dane zobowiązuje się dostarczyć każdorazowo, na żądanie EC i w terminie przez nią wyznaczonym, aktualną listę osób zaangażowanych w przetwarzanie Danych Osobowych w związku z niniejszą Umową DPA. Przetwarzający Dane ogranicza dostęp do powierzonych Danych Osobowych wyłącznie do osób, dla których dostęp jest niezbędny w celu realizacji Umowy Głównej lub niniejszej Umowy DPA.
4. Przetwarzający Dane może przetwarzać Dane Osobowe na podstawie niniejszej Umowy DPA jedynie w kraju i siedzibie, wskazanych w Załączniku I pkt 2 do niniejszej Umowy DPA. O wszystkich innych miejscach wykonywania czynności przetwarzania lub wszelkich zmianach dotychczasowych miejsc przetwarzania w tym samym kraju Przetwarzający Dane uprzednio informuje EC. W takim przypadku EC przysługuje prawo do sprzeciwu. Jeżeli EC nie wniesie sprzeciwu w terminie jednego miesiąca od otrzymania powyższych informacji od Przetwarzającego Dane, uznaje się, że wyraziła zgodę na inne miejsca lub zmianę miejsc przetwarzania w tym samym kraju w zakresie wskazanym w informacji otrzymanej od Przetwarzającego Dane.
5. Jeżeli Przetwarzający Dane zamierza przetwarzać Dane Osobowe w innym kraju, dla takiego Przetwarzania Danych Osobowych wymagana jest uprzednia pisemna zgoda EC.
6. Zaangażowanie Podprzetwarzających Dane oraz miejsca przetwarzania przez nich Danych Osobowych podlegają paragrafowi 8 niniejszej Umowy DPA.
7. Przetwarzający Dane ma obowiązek bez zbędnej zwłoki, w miarę możliwości nie później niż w ciągu 24 godzin od uzyskania informacji poinformować EC o Naruszeniu Ochrony Danych Osobowych, o wszelkich przypadkach poważnego zakłócenia operacji przetwarzania, jakimkolwiek podejrzeniu naruszenia ochrony



danych, nieprzestrzegania Prawa Ochrony Danych Osobowych, które dotyczy Danych Osobowych lub innych zauważonych przez niego nieprawidłowościach przy Przetwarzaniu Danych Osobowych przez Przetwarzającego Dane, pracowników Przetwarzającego Dane lub Podprzetwarzających Dane. Informacja taka powinna zostać przekazana na formularzu, którego wzór stanowi Załącznik III. Przetwarzający Dane powinien dostarczyć wraz z informacją, o której mowa powyżej, wszystkie informacje wymagane przez EC niezbędne do zgłoszenia Naruszenia Ochrony Danych Osobowych. Jeżeli określonych informacji, o których mowa w Załączniku III Przetwarzający Dane nie jest w stanie przedstawić w terminie wskazanym powyżej, zobowiązany jest je udzielać sukcesywnie bez zbędnej zwłoki, jednakże w żadnym wypadku nie później niż w ciągu 48 godzin od powzięcia danych informacji, wraz z wyjaśnieniem przyczyn opóźnienia. W każdym ze wskazanych powyżej przypadków Przetwarzający Dane bezzwłocznie podejmie wszystkie niezbędne kroki w celu zapewnienia należytej ochrony Danych Osobowych, a następnie postąpi zgodnie z poleceniami przekazanymi mu przez EC. Przetwarzający Dane umożliwi EC uczestnictwo w jakichkolwiek czynnościach wyjaśniających prowadzonych w związku z wymienionymi zdarzeniami. W przypadku jakiegokolwiek naruszenia Prawa Ochrony Danych Osobowych w związku z Przetwarzaniem Danych Osobowych przez Przetwarzającego Dane, Przetwarzający Dane ma obowiązek wspierania EC w powiadamianiu Podmiotów Danych dotkniętych naruszeniem oraz organu nadzorczego, jeżeli zostanie o to poproszony.

8. Jeżeli Przetwarzający Dane otrzyma jakąkolwiek skargę, powiadomienie lub zgłoszenie, które odnosi się do Przetwarzania Danych Osobowych przez Przetwarzającego Dane lub zgodności z Prawem Ochrony Danych Osobowych przez którąkolwiek ze Stron, Przetwarzający Dane niezwłocznie powiadomi o tym EC, w zakresie dozwolonym przepisami prawa, oraz będzie w niezbędnym zakresie współpracował z i pomagał EC w odniesieniu do takiej skargi, powiadomienia lub zgłoszenia.
9. Przetwarzający Dane ma obowiązek niezwłocznego poinformowania EC o każdej:
  - 1) skardze Podmiotu Danych w zakresie jej Danych Osobowych lub jakiegokolwiek prośbie otrzymanej od Podmiotu Danych o dostęp do jej Danych Osobowych lub o każdym innym zgłoszeniu odnoszącym się bezpośrednio lub pośrednio do Przetwarzania Danych Osobowych w związku z niniejszą Umową DPA; Przetwarzający Dane dostarczy EC wszystkich zażądanych informacji dotyczących takiej skargi, prośby lub zgłoszenia,
  - 2) korespondencji lub żądaniu jakiegokolwiek organu nadzoru ochrony Danych Osobowych mających związek z Przetwarzaniem Danych Osobowych, powierzonych Umową DPA,
    - a także niezwłocznie podejmie współpracę z EC lub Spółką w związku z takim żądaniem lub komunikacją, skargą, prośbą lub zgłoszeniem, co obejmuje między innymi odpowiedź na żądanie lub komunikację, skargę, prośbę lub zgłoszenie.
10. Jeżeli Podmiot Danych będzie wykonywać swoje prawo do dostępu, sprostowania, uzupełnienia, usunięcia lub ograniczenia przetwarzania Danych Osobowych względem EC, Przetwarzający Dane będzie zobowiązany do wykonania żądania Podmiotu Danych zgodnie z poleceniami EC. Jeżeli Podmiot Danych przekaże tego rodzaju żądanie bezpośrednio do Przetwarzającego Dane, Przetwarzający Dane jest zobowiązany do niezwłocznego poinformowania o tym EC i działania zgodnie z poleceniami EC.
11. Na żądanie EC Przetwarzający Dane będzie prowadził rejestry przetwarzania Danych Osobowych oraz dostarczy EC aktualne informacje dotyczące ochrony i bezpieczeństwa danych przetwarzanych na podstawie niniejszej Umowy DPA, również wynikające z prowadzonych rejestrów.
12. Po zakończeniu współpracy wynikającej z niniejszej Umowy DPA lub w każdym czasie na życzenie EC Przetwarzający Dane zobowiązuje się do zwrotu EC lub do zniszczenia wszystkich Danych Osobowych przetwarzanych na podstawie niniejszej Umowy DPA oraz do usunięcia ich w trwały sposób ze swoich nośników danych w terminie nie dłuższym niż 14 dni od zakończenia współpracy, chyba że przepisy obowiązującego prawa nakładają na Przetwarzającego Dane obowiązek przechowywania Danych Osobowych przez Przetwarzającego Dane. Wszystkie działania związane z niszczeniem danych powinny być przeprowadzone w sposób, który jest zgodny z najnowszą technologią w zakresie środków zapewnienia poufności danych, chyba że EC wyraźnie wymaga innej procedury. Na życzenie EC Przetwarzający dane przedłoży pisemne potwierdzenie usunięcia Danych Osobowych.

13. Jeżeli Przetwarzający Dane ustanowi Inspektora Ochrony Danych, Przetwarzający dane przekaże niezwłocznie EC jego dane kontaktowe.
14. Osoba wyznaczona przez Przetwarzającego do spraw ochrony danych będzie pozostawać w kontakcie z EC w zakresie wszelkich kwestii związanych z ochroną danych powierzonych Przetwarzającemu dane przez EC, w szczególności w przypadku wystąpienia incydentów Naruszenia Ochrony Danych Osobowych.
15. Przetwarzający Dane wykonuje prawa i obowiązki określone w niniejszym paragrafie odpowiednio w stosunku do Spółek w zakresie w jakim dotyczy to Danych Osobowych dla których to spółki są Administratorami.

#### **§7. Środki techniczne i administracyjne**

1. Przetwarzający Dane zobowiązuje się zapewnić adekwatne środki organizacyjne i techniczne lub personel, które zapewnią ochronę Danych Osobowych na poziomie nie niższym niż opisany w niniejszej umowie, w celu zapewnienia właściwego standardu bezpieczeństwa Danych Osobowych odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych. W szczególności Przetwarzający Dane zobowiązany jest zapewnić szczególną ochronę Danych Osobowych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, niedozwolonym ujawnieniem lub dostępem, przestaniem, przechowywaniem lub przetwarzaniem w inny sposób, co mogłoby w szczególności prowadzić do fizycznego, materialnego lub niematerialnego uszkodzenia Danych Osobowych. W celu zachowania bezpieczeństwa i zapobieżenia Przetwarzaniu Danych Osobowych niezgodnemu z niniejszą Umową DPA, Przetwarzający Dane oceni ryzyko związane z Przetwarzaniem Danych Osobowych i wdroży odpowiednie środki w celu minimalizacji tego ryzyka. Przed przystąpieniem do Przetwarzania Danych Osobowych, Przetwarzający Dane oceni wpływ planowanych czynności przetwarzania na ochronę Danych Osobowych i przedłoży wynik EC lub zapewni EC odpowiednie wsparcie, jeżeli ocena wpływu będzie przeprowadzana bezpośrednio przez EC.
2. Przetwarzający Dane jest zobowiązany do poinformowania EC o wszelkich istotnych decyzjach związanych z bezpieczeństwem, a dotyczących organizacji Przetwarzania Danych Osobowych oraz zastosowanych procedur.
3. Na wniosek EC lub Spółek, Przetwarzający Dane jest zobowiązany do dostarczenia EC wyczerpującej, aktualnej informacji na temat ochrony danych i bezpieczeństwa dla zleconego Przetwarzania Danych Osobowych na podstawie niniejszej Umowy DPA.

#### **§8. Podprzetwarzający Dane**

1. Przetwarzający Dane nie będzie powierzał żadnych czynności wynikających z niniejszej Umowy DPA jakimkolwiek osobom trzecim bez uprzedniej pisemnej zgody EC. EC zezwala Przetwarzającemu Dane na zaangażowanie Podprzetwarzających wyłącznie na zasadach wynikających z niniejszej Umowy DPA w zakresie, w jakim mogą i powinny mieć zastosowanie do Podprzetwarzającego Dane. Przetwarzający Dane odpowiedzialny jest za działania i zaniechania Podprzetwarzających Dane jak za swoje własne działania lub zaniechania Lista podmiotów, którym Przetwarzający Dane powierzył dalej przetwarzanie Danych Osobowych znajduje się w Załączniku IV. EC niniejszym wyraża zgodę na dalsze powierzenie Danych Osobowych do tych podmiotów.
2. Przetwarzający Dane podejmie odpowiednie kroki w celu zapewnienia, że Podprzetwarzający Dane będzie zobowiązany wobec Przetwarzającego Dane w taki sam sposób, w jaki Przetwarzający Dane jest zobowiązany względem EC oraz Administratora na podstawie niniejszej Umowy DPA. Przetwarzający Dane jest zobowiązany do przeprowadzania kontroli Podprzetwarzającego Dane w celu weryfikacji, czy Podprzetwarzający Dane prawidłowo wykonuje spoczywające na nim zobowiązania w związku z powierzeniem mu przez Przetwarzającego Dane Danych Osobowych do przetwarzania. W szczególności Przetwarzający Dane powinien sprawdzić, czy środki stosowane przez Podprzetwarzającego Dane są zgodne z ustalonymi między Przetwarzającym Dane a Podprzetwarzającym Dane środkami technicznymi i organizacyjnymi przed rozpoczęciem Przetwarzania Danych Osobowych i później - w regularnych odstępach

czasu. Wyniki tych audytów muszą być dokumentowane i przekazywane przez Przetwarzającego Dane EC oraz Administratorowi na ich życzenie.

3. Przetwarzający Dane jest zobowiązany do zagwarantowania, aby EC lub Spółki mogły przeprowadzać audyty względem Podprzetwarzającego Dane na co najmniej takich samych zasadach, na jakich może przeprowadzać audyty u Przetwarzającego Dane. Przetwarzający Dane ma obowiązek zawarcia odpowiednich postanowień umownych zabezpieczających prawo EC lub Spółek do audytu w umowie między nim a Podprzetwarzającym Dane. Powyższy obowiązek obejmuje uprawnienia do audytu, jakie EC lub Spółki uzyskują względem Przetwarzającego Dane na mocy niniejszej Umowy DPA.

#### **§9. Odpowiedzialność. Kary umowne.**

1. Przetwarzający Dane ponosi pełną odpowiedzialność względem EC za wszelkie naruszenia niniejszej Umowy DPA wynikłe z nieprawidłowego wykonywania niniejszej Umowy DPA przez Przetwarzającego Dane - poprzez zapłatę kar umownych lub odszkodowania. Wszelkie ograniczenia odpowiedzialności uzgodnione inaczej niż w niniejszej umowie nie znajdują zastosowania do niniejszej Umowy DPA.
2. W przypadku zawinionego naruszenia przez Przetwarzającego Dane niniejszej Umowy DPA EC przysługuje uprawnienie do naliczania kar umownych w wysokości 30.000,00 PLN (słownie trzydzieści tysięcy złotych 00/100) w przypadku każdego naruszenia odrębnie, przy czym za odrębne naruszenie uważany będzie pojedynczy incydent prowadzący do naruszeń niezależnie od ilości danych osobowych. Uprawnienie to przysługuje EC z tytułu naruszenia niniejszej Umowy DPA z przyczyn dotyczących wyłącznie nieprawidłowego wykonywania niniejszej Umowy DPA przez Przetwarzającego Dane.
3. Naliczenie zastrzeżonych Umową kar umownych nie wyłącza możliwości dochodzenia przez EC odszkodowania na zasadach ogólnych wynikających z przepisów kodeksu cywilnego do pełnej wysokości szkody (jeżeli wystąpiła) poniesionej przez EC w związku ze zdarzeniem, które jest podstawą naliczenia określonej kary.
4. Kary umowne są niezależne od siebie i należą się EC w pełnej wysokości. Za każdy przypadek naruszenia niniejszej Umowy DPA, rozumiany w sposób określony w ust.2, kary umowne będą naliczane odrębnie. Kary wynikające z niniejszej Umowy DPA mogą być naliczane w przypadku:
  - a) Uniemożliwienia przeprowadzenia kontroli i/lub niewywiązania się z obowiązków określonych w §5 ust.3 Umowy DPA związanych z przeprowadzeniem kontroli;
  - b) Uniemożliwienia przeprowadzenia kontroli i/lub niewywiązania się z obowiązków określonych w §5 ust.3 Umowy DPA w toku kontroli programów służących przetwarzaniu Danych Osobowych;
  - c) Naruszenia postanowień §6 ust.3 Umowy DPA w związku z obowiązkiem szkoleniowym;
  - d) Naruszenia postanowień §6 ust.3 zdanie 3 Umowy DPA, w związku z niedostarczeniem lub dostarczeniem znacząco po wyznaczonym terminie listy osób zaangażowanych w przetwarzanie Danych Osobowych;
  - e) Braku uzyskania zgody lub postąpienia wbrew sprzeciwowi EC, o którym mowa w §6 ust.4 Umowy DPA;
  - f) Przetwarzania danych w innym kraju bez zgody EC;
  - g) Postąpienie wbrew stanowisku EC w sytuacjach, o których mowa w §6 ust.7 Umowy DPA w przypadku braku poinformowania o poważnym zakłóceniu operacji przetwarzania, jakimkolwiek podejrzeniu naruszenia ochrony danych, nieprzestrzegania Prawa Ochrony Danych Osobowych, które dotyczy Danych Osobowych, lub innych zauważonych przez niego nieprawidłowościach przy Przetwarzaniu Danych Osobowych;
  - h) Brak poinformowania lub poinformowanie ze znacznym opóźnieniem o skardze, powiadomieniu lub zgłoszeniu, o którym mowa w §6 ust.8 Umowy DPA;

- i) Niewywiązania się z obowiązków nałożonych na Przetwarzającego Dane w §6 ust.9 ppkt 1 i 2 Umowy DPA;
- j) Naruszenia obowiązku określonego w §6 ust.10 Umowy DPA;
- k) Niewywiązania się z obowiązków wskazanych w §6 ust.11 Umowy DPA;
- l) Naruszenia lub niewywiązania się z obowiązków określonych w §6 ust.12 Umowy DPA;
- m) Niewywiązania się z obowiązku określonego w §7 ust.1 Umowy DPA;
- n) Niewywiązania się lub znacznego opóźnienia w wykonaniu obowiązku określonego w §7 ust.2 Umowy DPA;
- o) Niewywiązania się lub znacznego opóźnienia w wykonaniu obowiązku określonego w §7 ust.3 Umowy DPA;
- p) Naruszenia któregośkolwiek z obowiązków wskazanych w §8 ust.1 Umowy DPA;
- q) Nieprzeprowadzenia kontroli, o której mowa w §8 ust.2 Umowy DPA;
- r) Braku umownego zagwarantowania możliwości dokonania kontroli o której mowa w §8 ust.3 Umowy DPA;

W przypadku, o których mowa w niniejszym ust. 4 lit. c), d), k), o) przed nałożeniem kary konieczne będzie wezwanie Przetwarzającego Dane do zaprzestania naruszeń i wyznaczenie dodatkowego odpowiedniego terminu do ich usunięcia, co najmniej 5 dni roboczych.

5. Kary umowne są należne także w przypadku wypowiedzenia niniejszej Umowy DPA lub jej rozwiązania przez Stronę.
6. Kwoty kar umownych będą płatne w terminie 21 (dwadzieścia jeden) dni od otrzymania wezwania do zapłaty, co nie wyłącza możliwości potrącenia naliczonych kar ani zaspokojenia roszczeń z zabezpieczenia należytego wykonania niniejszej Umowy DPA, o ile takie zabezpieczenie zostało ustanowione.
7. Niezależnie od zasad odpowiedzialności uregulowanych w niniejszym paragrafie, Przetwarzający Dane ponosi odpowiedzialność za naruszenie ochrony danych osobowych na zasadach określonych w GDPR, w szczególności w art. 82 i 83, oraz na zasadach określonych w przepisach prawa krajowego dotyczących ochrony danych osobowych.
8. W przypadku skierowania przez osobę trzecią lub Spółkę będącą Administratorem Danych do EC jakichkolwiek roszczeń, w tym roszczeń odszkodowawczych, wynikających z zawinionych nieprawidłowości w przetwarzaniu Danych Osobowych wyłącznie przez Przetwarzającego Dane lub Podprzetwarzającego Dane, w tym przetwarzaniem Danych Osobowych niezgodnie z niniejszą Umową DPA lub niezgodnie z Prawem Ochrony Danych Osobowych lub niezgodnie z pisemnymi poleceniami EC lub Spółkę będącą Administratorem lub wbrew pisemnym poleceniom EC lub Spółek będących Administratorami Danych, Przetwarzający Dane zwolni EC z obowiązku świadczenia w przypadku jakiegokolwiek roszczenia osoby trzeciej lub Spółek będących Administratorem Danych w zakresie wszelkich odszkodowań należnych od EC w związku z takim naruszeniem w pełnym zakresie oraz pokrycia wszelkich kosztów związanych z dochodzeniem przez osobę trzecią lub Spółkę będącą Administratorem Danych tego roszczenia, w tym kosztów sądowych i kosztów zastępstwa procesowego. Podmiot Przetwarzający jest odpowiedzialny na zasadach wskazanych powyżej w stosunku do Spółek będących Administratorami Danych w zakresie kierowanych do niego roszczeń związanych z nieprawidłowym przetwarzaniem Danych Osobowych po stronie Przetwarzającego Dane.
9. Przetwarzający Dane jest zobowiązany do udzielenia EC lub Spółce będącej Administratorem Danych wszelkiej pomocy, w tym informacji i wyjaśnień, potrzebnych do podjęcia obrony przed ewentualnymi roszczeniami. Przetwarzający Dane wstąpi do procesu na miejsce pozwanego w razie zaistnienia sytuacji z

ust.8 lub, gdyby było to niemożliwe, wstąpi do procesu w charakterze interwenienta ubocznego, jeśli przepisy prawa lub charakter postępowania na to pozwolą.

10. Przetwarzający Dane ponosi względem EC lub Spółek będących Administratorami Danych pełną odpowiedzialność za wszelkie działania lub zaniechania Podprzetwarzających Dane, w zakresie, w jakim powierza im przetwarzanie Danych Osobowych, których dotyczy niniejsza Umowa DPA, jak za własne działania lub zaniechania, niezależnie od podjętych przez Przetwarzającego Dane działań mających na celu dokonanie oceny, czy Podprzetwarzający Dane daje rękojmię należytego przetwarzania Danych Osobowych, w tym czy stosuje właściwe środki techniczne lub organizacyjne zabezpieczenia Danych Osobowych.
11. EC nie ponosi żadnej odpowiedzialności w stosunku do Przetwarzającego Dane lub Podprzetwarzającego Dane za szkodę powstałą po stronie Przetwarzającego Dane lub Podprzetwarzającego Dane wskutek nałożenia odpowiednio na Przetwarzającego Dane lub Podprzetwarzającego Dane przez organ nadzorczy administracyjnej kary pieniężnej lub innej sankcji administracyjnej z tytułu Naruszenia Ochrony Danych Osobowych przez odpowiednio Przetwarzającego Dane lub Podprzetwarzającego Dane.

#### **§10. Komunikowanie się Stron**

1. EC wyznacza osobę kontaktową określoną w Załączniku I pkt 5 do niniejszej Umowy DPA.
2. Przetwarzający Dane wyznacza osobę kontaktową określoną w Załączniku I pkt 5 do niniejszej Umowy DPA.

#### **§11. Załączniki do Umowy DPA**

Poniższe Załączniki stanowią integralną część niniejszej Umowy DPA.

Załącznik I określa:

1. datę zawarcia niniejszej Umowy DPA,
2. strony Umowy DPA,
3. przedmiot Umowy DPA,
4. cel przetwarzania Danych Osobowych,
5. osoby kontaktowe Stron.

Załącznik II określa:

1. Dane Osobowe przetwarzane przez Przetwarzającego Dane,
2. Sposób przetwarzania Danych Osobowych.

Załącznik III określa:

1. Wzór formularza zgłoszenia naruszenia.

Załącznik IV określa:

1. Listę podmiotów, którym Wykonawca powierza przetwarzanie danych osobowych

#### **§12. Postanowienia końcowe**

1. Niniejsza Umowa DPA zaczyna obowiązywać w dniu jej podpisania przez obie Strony i zastępuje dotychczasowe regulacje odnoszące się do Danych Osobowych jakie obowiązywały pomiędzy Stronami. Niniejsza Umowa DPA ulega rozwiązaniu wraz z rozwiązaniem Umowy Głównej lub w inny sposób określony tamże.

2. Zmiany niniejszej Umowy DPA wymagają zachowania formy pisemnej pod rygorem nieważności, za wyjątkiem zmian osób kontaktowych Stron, o których Strony zawiadamiają się w formie pisemnej
3. EC może rozwiązać niniejszą Umowę DPA w każdym czasie bez zachowania okresu wypowiedzenia w przypadku poważnego naruszenia postanowień niniejszej Umowy DPA, przy czym za poważne naruszenie postanowień niniejszej Umowy DPA uznać należy w szczególności: (i) niewykonanie polecenia lub odmowa zezwolenia na kontrolę ze strony EC, w części lub w całości, lub (ii) Przetwarzanie Danych w zakresie innym niż dozwolony cel lub poza uzgodnionym krajem, lub (iii) zaangażowanie niezatwierdzonych Podprzetwarzających Dane, lub (iv) jakiegokolwiek istotne Naruszenie Ochrony Danych Osobowych lub brak zgłoszenia zgodnie z wymogami określonymi w § 6.6 powyżej.
4. Jeżeli podjęcie jakichkolwiek czynności Przetwarzania Danych Osobowych będzie konieczne po wygaśnięciu Umowy Głównej w celu dokonania właściwych rozliczeń między Stronami lub podjęcia innych czynności w celu wygaszenia wynikających z Umowy Głównej zobowiązań, do takiego dalszego Przetwarzania Danych Osobowych zastosowanie będą miały postanowienia niniejszej Umowy DPA.
5. W przypadku, gdy część niniejszej Umowy DPA straci ważność lub stanie się niewykonalna, jej pozostałe postanowienia będą nadal wiążące dla Stron, chyba że Umowa DPA bez tych nieważnych części lub postanowień stałaby się niewykonalna. W takim przypadku Strony natychmiast rozpoczną negocjacje w celu przyjęcia nowych postanowień pozwalających na wykonanie Umowy DPA w sposób jak najpełniej zaspokajający ich wzajemne zobowiązania.
6. Niniejsza Umowa DPA stanowi całość uzgodnień i ustaleń pomiędzy Stronami w zakresie spraw w niej uregulowanych i zastępuje jakiegokolwiek poprzednie umowy łączące Strony i odnoszące się do tych spraw.
7. Niniejsza Umowa DPA podlega prawu właściwemu dla EC i zgodnie z nim powinna być interpretowana. Wszelkie spory wynikające z niniejszej Umowy DPA będą rozstrzygane przez sądy właściwe dla siedziby EC.
8. Niniejsza Umowa DPA została sporządzona i podpisana w dwóch jednobrzmiących egzemplarzach po jednym egzemplarzu dla każdej ze Stron.

<i>Za EC</i>	<i>Za Przetwarzającego Dane</i>

## Załącznik I do Umowy DPA

### 1. Data zawarcia Umowy DPA

Niniejsza Umowa DPA została zawarta w dniu [...] 201[ ] r.

### 2. Strony Umowy DPA

<b>ENEA Centrum Sp. z o.o. z siedzibą w Poznaniu, pl. Władysława Andersa 7, 61-894 Poznań</b>	
wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu VIII Wydział Gospodarczy – Krajowy Rejestr Sądowy pod numerem KRS 477231, NIP 7770002843, REGON 630770227, wysokość kapitału zakładowego: 103.929.000,00 zł;	
zwana dalej „EC”	zwana dalej „Przetwarzającym Dane”
reprezentowana przez:	reprezentowana przez:
.....	.....
.....	.....
.....	.....

### 3. Przedmiot Umowy DPA

Strony łączy umowa [.....] z dnia ..... dotycząca świadczenia przez Przetwarzającego Dane usług na rzecz EC w postaci dostarczenia licencji Service Desk

Niniejsza Umowa DPA stanowi Załącznik do Umowy Głównej.

### 4. Cel przetwarzania danych osobowych

Przetwarzający Dane może przetwarzać Dane Osobowe, zgodnie z § 1 niniejszej Umowy DPA („Przetwarzanie Danych Osobowych”) wyłącznie dla celów opisanych w Umowie Głównej

### 5. Osoby kontaktowe Stron

	<i>po stronie EC</i>	<i>po stronie Przetwarzającego</i>
<i>Imię i nazwisko</i>		
<i>Stanowisko</i>		
<i>Telefon</i>		
<i>E-mail</i>		

## **Załącznik II do Umowy DPA**

### **1. Dane Osobowe przetwarzane przez Przetwarzającego Dane**

Na potrzeby realizacji przedmiotu Umowy dot. (...) przetwarzane Dane Osobowe dotyczą:

- Pracowników Spółek
- Klientów Spółek

#### Rodzaje Danych Osobowych, których przetwarzanie dotyczy:

- Imiona/Nazwiska/
- Adres
- Data urodzenia
- Miejsce urodzenia
- PESEL/NIP
- Dane o stanie cywilnym
- Tel./Faks
- Adres e-mail
- Obywatelstwo
- Stanowisko służbowe
- Rachunek bankowy, itd.
- Dane dotyczące PPE (Punktu Poboru Energii)
  - Numer
  - Moc umowna
  - Moc przyłączeniowa
  - Adres Punktu Poboru

#### Dane wrażliwe/specjalne (które muszą zostać tutaj wymienione szczegółowo):

- dane dotyczące przynależności związkowej
- dane dotyczące stanu zdrowia
- religia
- członkostwo w radzie pracowniczej
- płeć

### **2. Sposób przetwarzania Danych Osobowych**

Dane Osobowe będą przetwarzane poprzez dostęp do systemów Service Desk Plus, OpManager Professional oraz Application Manager Plugin, w których zgromadzone są te dane. Same systemy usadowione są w infrastrukturze ENEA. Dostęp do danych poprzez VPN funkcjonujący w Enea, bądź wysyłkę logów systemu.

## **Załącznik III do Umowy DPA**



**- Wzór zgłoszenia o Naruszeniu Ochrony Danych Osobowych**

Należy wypełnić w ciągu 24 godzin od uzyskania świadomości o Naruszeniu. Wypełnione zgłoszenie należy przesłać za pośrednictwem zaszyfrowanej wiadomości e-mail do osoby kontaktowej po stronie EC wskazanej w Umowie DPA.

Wzór zgłoszenia o Naruszeniu Ochrony Danych Osobowych		
Przetwarzający:		
Zgłaszający:		
Wydział/departament:	Numer telefonu:	E-mail:

Data zgłoszenia:	Czas zgłoszenia:
Data zdarzenia:	Czas zdarzenia:
Czy zgłoszenie zostało dokonane z opóźnieniem: <i>(minęły więcej niż 24 godzin od daty zdarzenia)</i>	<div style="display: flex; justify-content: space-around;"> <span>T</span> <span>N</span> </div> <div style="display: flex; justify-content: space-around;"> <input type="checkbox"/> <input type="checkbox"/> </div>
Powód opóźnienia:	
Opis Naruszenia Ochrony Danych Osobowych <i>(proszę krótko opisać zdarzenie)</i>  1) Kategorie podmiotów danych <i>(np. klienci, pracownicy)</i>  2) Liczba podmiotów danych dotkniętych Naruszeniem <i>(przybliżona)</i>  3) Kategorie zbiorów/rejestrów danych <i>(np. dane finansowe, numery rachunków bankowych)</i>  4) Liczba zbiorów/rejestrów danych dotkniętych Naruszeniem <i>(przybliżone)</i>	
Opis możliwych skutków Naruszenia Ochrony Danych Osobowych:	

- 1) Czy istnieje zagrożenie dla danych szczególnych kategorii? Jeśli tak, proszę wskazać w jakim zakresie.
- 2) Czy podmioty danych dotkniętych Naruszeniem mają świadomość Naruszenia?
- 3) Jaki wpływ i konsekwencje dla bezpieczeństwa ich danych może mieć Naruszenie?
- 4) Czy którykolwiek z podmiotów danych dotkniętych Naruszeniem złożył w związku z nim skargę lub zgłosił roszczenia?

#### Środki naprawcze

- 1) Jakie środki zostały wdrożone w celu zapobieżenia tego rodzaju zdarzeniom?
- 2) Czy zostały podjęte jakiekolwiek środki mające na celu ograniczenie wpływu zdarzenia na bezpieczeństwo danych? Jeśli tak, proszę je opisać szczegółowo.
- 3) Czy wobec danych dotkniętych Naruszeniem zastosowano środki naprawcze? Jeśli tak, proszę wskazać jakie i kiedy.
- 4) Jakie środki podjęto w celu zapobieżenia zajścia takich zdarzeń w przyszłości?

#### Szkolenia i wytyczne

- 1) Czy Twój personel został przeszkolony ze znajomości GDPR?
- 2) Czy szkolenia w zakresie GDPR są obligatoryjne? Czy osoby uczestniczące w zdarzeniu brały udział w szkoleniu?

#### Pozostałe

- 1) Czy policja została poinformowana o zdarzeniu? Jeśli tak, proszę podać szczegóły.
- 2) Czy pozostałe właściwe organy zostały poinformowane o zdarzeniu? Jeśli tak, proszę podać szczegóły.
- 3) Czy zdarzenie były przedmiotem jakichkolwiek doniesień medialnych? Jeśli tak, proszę podać szczegóły.

Czy zgodnie z Twoją wiedzą zdarzenie dotyczyło któregoś z poniższych elementów?

Telefon	<input type="checkbox"/>	Kradzież	<input type="checkbox"/>
Fax	<input type="checkbox"/>	Oszustwo	<input type="checkbox"/>
Kserokopiarka	<input type="checkbox"/>	Nieautoryzowany dostęp	<input type="checkbox"/>
Hardware komputerowy	<input type="checkbox"/>	Klienci	<input type="checkbox"/>
E-mail	<input type="checkbox"/>	Osoby trzecie	<input type="checkbox"/>
Pobranie z Internetu	<input type="checkbox"/>	Prawo autorskie	<input type="checkbox"/>
Wirus	<input type="checkbox"/>	Inne (proszę wskazać poniżej)	<input type="checkbox"/>

  

Czy zgłosiłeś Naruszenie: <i>(proszę zaznaczyć właściwe)</i>		T	N
Przełożony – Organy wykonawcze – Szef działu IT – Audytor wewnętrzny – Inny <i>(proszę wskazać poniżej)</i>		<input type="checkbox"/>	<input type="checkbox"/>

  

Dane kontaktowe na wypadek potrzeby uzyskania dalszych informacji lub wyjaśnień <i>(nazwisko, stanowisko, e-mail, telefon)</i>	
--	--

Podpis osoby upoważnionej przez Przetwarzającego Dane:	Data:
--	-------

#### **ZAŁĄCZNIK IV DO UMOWY DPA**

**Lista podmiotów, którym ..... (Wpisać dane wykonawcy) powierza przetwarzanie danych osobowych**

**Nazwa firmy/instytucji:**

**Adres:**

**Czy zawarto umowę dalszego powierzenia? TAK/NIE**

**Czy dalsza umowa powierzenia pozwala Procesorowi na powierzenie danych w zakresie wskazanym w niniejszej Umowie? TAK/NIE**

**Cel przetwarzania (przedmiot współpracy): (opis).**

## SOFTWARE LICENSE AGREEMENT

This SOFTWARE LICENSE AGREEMENT, (this “**Agreement**”), is made and entered into as of \_\_\_\_\_ (“**Effective Date**”)

by and between **Zoho Corporation B.V.** having its principal place of business at Churchilllaan 11, 3527 GV Utrecht, the

Netherlands including its holding company Zoho Corporation Pvt. Ltd. and affiliates (together hereinafter “Zoho”) and

\_\_\_\_\_, a \_\_\_\_\_ having its principal place of business at \_\_\_\_\_

\_\_\_\_ (“**Licensee**”)

### **1. License Grant:**

**Perpetual License:** Upon payment of the applicable license fees, Zoho grants Licensee a non-exclusive, non-transferable,

perpetual, world-wide license to Use the software products specified in Exhibit A (“**Licensed Software**”) including user

documentation that Licensee has downloaded from or received on media provided by Zoho, including all updates, where

applicable, provided that such access and Use of the Licensed Software is in accordance with the Single Installation

License granted by Zoho. Minor Releases and major releases to the Licensed Software will be provided as part of

maintenance and support. “Use” means installing, executing or displaying the Licensed Software. “Single Installation

License” means that license keys provided to Licensee shall not be used for more than one concurrent Use.

**Subscription License:** Upon payment of the applicable License Fees, Zoho grants Licensee a non-exclusive, nontransferable, world-wide license to Use the Licensed Software including user documentation that Licensee has

downloaded or received on media provided by Zoho, including all updates, where applicable, provided that such access

and Use of the Licensed Software is in accordance with the Single Installation License granted by Zoho. “Use” means

storing, locating, installing, executing or displaying the Licensed Software. “Single Installation License” means that the

license keys provided shall not be used for more than one concurrent Use.

Under the Subscription License, the Licensed Software is licensed only for the period of subscription

(“**Subscription**

**Period**”). If Licensee does not renew the Subscription beyond the Subscription Period, Licensee agrees to stop using the

software and remove the software from Licensee’s systems.

To continue using the Licensed Software beyond the Subscription Period, Licensee must renew the license at least 10

days before the expiry of the Subscription Period. As part of the Subscription License, all updates, upgrades, email

support for problem reporting and online access to product documentation to the Licensed Software will be provided to

Licensee at no additional cost during the Subscription Period.

**2. Third Party Products:** The Licensed Software may contain software which originated with third party vendors and without

limiting the general applicability of the other provisions of this Agreement, Licensee agrees that (a) the title to any third party

software incorporated in the Licensed Software shall remain with the third party which supplied the same; and

(b) Licensee will not distribute any such third party software available with the Licensed Software, unless the license terms of such third

party software provide otherwise.

**3. Restrictions on Use:** In addition to all other terms and conditions of this Agreement, Licensee shall not:

- |      |  |
|------|--|
| (i)  | install one copy of the Licensed Software on more than one server or machine;                          |
| (ii) | remove any copyright, trademark or other proprietary notices from the Licensed Software or its copies; |

(iii)	make any copies except for one back-up or archival copy, for temporary emergency purpose;
(iv)	rent, lease, license, sublicense or distribute the Licensed Software or any portions of it on a standalone basis or as part of Licensee's application; modify or enhance the Licensed Software; decompile or disassemble the Licensed Software. allow any third parties to access, use or support the Licensed Software except employees, contractors, consultants or other third parties engaged by Licensee to do any of the foregoing on behalf of or for the benefit of Licensee.
(v)	
(vi)	
(vii)	

#### **4. Technical Support:**

Perpetual License: Upon payment of annual maintenance and support fee, Zoho provides support that includes email

support for problem reporting, product updates, and online access to product documentation.

Subscription License: Zoho provides support that includes email support for problem reporting, product upgrades, updates,

and online access to product documentation during the Subscription Period.

**5. Ownership and Intellectual Property:** Zoho either owns all right, title and interest in and to the Licensed Software or is

authorized to distribute the Licensed Software under the terms of this Agreement. Zoho expressly reserves all rights not

granted to Licensee herein, notwithstanding the right to discontinue or not to release any Licensed Software and to alter

prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or characteristics

of the Licensed Software. The Licensed Software is only licensed and not sold to Licensee by Zoho.

**6. Audit:** Zoho has the right to audit Licensee's Use of the Licensed Software by providing at least seven (7) days prior written

notice of its intention to conduct such an audit at Licensee's facilities during normal business hours.

**7. Confidentiality:** The Licensed Software contains proprietary information of Zoho and Licensee hereby agrees to take all

reasonable efforts to maintain the confidentiality of the Licensed Software. Licensee agrees to reasonably communicate the

terms and conditions of this Agreement to those persons employed by Licensee who come into contact with or access the

Licensed Software, and to use reasonable efforts to ensure their compliance with such terms and conditions, including but

not limited to, not knowingly permitting such persons to use any portion of the Licensed Software for a purpose that is not

allowed under this Agreement.

**8. Warranty Disclaimer:** Zoho does not warrant that the Licensed Software will be error-free. Subject to applicable laws and

except as provided herein, the Licensed Software is furnished "as is" without warranty of any kind, including the warranties

of merchantability and fitness for a particular purpose and without warranty as to the performance or results Licensee may

obtain by using the Licensed Software. Licensee is solely responsible for determining the appropriateness of using the

Licensed Software and assumes all risks associated with the use of it, including but not limited to the risks of program

errors, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

**9. Limitation of Liability:** In no event will either party be liable to the other or to any third party for any special, incidental,

indirect, punitive or exemplary or consequential damages, or damages for loss of business, loss of profits,

business interruption, or loss of business information arising under this Agreement even if such party has been advised of the possibility of such damages. To the extent permitted by applicable laws, Zoho's entire liability with respect to its obligations under this agreement or otherwise with respect to the Licensed Software shall not exceed the amounts paid by the Licensee to Zoho in previous 12 months preceding the initiation of such claim.

**10. Indemnification:** Zoho agrees to indemnify and defend Licensee from and against any and all claims, actions or proceedings, arising out of any claim that the Licensed Software infringes or violates any valid U.S. patent, copyright or trade secret right of any third party; so long as Licensee provides; (i) prompt written notice to Zoho of such claim; (ii) cooperate with Zoho in the defense and/or settlement thereof, at Zoho's expense; and, (iii) allow Zoho to control the defense and all related settlement negotiations. The above is Zoho's sole obligation to Licensee and shall be Licensee's sole and exclusive remedy pursuant to this Agreement for intellectual property infringement. Zoho shall have no indemnity obligation for claims of infringement to the extent resulting or alleged to result from (i) any combination, operation, or use of the Licensed software with any programs or equipment not supplied by Zoho; (ii) any modification of the Licensed Software by a party other than Zoho; and (iii) Licensee's failure, within a reasonable time frame, to implement any replacement or modification of Licensed Software provided by Zoho.

**11. Termination:** This Agreement is effective until terminated by either party. Licensee may terminate this Agreement at any time by destroying or returning to Zoho all copies of the Licensed Software in Licensee's possession. Zoho may terminate this Agreement in the event that Licensee is in breach of any of the terms of this Agreement and does not cure such breach after thirty (30) days advance written notice. Upon termination, Licensee shall destroy or return to Zoho all copies of the Licensed Software and certify in writing that all known copies have been destroyed. All provisions relating to confidentiality, proprietary rights, non-disclosure, and limitation of liability shall survive the termination of this Agreement.

**12. General:** This Agreement shall be construed, interpreted and governed by the laws of the Netherlands exclusive of its conflicts of law provisions. The parties irrevocably submit to the jurisdiction of Amsterdam and waive any claim in respect of inconvenience thereof. This Agreement constitutes the entire agreement between the parties, and supersedes all prior communications, understandings or agreements between the parties. Any waiver or modification of this Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this Agreement is found invalid or unenforceable, the remainder shall be interpreted so as to reasonably effect the intention of the parties. Licensee shall not export the Licensed Software or Licensee's application containing the Licensed Software except in compliance with United States export regulations and applicable laws and regulations.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representatives as of the Effective Date.

**ZOHO CORPORATION B.V. LICENSEE**

Sign: \_\_\_\_\_ Sign: \_\_\_\_\_

Name: \_\_\_\_\_ Name: \_\_\_\_\_  
Title: \_\_\_\_\_ Title: \_\_\_\_\_  
Churchillaan 11, 3527 GV Utrecht, the Netherlands  
v1.0 Aug 2018 Confidential Page 5 of 5



**EXHIBIT A**

**Software licensed under Subscription/Perpetual License.**



Churchillaan 11, 3527 GV Utrecht, the Netherlands

*Tłumaczenie uwierzytelnione z języka angielskiego*

## UMOWA LICENCYJNA NA OPROGRAMOWANIE

Niniejsza UMOWA LICENCYJNA NA OPROGRAMOWANIE, (zwana "Umową") została zawarta oraz wchodzi w życie z dniem \_\_\_\_\_ ("Dzień Wejście w Życie") przez i pomiędzy Zoho Corporation B.V., której głównym miejscem prowadzenia działalności jest Churchillaan 11, 3527 GV Utrecht, Holandia, w tym jej spółka holdingowa Zoho Corporation Pvt. Ltd. oraz podmioty powiązane (zwane dalej łącznie "Zoho") oraz \_\_\_\_\_ mająca swoje główne miejsce prowadzenia działalności gospodarczej w \_\_\_\_\_ ("Licencjodawca"),

### 1. Udzielenie Licencji:

Licencja Wieczysta: W chwili dokonania płatności odpowiednich opłat licencyjnych, Zoho udziela Licencjodawcy niewyłącznej, niezbywalnej, wieczystej Licencji na cały świat na Używanie produktów oprogramowania określonych w Załączniku A ("Oprogramowanie Licencjonowane") łącznie z dokumentacją użytkownika, którą Licencjodawca pobrał z lub otrzymał na środki przekazu dostarczone przez Zoho, łącznie ze wszystkimi aktualizacjami, jeśli mają zastosowanie pod warunkiem, że taki dostęp oraz Użytkowanie Licencjonowanego Oprogramowania jest zgodne z Pojedynczą Licencją Instalacyjną oraz głównymi wersjami do Licencjonowanego Oprogramowania, które zostaną dostarczone jako część usług konserwacyjnych i serwisowych. "Użytkowanie" oznacza instalowanie, wykonanie lub wyświetlanie Licencjonowanego Oprogramowania. "Pojedyncza Licencja Instalacyjna" oznacza, że klucze licencyjne dostarczone Licencjodawcy nie będą używane w przypadku więcej niż pojedynczego Użycia.

Subskrypcja Licencji: W chwili dokonania płatności odpowiednich Opłat Licencyjnych, Zoho udziela niewyłącznej, niezbywalnej licencji na cały świat na Użytkowanie Licencjonowanego Oprogramowania łącznie z dokumentacją użytkownika, które Licencjodawca pobrał z lub otrzymał na środki dostarczone przez Zoho "Użytkowanie" oznacza składowanie, lokalizowanie, instalowanie, wykonywanie lub wyświetlanie Licencjonowanego Oprogramowania. "Pojedyncza Licencja Instalacyjna" oznacza, że klucze licencji dostarczone nie będą używane w przypadku więcej niż jednego Użycia.

Zgodnie z Subskrypcją Licencji, Licencjonowane Oprogramowanie jest licencjonowane tylko w przypadku okresu subskrypcji ("Okres Subskrypcji"). Jeśli Licencjodawca nie odnawia Subskrypcji poza Okres Subskrypcji, Licencjodawca zgadza się przestać użytkowania oprogramowania oraz usunąć oprogramowanie z systemów Licencjodawcy.

Aby nadal używać Licencjonowanego Oprogramowania poza Okresem Subskrypcji, Licencjodawca musi odnowić licencję na przynajmniej 10 dni przed upływem ważności Okresu Subskrypcji. Częścią Subskrypcji Licencji jest dostarczanie wszelkich aktualizacji, modernizacji, wsparcia email względem zgłoszonego problem oraz dostęp online do dokumentacji produktu Licencjonowanego Oprogramowania bez kosztów dodatkowych w Okresie Subskrypcji.

2. **Produkty Strony Trzeciej:** Licencjonowane Oprogramowanie może zawierać oprogramowanie, które pochodzi od sprzedawców strony trzeciej oraz bez ograniczenia dla zastosowania postanowień niniejszej Umowy, Licencjodawca zgadza się, że (a) tytuł do oprogramowania strony trzeciej ujęty w Licencjonowanym Oprogramowaniu pozostaje u strony trzeciej, która go dostarczyła; oraz (b) Licencjodawca nie będzie rozprowadzał takiego oprogramowania strony trzeciej dostępnego z Oprogramowaniem Licencjonowanym chyba że, warunki licencji oprogramowania takiej strony trzeciej stanowią inaczej.
3. **Ograniczenia Użytkowania:** Poza wszelkimi innymi warunkami Umowy, Licencjodawca nie:
- (i) zainstaluje kopii Licencjonowanego Oprogramowania na więcej niż jednym serwerze lub urządzeniu;
  - (ii) usunie prawa autorskiego, znaku handlowego lub innych oznaczeń zastrzeżonych z Licencjonowanego Oprogramowania, ani jego kopii;
  - (iii) dokona kopii z wyjątkiem jednej kopii zapasowej lub archiwalnej, dla tymczasowych celów awaryjnych;



*[Handwritten signature]*



- (iv) pożyczy, wydzierżawi, udzieli licencję, podlicencję lub rozprowadzi Licencjonowane Oprogramowanie lub jakiegokolwiek jego części na zasadzie standardowej lub w ramach stosowania Licencjodawcy
- (v) zmodyfikuje, ani nie zwiększy Oprogramowania Licencjonowanego;
- (vi) zdekompiluje, ani nie zdemontuje Licencjonowanego Oprogramowania.
- (vii) Pozwoli osobom na trzeci na dostęp, użytkowanie oraz wspomaganie Licencjonowanego Oprogramowania z wyjątkiem pracowników, wykonawców, konsultantów lub innych osób trzecich zaangażowanych przez Licencjodawcę do wykonywania czegokolwiek z powyższych czynności w imieniu lub na korzyść Licencjodawcy.

#### 4. Wsparcie Techniczne:

Licencja Wieczysta: W chwili dokonania płatności rocznej opłaty konserwacyjnej, Zoho dostarczy wsparcie, które będzie obejmowało wsparcie dla zgłoszonego problemu aktualizacji produktu oraz dostępu online do dokumentacji produktu.

Subskrypcja Licencji: Zoho dostarczy wsparcie, które będzie obejmowało wsparcie drogą mailową dla zgłoszonego problemu, aktualizacji produktu oraz dostępu online do dokumentacji produktu w Okresie Subskrypcji.

- 5. **Własność i Własność Intelektualna:** Zoho posiada wszystkie prawa, tytuły oraz udziały w Licencjonowanym Oprogramowaniu lub jest upoważniona do dystrybucji oprogramowania Licencjonowanego. Zoho wyraźnie zastrzega wszystkie prawa nie udzielone Licencjodawcy, bez względu na prawo do przerwania lub nie wydawania Licencjonowanego Oprogramowania oraz do zmiany cen, cech, specyfikacji, możliwości, funkcji, warunków licencji, dat wydawania, ogólnej dostępności lub cech Licencjonowanego Oprogramowania. Licencjonowane Oprogramowanie podlega licencji i nie będzie sprzedawane Licencjodawcy przez Zoho
- 6. **Audyt:** Zoho posiada prawo do audytu Użytkowania przez Licencjodawcę Licencjonowanego Oprogramowania dostarczając co najmniej siedmiodniowe (7) uprzednie zawiadomienie o zamiarze przeprowadzenia takiego audytu w obiekcie Licencjodawcy podczas normalnych godzin roboczych.
- 7. **Poufność:** Licencjonowane Oprogramowanie zawiera informacje zastrzeżone Zoho, i Licencjodawca niniejszym wyraża zgodę na podjęcie wszelkich racjonalnych starań w celu zachowania poufności Oprogramowania Licencjonowanego. Licencjodawca zgadza się w sposób uzasadniony przekazywać warunki Umowy osobom zatrudnionym przez Licencjodawcę, które mają kontakt lub ma dostęp do Licencjonowanego Oprogramowania oraz zgadza się podjąć wszelkie wysiłki w celu zapewnienia zgodności z takimi warunkami, łącznie z, ale nie tylko, nie pozwoli świadomie takim osobom na korzystanie z jakiegokolwiek części Licencjonowanego Oprogramowania w celu, który nie jest dozwolony niniejszą Umową.
- 8. **Zrzeczenie się:** Zoho nie gwarantuje, że Licencjonowane Oprogramowanie będzie wolne od wad. Zgodnie z obowiązującym prawem oraz zgodnie z wyjątkami określonymi niniejszym, Licencjonowane Oprogramowanie zostanie dostarczone "tak jak jest" bez rękojmi jakiegokolwiek rodzaju, łącznie z rękojmiami przydatności do celu co do wykonania oraz wyników, jakie Licencjodawca może uzyskać poprzez korzystanie z Licencjonowanego Oprogramowania. Licencjodawca jest wyłącznie odpowiedzialny za określenie przydatności w użytkowaniu Licencjonowanego Oprogramowania oraz przyjmuje wszelkie ryzyko związane z jego użytkowaniem, łącznie z, ale nie tylko ryzykiem błędów w programie, szkody lub utraty danych, programów lub sprzętu oraz braku dostępności lub zakłóceń w działaniu.
- 9. **Ograniczenie Odpowiedzialności:** W przypadku gdy którakolwiek ze stron będzie odpowiedzialna względem drugiej lub osoby trzeciej za szkody specjalne, przypadkowe, pośrednie, wtórne lub przykładowe lub szkody z tytułu utraty działalności, zysków, zakłócenia w prowadzenia działalności lub utrata informacji biznesowych wynikająca z niniejszej Umowy nawet, jeśli taka strona została poinformowana o możliwości powstania takich szkód. W zakresie dozwolonym prawem, całkowita odpowiedzialność Zoho w odniesieniu do zobowiązań wynikających z niniejszej umowy lub w inny sposób w odniesieniu do Oprogramowania Objętego Licencją nie przekracza kwot zapłaconych przez Licencjodawcę na rzecz Zoho w ciągu ostatnich 12 miesięcy poprzedzających wniesienie takiego roszczenia.



*[Handwritten signature]*



**10. Odszkodowanie:** Zoho zgadza się nie narazić na szkodę Licencjobiorcę względem szkód z tytułu roszczeń, działań lub postępowań, wynikających z takiego roszczenia, w ramach których Licencjonowane Oprogramowanie narusza patenty USA, prawa autorskie lub tajemnice handlowe osoby trzeciej; o ile Licencjobiorca; (i) dostarczy niezwłoczne pisemne zawiadomienie do Zoho o takim roszczeniu; (ii) będzie współpracował z Zoho W ramach obrony oraz/lub uregulowania roszczenia, na koszt Zoho; oraz (iii) pozwoli Zoho sprawowania kontroli nad obroną i wszystkimi związanymi z nią negocjacjami ugodowymi. Powyższe jest wyłącznym obowiązkiem Zoho wobec Licencjobiorcy i będzie wyłącznym środkiem naprawczym zgodnie z niniejszą Umową za naruszenie własności intelektualnej.

Zoho nie ma obowiązku odszkodowawczego za naruszenie w zakresie wynikającym z lub w sposób domniemany wynikający z (i) połączenia, działania lub użytkowania Licencjonowanego Oprogramowania z jakimkolwiek programami, sprzętem nie dostarczonym przez Zoho; (ii) jakichkolwiek modyfikacji Licencjonowanego Oprogramowania przez stronę inną niż Zoho; oraz (iii) niewdrożenia przez Licencjobiorcę zmiany lub wymiennika Licencjonowanego Oprogramowania dostarczonego przez Zoho

**11. Rozwiązanie:** Niniejsza Umowa jest skuteczna do chwili rozwiązania przez którąkolwiek stronę. Licencjobiorca może rozwiązać niniejszą Umowę w każdym czasie poprzez zniszczenie lub zwrot na rzecz Zoho wszystkich kopii Licencjonowanego Oprogramowania znajdujących się w posiadaniu Licencjobiorcy. Zoho może rozwiązać niniejszą Umowę w przypadku, gdy Licencjobiorca narusza jakiegokolwiek warunki niniejszej Umowy i nie naprawi takiego naruszenia w ciągu trzydziestu (30) dni od pisemnego zawiadomienia. Po rozwiązaniu umowy Licencjobiorca zniszczy lub zwróci Zoho wszystkie kopie Oprogramowania objętego Licencją i potwierdzi na piśmie, że wszystkie znane kopie zostały zniszczone.

Wszystkie postanowienia dotyczące poufności, praw własności, nieujawniania i ograniczenia odpowiedzialności pozostaną w mocy po rozwiązaniu niniejszej Umowy.

**12. Postanowienia Ogólne:** Niniejsza Umowa będzie interpretowana i będzie podlegała prawu Holandii, bez sprzeczności z prawem. Strony nieodwołalnie poddają się jurysdykcji Amsterdamu i zrzekają się wszelkich roszczeń w tym względzie. Niniejsza Umowa stanowi całkowite porozumienie pomiędzy jej stronami i zastępuje wszelkie uprzednie ustalenia, porozumienia oraz umowy pomiędzy stronami. Wszelkie zrzeczenie się lub modyfikacja Umowy będzie skuteczna tylko w formie pisemnej, podpisanej przez obie strony. Jeśli jakakolwiek część niniejszej Umowy okaże się nieważna lub niewykonalna, nie będzie miało to wpływu na pozostałą część Umowy. Licencjobiorca nie będzie eksportował Licencjonowanego Oprogramowania lub aplikacji Licencjobiorcy zawierającej Licencjonowane Oprogramowanie z wyjątkiem przypadków zgodnych z przepisami eksportowymi USA oraz obowiązującym prawem.

W DOWÓD POWYŻSZEGO, strony podpisały niniejszą Umowę w ramach swoich upoważnionych przedstawicieli na Dzień Wejścia jej w Życie.

**ZOHO Corporation Private Limited**

Podpis: \_\_\_\_\_

Nazwisko: \_\_\_\_\_

Stanowisko: \_\_\_\_\_

**LICENCJOBORCA**

Podpis: \_\_\_\_\_

Nazwisko: \_\_\_\_\_

Stanowisko: \_\_\_\_\_



*[Handwritten signature]*

Załącznik A

Oprogramowanie licencjonowane w ramach Subskrypcji Licencji

Ja, Małgorzata Truszyńska, Tłumacz Przysięgły Języka Angielskiego, o numerze w rejestrze Ministerstwa Sprawiedliwości TP/1690/06, niniejszym potwierdzam zgodność niniejszego tłumaczenia z przedstawionym dokumentem.

Nr Rep. 246/10/2019

Dnia 29.10.2019

Pobrano opłatę za 10 stron.



*Małgorzata Truszyńska*

## **DATA PROCESSING ADDENDUM**

This Data Processing Addendum ("**DPA**") is made effective as of \_\_\_\_\_ between the parties listed in Annex I of Schedule 1 (each a "**Party**").

(A) The Parties have entered into an agreement for the provision of services by Zoho under the online terms of service or other electronically/physically signed service agreement (the appropriate one, hereinafter "**Service Agreement**").

(B) The Parties acknowledge that, during the provision of services, personal data will be processed by Zoho. Accordingly, the Parties enter into this DPA for the purposes and scope mentioned under Clause 1 of the Schedule 1.

(C) This DPA includes the Schedule(s) and Annexures. Any reference to this DPA includes reference to the Schedule(s) and Annexures.

### **PARTIES HEREBY AGREE AS FOLLOWS:**

**1. Instructions:** For the purposes of Clause 7.1 of the Schedule 1, Customer agrees that its instructions to Zoho for processing personal data are:

- a.** to process such data strictly in accordance with the Service Agreement and this DPA;
- b.** to process data where such processing is initiated by Customer via the user interface of the Zoho services;
- c.** to process data for fraud prevention, spam filtering, and service improvement, including automation; and
- d.** to process data to comply with other documented reasonable instructions provided by Customer (eg., via email) where such instructions are consistent with the Service Agreement and this DPA.

**2. Documentation and Compliance:** For the purposes of Clause 7.6 of the Schedule 1:

**2.1 Demonstration of Compliance.** Upon request by Customer, Zoho will demonstrate its compliance with GDPR and this DPA by way of reports of audits conducted in the previous 12 months by qualified and independent third party auditors, certifications approved under Article 42 of the GDPR, or approved code(s) of conduct as specified under the GDPR.

**2.2 Right to Audit.** Customer shall have a right to audit Zoho's data processing facilities, practices and procedures against GDPR and this DPA, provided that:

- (i) Customer shall, in the first instance, always try to obtain the required information by requesting from Zoho information specified under section 2.1;
- (ii) where information provided by Zoho is not sufficient to demonstrate compliance with GDPR and this DPA, Customer:
  - (a) shall objectively demonstrate the insufficiency by enumerating the specific obligations under GDPR and/or this DPA that are not addressed by the information provided by Zoho under section 2.1 ("Possible Compliance Gap"); and
  - (b) may audit Zoho's data processing facilities, practices and procedures according to the audit procedure in section 2.3; and

(iii) Customer shall reimburse Zoho for any time expended for the audit at Zoho's then-current professional services rates, which shall be made available to Customer upon request.

**2.3 Audit Procedure.** The procedure for audit is agreed as follows:

(i) A reasonably specific and detailed audit plan for the Possible Compliance Gap, the proposed audit date and the duration of the audit shall be communicated to Zoho according to the notice procedure at least 30 days prior to the proposed audit date.

(ii) Zoho shall review the proposed audit plan and provide Customer with any concerns or questions along with an estimate of the charges as specified under clause (iii) of section 2.2 based on the proposed duration of audit. Zoho shall cooperate with Customer to agree on a final audit plan.

(iii) The audit shall be performed only by individuals that have an appropriate level of expertise and qualification in the subject matter to perform the audit.

(iv) The audit shall be conducted during regular business hours at the applicable data processing facility, subject to the agreed final audit plan and Zoho's privacy, security and safety or other relevant policies and without unreasonably interfering with Zoho's business activities or compromising the security of Zoho's own data or other customers' data.

(v) Customer shall require the auditor to share the draft audit report to Zoho for review and incorporate reasonable changes suggested by Zoho.

(vi) Upon completion of the audit, Customer will promptly provide Zoho with a copy of the audit report.

## **2.4 Confidentiality of Information Exchanged.**

(i) Customer acknowledges that all documents and information disclosed by Zoho under section 2.1, 2.2 and 2.3 and all interactions between the parties to the extent such interactions contain information about Zoho's systems and practices, including information observed or learnt by the auditor during audit and the draft and final reports ("Audit Information"), constitute Zoho's confidential information. Customer understands that unauthorized access, use or disclosure of Audit Information may cause irreparable injury to Zoho. Accordingly, Customer agrees to take, and to require the auditor engaged by Customer to take, reasonable measures to protect the confidentiality of the Audit Information from unauthorized access, use or disclosure.

(ii) Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements or confirming compliance with the requirements of this Data Processing Agreement by Zoho.

**2.5 Consequences of Material Non-Compliance.** In the event the audit reveals a material non-compliance by Zoho, Customer will not be required to pay the charges specified under clause (iii) of section 2.2 and Zoho shall reimburse the cost incurred by Customer for engaging the auditor for the audit.

## **2.6 Role of Parties**

Where the Customer acts as the Controller of the personal data, Zoho will be a processor of such data; where the Customer is by itself a Processor of the personal data acting on behalf of its group entities, Zoho will be a sub-processor of such personal data.

The Parties agree that the Customer will be Zoho's sole point of contact and Zoho shall process the personal data solely as per Customer's Instructions as described in section 1

Customer shall ensure that its instructions to Zoho are in consonance with the instructions of the Controller.



### **3. Use of Sub-processors**

For the purposes of Clause 7.7 of the Schedule 1:

- a. The agreed list of sub-processor is published by Zoho on its websites. Customer may request Zoho for relevant information on processing by such sub-processors. Zoho shall, upon such request, make the information available to Customer.
- b. Changes to the agreed sub-processor list (whether addition or replacement of a sub-processor), which apply to Customer's then current use of the service, will be communicated to Customer by email. Upon notification regarding such change by Zoho, Customer shall notify Zoho of its objection (if any) to processing by a sub-processor engaged by Zoho, in writing, within 10 business days from the date of Zoho's notice. Customer may also object in writing to processing by a sub-processor at any time during the term of Service Agreement.
- c. If Customer objects to processing by a sub-processor (as permitted by Clause 7.7 of the Schedule 1 and section 3b), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the services to avoid processing of personal data by the sub-processor. If Customer is not satisfied with the changes suggested by Zoho, Customer may, upon written notice to Zoho, terminate the Service Agreement. In the event of such termination, Zoho will refund Customer on a pro-rata basis any amounts paid by Customer for use of the service.

### **4. Third Parties**

**4.1** In addition to sub-processors, Zoho has Customer's general authorisation for the engagement of third party service providers from the agreed list published by Zoho on its websites for providing: (a) specific functionalities of Zoho services; and (b) certain essential functions such as fraud detection, spam filtering and improvement of services ("**Third Parties**").

**4.2** Customer may request Zoho for relevant information on processing by such Third Parties. Zoho shall, upon such request, make the information available to Customer.

**4.3** Changes to the agreed list (whether addition or replacement of a Third Party), which apply to Customer's then current processing of personal data, will be communicated to Customer by email. Upon notification regarding such change by Zoho, Customer shall notify Zoho of its objection (if any) to processing by a Third Party, in writing, within 10 business days from the date of Zoho's notice. Customer may also object in writing to processing by a Third Party at any time during the term of Service Agreement.

**4.4** If Customer objects to processing by a Third Party (as permitted by section 4.3), Zoho will recommend to Customer commercially reasonable changes in the configuration or use of the services to avoid processing of personal data by the Third Party. If Customer is not satisfied with the changes suggested by Zoho, Customer may, upon written notice to Zoho, terminate the Service Agreement. In the event of such termination, Zoho will refund Customer on a pro-rata basis any amounts paid by Customer for use of the service.

## **5. International Transfers**

**5.1** For the purposes of Clause 7.8, Customer understands that personal data; (i) will be stored in Zoho's data centers in the European Economic Area (EEA); (ii) may be accessed on a need basis by applicable Zoho group entities as described in Schedule 2; and (iii) will be transferred outside EEA to the sub-processors and Third Parties depending on the Zoho services used by Customer. Customer agrees that such transfers of personal data are necessary for providing the services and will be deemed as instructions by Customer.

**5.2** Where Zoho transfers personal data to Zoho group entities, sub-processors, or Third Parties located outside EEA, Zoho shall ensure that a valid basis of transfer as required by GDPR is in place.

## **6. Data Subject Requests**

**6.1** For the purposes of Clause 8(a), Customer authorizes Zoho to respond to the requests from data subjects before notifying Customer, to determine if the request is with respect to the personal data processed by Zoho on behalf of the Customer.

**6.2** For the purposes of Clause 8(b), Zoho shall implement technical and organizational measures to enable Customer to comply with requests from data subjects who wish to exercise their rights such as right to restrict processing, right to erasure, right to rectification, right to access, right not to be subject to an automated individual decision making or data portability. Where Customer requests Zoho's assistance (under this section and Clause 8) and Zoho has already enabled

Customer to comply with such requests by implementing appropriate technical and organizational measures, Zoho shall have the right to charge the Customer for any reasonable costs or expenses incurred by Zoho in order to assist Customer with request(s) from data subjects.

## **7. Other Assistance to the Controller**

**7.1** For the purposes of Clause 8(c), Parties agree that Zoho's obligation to assist Customer in its obligation to (i) conduct a data protection impact assessment; and (ii) consult the competent supervisory authority/ies, is limited to providing the relevant information to Customer.

**7.2** For the purposes of Clause 9.1, Parties agree that Zoho's obligation to assist the Customer in notifying the supervisory authority and in notifying the data subjects is limited to: (i) the extent such breach involves personal data processed by Zoho on behalf of the Customer; and (ii) providing relevant information about the breach to Customer, if such information is available to Zoho and otherwise not available to Customer.

## **8. Return and Deletion of Data**

For the Purposes of Clause 10(d), Customer acknowledges and agrees that:

- a. Return of personal data processed by Zoho should be achieved via Customer initiating the export of such personal data via the user interface made available by Zoho;
- b. Zoho will automatically delete personal data processed by Zoho at the next routine clean-up cycle from the primary servers (that occurs once in 6 months). The data deleted from primary servers will be deleted from backups 3 months thereafter; and
- c. Zoho will provide confirmation of the completion of the relevant clean-up cycle as certification of deletion of the personal data. Such certificate will be provided only upon request from Customer.

## **9. Governing Law and Jurisdiction**

**9.1** This DPA shall be governed by and construed strictly in accordance with the laws of the Netherlands (excluding the rules governing conflict of laws).

**9.2** Any dispute arising out of or resulting from this Agreement shall be subject to the exclusive jurisdiction of courts in Amsterdam to the exclusion of all other courts.

## **10. DPA to Supersede Prior Agreements**

Parties agree that this DPA will supersede and prevail over all the previous data protection and privacy agreement(s) between Customer and Zoho.

#### **SCHEDULE 1**

## STANDARD CONTRACTUAL CLAUSES

### SECTION I

#### *Clause 1 (Purpose and scope)*

**(a)** The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation/"GDPR").

**(b)** The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of GDPR.

**(c)** These Clauses apply to the processing of personal data as specified in Annex II.

**(d)** Annexes I to IV are an integral part of the Clauses.

**(e)** These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.

**(f)** These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

#### *Clause 2 (Invariability of the Clauses)*

**(a)** The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

**(b)** This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

#### *Clause 3 (Interpretation)*

**(a)** Where these Clauses use the terms defined in GDPR, those terms shall have the same meaning as in the GDPR.

**(b)** These Clauses shall be read and interpreted in the light of the provisions of GDPR.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

#### ***Clause 4 (Hierarchy)***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### ***Clause 5 (Docking clause)***

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

## **SECTION II**

### **OBLIGATIONS OF THE PARTIES**

#### ***Clause 6 (Description of processing(s))***

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

#### ***Clause 7 (Obligations of the Parties)***

##### **7.1. Instructions**

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be

given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

**(b)** The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the GDPR or the applicable Union or Member State data protection provisions.

## **7.2. Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

## **7.3. Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

## **7.4. Security of processing**

**(a)** The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

**(b)** The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

## **7.5. Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

## **7.6. Documentation and compliance**

**(a)** The Parties shall be able to demonstrate compliance with these Clauses.

**(b)** The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

**(c)** The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from GDPR. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

**(d)** The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

**(e)** The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

#### **7.7. Use of sub-processors**

**(a)** The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

**(b)** Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to GDPR.

**(c)** At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.



**(d)** The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

**(e)** The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## **7.8. International transfers**

**(a)** Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of GDPR.

**(b)** The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of GDPR, the processor and the sub-processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of GDPR, provided the conditions for the use of those standard contractual clauses are met.

## ***Clause 8 (Assistance to the controller)***

**(a)** The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by controller.

**(b)** The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

**(c)** In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) The obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) The obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) The obligation in Article 32 of GDPR.

(5) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

### ***Clause 9 (Notification of personal data breach)***

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of GDPR, where applicable, taking into account the nature of processing and the information available to the processor.

#### **9.1 Data breach concerning data processed by the controller**

In the event of personal data breach concerning data processed by the controller, the processor shall assist the controller:

**(a)** In notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

**(b)** In obtaining the following information which, pursuant to Article 33(3) of GDPR, shall be stated in the controller's notification, and must at least include:

(1) The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) The likely consequences of the personal data breach;

(3) The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) In complying, pursuant to Article 34 of GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

## **9.2 Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of GDPR.

## **SECTION III**

### **FINAL PROVISIONS**

#### ***Clause 10 (Non-compliance with the Clauses and termination)***

(a) Without prejudice to any provisions of GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The

processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

**(b)** The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) The processor is in substantial or persistent breach of these Clauses or its obligations under GDPR.

(3) The processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to GDPR.

**(c)** The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

**(d)** Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

## ANNEX I

### List of parties

**Controller(s):** [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer*] ("**Customer**")

Name: \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date \_\_\_\_\_

Contact \_\_\_\_\_

**Processor(s):**

Name: Zoho Corporation B.V ("**Zoho**")

Address: Beneluxlaan 4B, 3527 HT UTRECHT, The Netherlands

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date \_\_\_\_\_

Contact [privacy@eu.zohocorp.com](mailto:privacy@eu.zohocorp.com)

## ANNEX II

### Description of the processing

#### ***Categories of data subjects whose personal data is processed:***

The personal data processed concern the following categories of data subjects:

Zoho may process any data inputted by authorised users of Zoho's online collaboration and management tools. Primarily, this will relate to living individuals who are:

- users who are authorised by Customer to use the services

- employees, agents, contractors, and contacts of the Customer

- prospects, customers and clients, business partners and vendors of the Customer

- advisers and professional experts of the Customer

- employees, agents, contractors, and contacts of the Customer's prospects, customers and clients, business partners, vendor, advisers and professional experts.

#### ***Categories of personal data processed:***

Categories of personal data processed may include, but are not limited to:

- Name, contact details, address

- Employment related data

- Financial information

*Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:*

Zoho provides options to encrypt sensitive data at rest. The ability to encrypt data at rest is different in each Zoho service and it may not be enabled by default. The details of encryption capabilities in Zoho services are either published by Zoho on its websites or available to Customer upon request. Based on the nature of the sensitive personal data processed, Customer shall determine

the suitability or adequacy of encryption capabilities provided by Zoho service(s) and enable encryption.

***Nature of the processing:*** The nature of processing by Zoho will include the provision of Zoho services pursuant to the terms of Service Agreement, this DPA or any other agreement between Customer and Zoho.

***Purpose(s) for which the personal data is processed on behalf of the controller:*** To provide Zoho services in accordance with instructions provided by Customer as described under section 1 of this DPA.

***Duration of the processing:*** Duration of the Service Agreement

*For processing by (sub-) processors, also specify subject matter, nature and duration of the processing:*

As specified under section 3, Sub-processor(s) will process personal data for the duration of the Service Agreement.

### **Annex - III**

**Technical and Organizational Security Measures applicable to Manage Engine Service Desk**

## **Plus**

### **Introduction**

ManageEngine makes IT management solutions that enable IT admins address their IT challenges proactively. We improve our customers' security posture and prioritize their data security and privacy. In this article, we document our security processes at the organizational and product levels.

### **I. Organization security**

We have an Information Security Management System (ISMS) in place which takes in into account our security objectives as well as the risks and mitigation concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

#### **Employee background checks**

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

#### **Security Awareness**

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles. We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

#### **Dedicated security and privacy teams**

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They regulate and maintain defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

#### **Internal audit and compliance**

We have a dedicated compliance team to review procedures and policies in ManageEngine to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards.



This team also does periodic internal audits and facilitates independent audits and assessments by third parties. For more details, check out our [compliance portfolio](#).

### **Endpoint security**

All workstations issued to ManageEngine employees run up-to-date OS versions and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by ManageEngine's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

## **II. Application security**

ServiceDesk Plus is a help desk management platform that includes core help desk and IT management applications and project management, contract management, asset management, CMDB, and features for ITIL (information technology infrastructure library) compliance. ServiceDesk Plus is currently used by various organizations; some of them have installed and configured ServiceDesk Plus within their network whereas few others have installed and configured ServiceDesk Plus to be accessed over the internet. So, any compromise on the security of customer data will expose organizations to serious risks. Therefore, ServiceDesk Plus is designed to offer maximum security at all times, including application installation, user authentication, data transmission, storage, and regular use.

### **Secure by design**

Our Software Development Life Cycle (SDLC) model mandates our ServiceDesk Plus engineering team to strictly adhere to our secure coding standards. In addition, we adhere to security standards across the SDLC process.

#### **Security standard during the analysis and design phase.**

- ❑ Our engineering team gathers and analysis requirements to identify any security flaws and loopholes in new features.
- ❑ Prepares a vulnerability assessment plan to address security concerns posed by users and security analysts in the previous releases/versions.
- ❑ Develops a product or feature prototype, including changes and subjects them to the change management authority for approval.

#### **Security standard during the development phase**

- ❑ The development team follows the security guidelines given by the product security team.
- ❑ The source code is periodically reviewed by the security coordinator and team lead.
- ❑ Before using any third-party code dependencies and libraries, our legal and security teams will verify whether the third party libraries have any known security issues or not.
- ❑ Only authorized engineers can access the source code repository.

- Approval/review process is enabled for modified sources.

### **Security standard during the QA/release phase**

- Performs integration, automation, and penetration tests to ensure that the new features or modules are secure from potential vulnerabilities/flaws.
- Continuous smoke testing to ensure that the core functionality of the product remains intact without opening new security loopholes.
- Generates security assessment reports to identify further areas of improvement.
- Runs continuous vulnerability scans post release for timely identification and patching of vulnerabilities.

### **Security review process**

We have a security team to ensure the released build/product is free from security vulnerabilities. The team will follow the below process during the security review process.

- Runs automated security audit tool on new features.
- Conducts a security audit program for all features and bug fixes.
- Analyze third-party files usage and its known vulnerabilities.
- Collects brief feature/bug fixes details from developers to discover possible vulnerabilities.
- Creates security briefs for both developers and support team to provide instant solution to customers.
- Monitors recently discovered vulnerabilities.
- As a final check, white box testing, i.e. manual source code review, is also carried out by the security team to discover any defects in the build. In this stage, the security team develops test cases to verify the proper working of all functionalities and error handling of the developed feature.
- Once all issues are resolved and a fresh build is created, the security team will approve the build as final.

### **Other security standards**

- Our repository and build infrastructure are secured with SSH/HTTPS protocol and are placed in a secure, segmented network with stricter authentication and access controls.
- Our security and code frameworks are OWASP-compliant and implemented at the application layer.
- All code changes, third-party dependencies, release bundles, and upgrade packs are subject to multiple levels of internal security review, automation, and penetration testing efforts, and vulnerability scans to ensure they are well secured from logical bugs and security issues.
- Every update and new feature in ServiceDesk Plus is subject to internal change management policies and regular vulnerability assessments, and changes are implemented into production only if approved by the concerned change and security management authorities.
- The binaries are signed with a code signing certificate and the private key is securely stored in the segmented network with limited access.

- The ServiceDesk Plus engineering team works closely with internal security teams to obtain their feedback and identify areas of improvement to strengthen our security posture.

Besides the security measures described above, we are continuously striving to make the application more secure. The following section provides comprehensive details about security specifications of ManageEngine ServiceDesk Plus.

### **ServiceDesk Plus: Security specifications**

Refer to the below link to know more about product security specifications.

<https://www.manageengine.com/products/service-desk/servicedesk-plus-security-specifications.html>

## **III. Operational security**

### **Customer data protection in ServiceDesk Plus**

ServiceDesk Plus is an installable product, so all data resides in the customer environment. Therefore, data breach is not possible in the ServiceDesk Plus On Premises version. Only customer's support tickets and log files are stored in our customer support portal.

- The files uploaded by customers are stored securely in a customer support portal.
- The uploaded files are accessible only to authorized support technicians.
- Data uploaded in server will be kept confidential and will be used for debugging purposes only.
- The uploaded files are allowed to download only in specific servers and the server credentials are not shared to anyone.
- The uploaded files will be removed automatically in the following conditions.
  - During ticket closure, we ensure the log & data files are deleted in the server.
  - File uploaded in server will be deleted automatically after 25 days.

### **Build and patching process**

- The ServiceDesk Plus team works closely with the MESRC to run mandatory vulnerability scans and penetration tests before every major release to ensure that latest builds are completely foolproof. In addition, the team runs continuous vulnerability assessments on these builds to ensure that they are free from any new vulnerabilities.
- Users are notified immediately to upgrade to the latest version as and when there is a new security patch or update.
- In the event of a security concern or escalation, users are requested to submit a detailed report on the vulnerability or security bug. Meanwhile, the product team evaluates the validity and risks associated with the bug and prioritizes the release based on its severity.

### **Logging and monitoring**

Product logs certain data for debugging and to prevent any misuse. The log files generated by ServiceDesk Plus are stored in customer machines. A maximum of 50 log files can be stored with the size capped to 10 MB for each file. Once this limit is reached, the log files are rolled over; the older files are removed from user machines. We do not have access to the log files unless the user shares it to avail support services. In this case, only the support staff and development team, limited by their roles, have access to the log files. After the issue is identified, the log files are deleted.

## **Business Continuity**

We have backup power, temperature control systems, and fire-suppression and fire-protection systems to ensure business continuity. Dedicated business continuity plans are present for major operations such as infrastructure management and technical support. We have a well planned business continuity and disaster recovery plan in place to assist us in the event of extended service outages, thereby affecting the services provided to the customers by factors beyond our control e.g., natural calamities, man-made disasters, etc., to resume endpoint management operations to the maximum possible extent within a minimal time frame. The plan encompasses all our internal operations to ensure continued services for our customers. We have three recovery teams namely, the Emergency Management Team (EMT), the Disaster Recovery Team (DRT), and the IT Technical Services (IT) team, in place for better coordination and support among various teams.

## **IV. Incident Management**

### **Reporting**

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will provide you with necessary evidence regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations. We respond to the security or privacy incidents you report to us through [incidents@zohocorp.com](mailto:incidents@zohocorp.com), with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address of the Organization administrator registered with us).

### **Breach Notification**

As data controllers, we notify the concerned Data Protection Authority of a breach within 72 hours after we become aware of it, according to the General Data Protection Regulation (GDPR). Depending on specific requirements, we notify the customers, when necessary.

## **V. Responsible Disclosure**

We have a vulnerability reporting program called "Bug Bounty", which recognizes and rewards the work of security researchers in identifying vulnerabilities. We are committed to working with the community to verify, reproduce, respond, legitimate, and implement appropriate solutions for the reported vulnerabilities. If you happen to find any, please submit the issues at <https://bugbounty.zoho.com>. If you want to report vulnerabilities to us directly, mail us at [support@servicedeskplus.com](mailto:support@servicedeskplus.com)

## **I. Organization security**

We have an Information Security Management System (ISMS) in place which takes into account our security objectives as well as the risks and mitigation concerning all the interested parties.

We

employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

### **Employee background checks**

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

### **Security Awareness**

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles. We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

### **Dedicated security and privacy teams**

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They regulate and maintain defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

### **Internal audit and compliance**

We have a dedicated compliance team to review procedures and policies in ManageEngine to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties.

For more details, check out our [compliance portfolio](#).

### **Endpoint security**

All workstations issued to ManageEngine employees run up-to-date OS versions and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by ManageEngine's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

## **II.Application security**

### **i.Secure by Design**

We adhere to the secure coding guidelines of the Software Development Life Cycle (SDLC) and these guidelines are shared with all developers. As the next step, we screen the code changes to look for potential security issues by first, manually reviewing it, and second, using our code analyzer, and vulnerability scanner tools. This entire process is carried out before the release of any new feature. If any issue is found, they are immediately checked and fixed. Furthermore, a robust security framework, that is based on the OWASP standards, is implemented in the application layer. This framework provides means to mitigate threats such as SQL Injection, Cross-Site Scripting, and Application Layer DoS attacks. To top it all, we conduct regular sessions to educate developers about secure coding practices.

### **ii.Identity and Access control**

#### **●Role-Based Access Control**

Role-Based Access Control allows only authorized users to access a specific function. Users are designated with specific roles and their access to each functionality depends on the permission granted to them.

### **iii.Encryption**

#### **●In transit:**

- Any data transfer from the agent application to the server happens using the strong encryption protocol, HTTPS. Users can set HTTPS as the default protocol for all communication from the web console.
- Users can disable older version of TLS in the server.xml. The support for older version of TLS is provided to enable users to manage their running on older Windows versions. Additionally, TLS 1.2 and strong ciphers are supported for the latest systems.

This ensures that the data is always encrypted during its transfer.

- At rest:** Sensitive data, such as passwords, auth-tokens, and the like, that are stored in databases are encrypted using 256-bit Advanced Encryption Standard (AES).

**Database Protection:** The product database can be accessed only by providing instance-specific credentials and is limited to local host access. The passwords stored are one-way hashed using bcrypt and are filtered from all of our logs. As bcrypt hashing algorithm with per-user-salt is used, it would be exorbitant and heavily time-consuming to reverse engineer the passwords and the database resides in Customer setup only.

### **3.Operational security**

**a.Customer data security:** The customer data resides only in their environment, as the product is an on-premise solution.

**Note:** In case any customer requires help in resolving any issue, we may require the customer's logs. The customer uploads the logs through a secure portal owned by us, that can be accessed only by authorized personnel and grants us permission to access them. The logs will be deleted automatically after five days from the time of upload. In addition to this, any breaches that occur will be notified to the customer.

#### **b.Vulnerability and patch management:**

We have a dedicated vulnerability process that actively scans for security threats or vulnerabilities using a combination of certified third-party scanning tools, and in-house tools. Subsequently, automated and manual testing is performed. Furthermore, the security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to identify security incidents that might affect the company. Once we identify a vulnerability that requires remediation, it is logged, prioritized according to severity, and is assigned an owner. We further identify the associated risks and mitigate them by either patching the vulnerable systems or applying relevant controls.

After assessing the severity of the vulnerability based on the impact analysis, we commit to resolve the issue within our defined SLA. Depending upon the severity, we send the security advisories to all our customers describing the vulnerability, the patch and the steps to be taken by the customer.

#### **c.Business continuity:**

- We have backup power, temperature control systems, and fire-suppression and fire-protection systems to ensure business continuity. Dedicated business continuity plans are present for major operations such as infrastructure management and technical support.



- We have a well planned business continuity and disaster recovery plan in place to assist us in the event of extended service outages, thereby affecting the services provided to the customers by factors beyond our control e.g., natural calamities, man-made disasters, etc., to resume endpoint management operations to the maximum possible extent within a minimal time frame. The plan encompasses all our internal operations that ensures continued services for our customers. We have three recovery teams namely, the Emergency Management Team (EMT), the Disaster Recovery Team (DRT), and the IT Technical Services (IT) team, in place for better coordination and support among various teams.

#### **d.Responsible Disclosure**

A vulnerability reporting program in "Bug Bounty", to reach the community of researchers is in place, which recognizes and rewards the work of security researchers. We are committed to working with the community to verify, reproduce, respond, legitimate, and implement appropriate solutions for the reported vulnerabilities. If you happen to find any, please submit the issues at <https://bugbounty.zoho.com> or mail us at: [opmanager-support@manageengine.com](mailto:opmanager-support@manageengine.com).

#### **e.Customer controls for security**

So far, we have discussed what we do to offer security on various fronts to our customers. Here are the things that you as a customer can do to ensure security from your end:

- Choose a unique and complex password.
- Secure Network shared folders.
- Use trusted third party certificates to ensure secured connections.
- Check for latest patches and update your endpoints regularly.
- <https://www.manageengine.com/network-monitoring/service-packs.html>

## **UMOWA O POWIERZENIE PRZETWARZANIA DANYCH**

Niniejsza Umowa o Powierzenie Przetwarzania Danych („UPD”) wchodzi w życie z dniem \_\_\_\_\_ pomiędzy stronami wymienionymi w Dodatku I do Załącznika nr 1 (z których każda zwana jest dalej „Stroną”).

A) Strony zawarły umowę o świadczenie przez Zoho usług na podstawie zamieszczonych w Internecie warunków świadczenia usług lub inną podpisaną elektronicznie/fizycznie umowę o świadczenie usług (w zależności od przypadku; dalej zwaną „Umową Serwisową”).

B) Strony przyjmują do wiadomości, iż podczas świadczenia usług Zoho będzie przetwarzać dane osobowe. W związku z powyższym Strony zawiefrają niniejszą UPD w celach i w zakresie, o których mowa w Klauzuli 1 Załącznika nr 1.

C) Niniejsza UPD obejmuje Załącznik(i) i Dodatki. Wszelkie odniesienia do niniejszej UPD dotyczą również Załącznika(-ów) i Dodatków.

### **STRONY NINIEJSZYM POSTANAWIAJĄ, CO NASTĘPUJE:**

**1. Polecenia:** Na potrzeby Klauzuli 7.1 Załącznika nr 1 Zamawiający zgadza się, że jego polecenia dla Zoho dotyczące przetwarzania danych osobowych są następujące:

- a. przetwarzanie takich danych w ścisłej zgodności z Umową Serwisową i niniejszą UPD;
- b. przetwarzanie danych w przypadku, gdy takie przetwarzanie jest inicjowane przez Zamawiającego za pośrednictwem interfejsu użytkownika usług Zoho;
- c. przetwarzanie danych do celów zapobiegania oszustwom, filtrowania spamu i ulepszania usług, w tym automatyzacji; oraz
- d. przetwarzanie danych w celu zachowania zgodności z innymi udokumentowanymi, uzasadnionymi poleceniami przekazanymi przez Zamawiającego (np. za pośrednictwem poczty elektronicznej), jeśli takie polecenia są zgodne z Umową Serwisową i niniejszą UPD.

**2. Dokumentacja i zgodność:** Na potrzeby Klauzuli 7.6 Załącznika nr 1:

**2.1 Wykazanie zgodności.** Na żądanie Zamawiającego Zoho wykaże zgodność z RODO i niniejszą UPD w formie raportów z audytów przeprowadzonych w ciągu ostatnich 12 miesięcy przez wykwalifikowanych i niezależnych audytorów będących stronami trzecimi, certyfikatów

zatwierdzonych zgodnie z art. 42 RODO lub zatwierdzonego(-ych) kodeksu(-ów) postępowania określonego(-ych) w RODO.

**2.2 Prawo do audytu.** Zamawiający ma prawo do audytu obiektów, praktyk i procedur przetwarzania danych Zoho pod kątem RODO i niniejszej UPD z zastrzeżeniem, że:

i) Zamawiający zobowiązany jest zawsze w pierwszej kolejności starać się uzyskać wymagane informacje poprzez zwrócenie się do Zoho o informacje określone w punkcie 2.1;

ii) w przypadku, gdy informacje przekazane przez Zoho nie są wystarczające do wykazania zgodności z RODO i niniejszą UPD, Zamawiający:

a) zobowiązany jest w sposób obiektywny wykazać ich niewystarczalność, wymieniając konkretne obowiązki wynikające z RODO i/lub niniejszej UPD, które nie zostały uwzględnione w informacjach przekazanych przez Zoho zgodnie z punktem 2.1 („Ewentualny Brak Zgodności”); oraz

b) może przeprowadzić audyt infrastruktury, praktyk i procedur przetwarzania danych Zoho zgodnie z procedurą audytu opisaną w punkcie 2.3; oraz

iii) Zamawiający zobowiązany jest zrekompensować Zoho wszelki czas poświęcony na audyt zgodnie ze stawkami za usługi profesjonalne Zoho obowiązującymi w danym czasie, które udostępnia się Zamawiającemu na żądanie.

**2.3 Procedura audytu.** Uzgadnia się następującą procedurę audytu:

i) Plan audytu o uzasadnionym poziomie konkretności i szczegółowości dotyczący Ewentualnego Braku Zgodności, proponowany termin audytu oraz czas jego trwania zostaną zakomunikowane Zoho zgodnie z procedurą powiadamiania na co najmniej 30 dni przed proponowanym terminem audytu.

ii) Zoho dokonuje przeglądu proponowanego planu audytu i przekazuje Zamawiającemu wszelkie wątpliwości lub pytania wraz z oszacowaniem opłat zgodnym z podpunktem iii) punktu 2.2, opartym na proponowanym czasie trwania audytu. Zoho współpracuje z Zamawiającym w celu uzgodnienia ostatecznego planu audytu.

iii) Audyt przeprowadzają wyłącznie osoby fizyczne posiadające odpowiedni do przeprowadzenia audytu poziom wiedzy eksperckiej i kwalifikacji w zakresie jego przedmiotu.

iv) Audyt przeprowadza się w normalnych godzinach pracy we właściwym obiekcie przetwarzania danych z zastrzeżeniem uzgodnionego ostatecznego planu audytu oraz polityk dotyczących prywatności, bezpieczeństwa i ochrony Zoho lub innych stosownych polityk, a także bez nieuzasadnionej ingerencji w działalność gospodarczą Zoho i bez narażania bezpieczeństwa własnych danych Zoho lub danych innych klientów.

v) Zamawiający zobowiązuje audytora do udostępnienia Zoho projektu raportu z audytu w celu jego przeglądu oraz do ujęcia uzasadnionych zmian sugerowanych przez Zoho.

vi) Po zakończeniu audytu Zamawiający niezwłocznie przekaze Zoho egzemplarz raportu z audytu.

## **2.4 Poufność wymienianych informacji**

i) Zamawiający przyjmuje do wiadomości, iż wszystkie dokumenty i informacje ujawnione przez Zoho zgodnie z punktami 2.1, 2.2 i 2.3 oraz wszystkie interakcje pomiędzy stronami w zakresie, w jakim takie interakcje obejmują informacje o systemach i praktykach Zoho, w tym informacje uzyskane w wyniku obserwacji lub powzięte przez audytora podczas audytu oraz projekt raportu i raport końcowy („Informacje z Audytu”), stanowią informacje poufne Zoho. Zamawiający rozumie, iż nieuprawniony dostęp, wykorzystanie lub ujawnienie Informacji z Audytu może wyrządzić Zoho nieodwracalne szkody. W związku z tym Zamawiający zobowiązuje się przedsięwziąć uzasadnione środki, a także zobowiązać audytora, z którego usług korzysta Zamawiający, do przedsięwzięcia takich środków, w celu ochrony poufności Informacji z Audytu przed nieuprawnionym dostępem, wykorzystaniem lub ujawnieniem.

ii) Zamawiający może wykorzystywać raporty z audytu wyłącznie na potrzeby spełnienia wymogów swojego audytu regulacyjnego lub potwierdzenia zgodności z wymogami niniejszej Umowy o Powierzenie Przetwarzania Danych ze strony Zoho.

**2.5 Konsekwencje istotnej niezgodności.** W przypadku, gdy audyt ujawni istotną niezgodność ze strony Zoho, Zamawiający nie będzie zobowiązany do uiszczenia opłat określonych w podpunkcie iii) punktu 2.2, a Zoho zwraca koszty poniesione przez Zamawiającego na skorzystanie z usług audytora w celu przeprowadzenia audytu.

## **2.6 Rola Stron**

W przypadku, gdy Zamawiający występuje jako Administrator danych osobowych, Zoho będzie podmiotem przetwarzającym takie dane; w przypadku, gdy Zamawiający sam jest Podmiotem Przetwarzającym dane osobowe działającym w imieniu podmiotów należących do jego grupy, Zoho będzie podmiotem podprzetwarzającym takie dane osobowe.

Strony uzgadniają, iż Zamawiający będzie jedynym punktem kontaktowym Zoho, a także że Zoho przetwarza dane osobowe wyłącznie w sposób zgodny z Poleceniami Zamawiającego opisanymi w punkcie 1.

Zamawiający zobowiązany jest zapewnić zgodność jego poleceń dla Zoho z poleceniami Administratora.

### **3. Korzystanie z usług podmiotów podprzetwarzających**

Na potrzeby Klauzuli 7.7 Załącznika nr 1:

- a. Uzgodniony wykaz podmiotów podprzetwarzających publikowany jest przez Zoho na stronach internetowych Zoho. Zamawiający może zażądać od Zoho stosownych informacji dotyczących przetwarzania przez takie podmioty podprzetwarzające. Na przedmiotowe żądanie Zoho udostępnia informacje Zamawiającemu.
- b. Zmiany w uzgodnionym wykazie podmiotów podprzetwarzających (dodanie lub zastąpienie podmiotu podprzetwarzającego), które dotyczą korzystania z usługi przez Zamawiającego w danym czasie, zostaną zakomunikowane Zamawiającemu pocztą elektroniczną. Po powiadomieniu o takiej zmianie przez Zoho Zamawiający pisemnie powiadamia Zoho o swoim ewentualnym sprzeciwie wobec przetwarzania przez podmiot podprzetwarzający, z którego usług korzysta Zoho, w terminie 10 dni roboczych od daty powiadomienia Zamawiającego przez Zoho. Zamawiający może również wyrazić pisemny sprzeciw wobec przetwarzania przez podmiot podprzetwarzający w dowolnej chwili w okresie obowiązywania Umowy Serwisowej.
- c. Jeśli Zamawiający wyrazi sprzeciw wobec przetwarzania przez podmiot podprzetwarzający (w zakresie dopuszczalnym na mocy Klauzuli 7.7 Załącznika nr 1 i punktu 3b), Zoho zaleci Zamawiającemu uzasadnione pod względem gospodarczym zmiany w konfiguracji lub korzystaniu z usług w celu uniknięcia przetwarzania danych osobowych przez ten podmiot podprzetwarzający. Jeśli Zamawiający nie jest usatysfakcjonowany zmianami sugerowanymi przez Zoho, może on, za pisemnym powiadomieniem Zoho, rozwiązać Umowę Serwisową. W przypadku takiego rozwiązania Umowy Serwisowej Zoho zwróci Zamawiającemu na zasadzie proporcjonalności wszelkie kwoty zapłacone przez niego za korzystanie z usługi.

### **4. Strony Trzecie**

**4.1** Oprócz podmiotów podprzetwarzających Zoho posiada ogólną zgodę Zamawiającego na korzystanie z usług usługodawców będących stronami trzecimi wpisanych do uzgodnionego wykazu, publikowanego przez Zoho na stronach internetowych Zoho, w celu zapewnienia: a) określonych funkcjonalności usług Zoho oraz b) niektórych istotnych funkcji takich, jak wykrywanie oszustw, filtrowanie spamu i ulepszanie usług („**Strony Trzecie**”).

**4.2** Zamawiający może zażądać od Zoho stosownych informacji dotyczących przetwarzania przez takie Strony Trzecie. Na przedmiotowe żądanie Zoho udostępnia informacje Zamawiającemu.

**4.3** Zmiany w uzgodnionym wykazie (dodanie lub zastąpienie Strony Trzeciej), które dotyczą przetwarzania danych osobowych przez Zamawiającego w danym czasie, zostaną zakomunikowane Zamawiającemu pocztą elektroniczną. Po powiadomieniu o takiej zmianie przez Zoho Zamawiający pisemnie powiadamia Zoho o swoim ewentualnym sprzeciwie wobec przetwarzania przez Stronę Trzecią w terminie 10 dni roboczych od daty powiadomienia Zamawiającego przez Zoho. Zamawiający może również wyrazić pisemny sprzeciw wobec przetwarzania przez Stronę Trzecią w dowolnej chwili w okresie obowiązywania Umowy Serwisowej.

**4.4** Jeśli Zamawiający wyrazi sprzeciw wobec przetwarzania przez Stronę Trzecią (w zakresie dopuszczalnym na mocy punktu 4.3), Zoho zaleci Zamawiającemu uzasadnione pod względem gospodarczym zmiany w konfiguracji lub korzystaniu z usług w celu uniknięcia przetwarzania danych osobowych przez tę Stronę Trzecią. Jeśli Zamawiający nie jest usatysfakcjonowany zmianami sugerowanymi przez Zoho, może on, za pisemnym powiadomieniem Zoho, rozwiązać Umowę Serwisową. W przypadku takiego rozwiązania Umowy Serwisowej Zoho zwróci Zamawiającemu na zasadzie proporcjonalności wszelkie kwoty zapłacone przez niego za korzystanie z usługi.

## **5. Międzynarodowe przekazywanie danych**

**5.1** Na potrzeby Klauzuli 7.8 Zamawiający rozumie, że: i) dane osobowe będą przechowywane w centrach danych Zoho w Europejskim Obszarze Gospodarczym (EOG); ii) dostęp do danych osobowych może być w razie potrzeby uzyskiwany przez właściwe podmioty z grupy Zoho, jak określono w Załączniku nr 2; oraz iii) dane osobowe będą przekazywane poza EOG do podmiotów podprzetwarzających i Stron Trzecich w zależności od usług Zoho, z których korzysta Zamawiający. Zamawiający zgadza się, że takie przekazywanie danych osobowych jest niezbędne do świadczenia usług i będzie poczytywane za odbywające się na polecenie Zamawiającego.

**5.2** W przypadku, gdy Zoho przekazuje dane osobowe podmiotom z grupy Zoho, podmiotom podprzetwarzającym lub Stronom Trzecim znajdującym się poza EOG, Zoho zapewnia istnienie ważnej podstawy przekazywania danych wymaganej przez RODO.

## **6. Żądania osoby, której dane dotyczą**

**6.1** Na potrzeby Klauzuli 8 lit. a) Zamawiający upoważnia Zoho do udzielania odpowiedzi na żądania osób, których dane dotyczą, przed powiadomieniem Zamawiającego w celu ustalenia, czy żądanie dotyczy danych osobowych przetwarzanych przez Zoho w imieniu Zamawiającego.

**6.2** Na potrzeby Klauzuli 8 lit. b) Zoho wdraża środki techniczne i organizacyjne w celu umożliwienia Zamawiającemu spełnienia żądań osób, których dane dotyczą, chcących skorzystać ze swoich praw takich, jak prawo do ograniczenia przetwarzania danych osobowych, prawo do ich usunięcia lub sprostowania, prawo dostępu do danych osobowych, prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach lub prawo do przenoszenia danych osobowych. W przypadku, gdy Zamawiający zwróci się o pomoc Zoho (na mocy niniejszego punktu i Klauzuli 8), przy czym spełnienie takich żądań przez Zamawiającego zostało już umożliwione przez Zoho poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, Zoho ma prawo obciążyć Zamawiającego wszelkimi uzasadnionymi kosztami lub wydatkami poniesionymi przez Zoho w celu udzielenia mu pomocy dotyczącej żądania(-ń) od osób, których dane dotyczą.

## **7. Inna pomoc dla administratora**

**7.1** Na potrzeby Klauzuli 8 lit. c) Strony uzgadniają, że obowiązek Zoho dotyczący pomagania Zamawiającemu w zakresie jego obowiązku i) przeprowadzenia oceny skutków dla ochrony danych oraz ii) konsultacji z właściwym(i) organem(-ami) nadzorczym(i) ogranicza się do przekazania Zamawiającemu stosownych informacji.

**7.2** Na potrzeby Klauzuli 9.1 Strony uzgadniają, że obowiązek Zoho dotyczący pomagania Zamawiającemu przy zawiadomieniu organu nadzorczego oraz przy zawiadomieniu osób, których dane dotyczą, ogranicza się do: i) zakresu, w jakim przedmiotowe naruszenie dotyczy danych osobowych przetwarzanych przez Zoho w imieniu Zamawiającego oraz ii) przekazania Zamawiającemu stosownych informacji o naruszeniu, jeżeli takie informacje są dostępne dla Zoho i nie są dostępne w inny sposób dla Zamawiającego.

## **8. Zwrot i usuwanie danych**

Na potrzeby Klauzuli 10 lit. d) Zamawiający przyjmuje do wiadomości i zgadza się, że:

- a.** Zwrot danych osobowych przetwarzanych przez Zoho powinien nastąpić poprzez zainicjowanie przez Zamawiającego eksportu tych danych osobowych za pośrednictwem interfejsu użytkownika udostępnionego przez Zoho;
- b.** Zoho automatycznie usunie dane osobowe przetwarzane przez Zoho z serwerów głównych podczas następnego rutynowego cyklu czyszczenia (który ma miejsce raz

na 6 miesięcy). Dane usunięte z serwerów głównych zostaną usunięte z kopii zapasowych 3 miesiące później; oraz

- c. Zoho poświadczy usunięcie danych osobowych, przekazując potwierdzenie zakończenia stosownego cyklu czyszczenia. Zaświadczenie takie zostanie przekazane wyłącznie na żądanie Zamawiającego.

## **9. Prawo właściwe i właściwość sądu**

**9.1** Niniejsza UPD podlega prawu holenderskiemu i jest interpretowana w ścisłej zgodności z tym prawem (z wyłączeniem norm kolizyjnych).

**9.2** Wyłącznie właściwość w sprawie wszelkich sporów wynikających z niniejszej Umowy mają sądy w Amsterdamie, co wyklucza zarazem właściwość wszystkich innych sądów.

## **10. Zastąpienie wcześniejszych umów przez UPD**

Strony uzgadniają, iż niniejsza UPD zastąpi wszystkie poprzednie umowy pomiędzy Zamawiającym a Zoho dotyczące ochrony danych i prywatności oraz będzie w stosunku do nich nadrzędna.



## **ZAŁĄCZNIK NR 1**

### **STANDARDOWE KLAUZULE UMOWNE**

#### **SEKCJA I**

##### ***Klauzula 1 (Cel i zakres)***

**a)** Celem niniejszych Standardowych Klauzul Umownych (Klauzule) jest zapewnienie przestrzegania art. 28 ust. 3 i 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych/„RODO”).

**b)** Administratorzy i podmioty przetwarzające wymienieni w Dodatku I uzgodnili niniejsze Klauzule w celu zapewnienia przestrzegania art. 28 ust. 3 i 4 RODO.

**c)** Niniejsze Klauzule mają zastosowanie do przetwarzania danych osobowych określonego w Dodatku II.

**d)** Dodatki I do IV stanowią integralną część Klauzul.

**e)** Niniejsze Klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator na mocy RODO.

**f)** Niniejsze Klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V RODO.

##### ***Klauzula 2 (Niezmienność Klauzul)***

**a)** Strony zobowiązują się nie zmieniać Klauzul z wyjątkiem dodawania informacji do Dodatków lub aktualizowania zawartych w nich informacji.

**b)** Postanowienie to nie uniemożliwia Stronom umieszczania standardowych klauzul umownych określonych w niniejszych Klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie będą one bezpośrednio lub pośrednio sprzeczne z Klauzulami ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

##### ***Klauzula 3 (Wykładnia)***

a) Jeżeli w niniejszych Klauzulach użyto terminów zdefiniowanych w RODO, terminy te mają takie samo znaczenie jak w RODO.

b) Niniejsze Klauzule odczytuje się i interpretuje w świetle przepisów RODO.

c) Niniejszych Klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w RODO ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

#### ***Klauzula 4 (Hierarchia)***

W razie sprzeczności między niniejszymi Klauzulami a postanowieniami powiązanych umów między Stronami istniejących w chwili uzgodnienia niniejszych Klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze Klauzule.

#### ***Klauzula 5 (Klauzula przystąpienia)***

a) Każdy podmiot niebędący Stroną niniejszych Klauzul może za zgodą wszystkich Stron przystąpić do niniejszych Klauzul jako administrator lub podmiot przetwarzający w dowolnym czasie, wypełniając Dodatki i podpisując Dodatek I.

b) Po wypełnieniu i podpisaniu Dodatków wymienionych w lit. a) podmiot przystępujący jest traktowany jako Strona niniejszych Klauzul i ma prawa i obowiązki administratora lub podmiotu przetwarzającego, zgodnie z rolą nadaną mu w Dodatku I.

c) Podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych Klauzul w odniesieniu do okresu, zanim został ich Stroną.

## **SEKCJA II**

### **OBOWIĄZKI STRON**

#### ***Klauzula 6 (Opis przetwarzania)***

Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele przetwarzania, dla których dane osobowe są przetwarzane w imieniu administratora, określono w Dodatku II.

#### ***Klauzula 7 (Obowiązki Stron)***

##### **7.1. Polecenia**

a) Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.

b) Podmiot przetwarzający bezzwłocznie powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenia wydane przez administratora naruszają RODO lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

## **7.2. Ograniczenie celu**

Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym(-ych) celu(-ach) przetwarzania, określonym(-ych) w Dodatku II, chyba że otrzyma dalsze polecenia od administratora.

## **7.3. Czas trwania przetwarzania danych osobowych**

Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w Dodatku II.

## **7.4. Bezpieczeństwo przetwarzania**

a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w Dodatku III. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, Strony należyście uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.

b) Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezzwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

## **7.5. Dane wrażliwe**

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), podmiot przetwarzający stosuje szczególne ograniczenia i/lub dodatkowe zabezpieczenia.

## **7.6. Dokumentacja i zgodność**

- a) Strony są w stanie wykazać zgodność z niniejszymi Klauzulami.
- b) Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi Klauzulami.
- c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych Klauzulach i wynikają bezpośrednio z RODO. Na żądanie administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi Klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.
- d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
- e) Na żądanie właściwego(-ych) organu(-ów) nadzorczego(-ych) Strony udostępniają mu (im) informacje, o których mowa w niniejszej Klauzuli, w tym wyniki wszelkich audytów.

## **7.7. Korzystanie z usług podmiotów podprzetwarzających**

- a) Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu. Podmiot przetwarzający wyraźnie informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co

najmniej 30 dni, dając tym samym administratorowi wystarczająco dużo czasu na wyrażenie sprzeciwu wobec takich zmian przed rozpoczęciem korzystania z usług danego(-ych) podmiotu(-ów) podprzetwarzającego(-ych). Podmiot przetwarzający przekazuje administratorowi niezbędne informacje umożliwiające mu skorzystanie z prawa sprzeciwu.

**b)** Jeżeli podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych, jak obowiązki nałożone na podmiot przetwarzający dane zgodnie z niniejszymi Klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych Klauzul oraz RODO.

**c)** Na żądanie administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, oraz wszelkich późniejszych zmian. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed udostępnieniem jej kopii.

**d)** Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z podmiotem przetwarzającym. Podmiot przetwarzający powiadamia administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.

**e)** Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą – jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i polecić mu usunięcie lub zwrot danych osobowych.

## **7.8. Międzynarodowe przekazywanie danych**

**a)** Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V RODO.

**b)** Jeżeli zgodnie z Klauzulą 7.7 podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu

administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V RODO, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V RODO za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 RODO, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

#### ***Klauzula 8 (Pomoc dla administratora)***

a) Podmiot przetwarzający niezwłocznie zawiadamia administratora o każdym żądaniu otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na takie żądanie samodzielnie, chyba że administrator wyraził na to zgodę.

b) Podmiot przetwarzający pomaga administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na żądania osób, których dane dotyczą, związane z wykonywaniem przysługujących im praw, z uwzględnieniem charakteru przetwarzania. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.

c) Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z Klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji dostępnych podmiotowi przetwarzającemu:

1) Obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych”), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;

2) obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu jego minimalizacji;

3) obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;

4) obowiązek określony w art. 32 RODO.

5) Strony określają w Dodatku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej Klauzuli, jak również zakres wymaganej pomocy.

#### ***Klauzula 9 (Zgłaszanie naruszenia ochrony danych osobowych)***

W przypadku naruszenia ochrony danych osobowych podmiot przetwarzający współpracuje z administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających, w stosownych przypadkach, z art. 33 i 34 RODO, z uwzględnieniem charakteru przetwarzania i informacji dostępnych podmiotowi przetwarzającemu.

### **9.1 Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora**

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający pomaga administratorowi:

a) przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorcemu(-ym) bez zbędnej zwłoki po tym, jak administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);

b) przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO winny być zawarte w zgłoszeniu administratora i obejmować co najmniej:

- 1) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- 2) możliwe konsekwencje naruszenia ochrony danych osobowych;
- 3) środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

c) przy wypełnianiu – zgodnie z art. 34 RODO – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

### **9.2 Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający**

W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi bez

zbędnej zwłoki po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:

- a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
- b) dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
- c) wskazanie prawdopodobnych konsekwencji naruszenia oraz środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

Strony określają w Dodatku III wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, pomagając administratorowi w wypełnianiu jego obowiązków określonych w art. 33 i 34 RODO.

### **SEKCJA III**

#### **POSTANOWIENIA KOŃCOWE**

##### ***Klauzula 10 (Naruszenie Klauzul i rozwiązanie umowy)***

a) Bez uszczerbku dla przepisów RODO, w przypadku gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych Klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi Klauzulami lub umowa ulegnie rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych Klauzul.

b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi Klauzulami, jeżeli:

- 1) administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi Klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;



2) podmiot przetwarzający poważnie lub stale narusza niniejsze Klauzule lub swoje obowiązki wynikające z RODO;

3) podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych Klauzul lub z RODO.

**c)** Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi Klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z Klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.

**d)** Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza administratorowi, że tego dokonał, lub zwraca administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszych Klauzul do czasu usunięcia lub zwrotu danych.

## DODATEK I

### Wykaz stron

**Administrator(-rzy):** *[dane identyfikacyjne i kontaktowe administratora(-ów) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez administratora]*  
**(„Zamawiający”)**

Imię i nazwisko lub nazwa: \_\_\_\_\_

Adres: \_\_\_\_\_

Podpis \_\_\_\_\_

Imię i nazwisko \_\_\_\_\_

Stanowisko \_\_\_\_\_

Data \_\_\_\_\_

Kontakt \_\_\_\_\_

**Podmiot(y) przetwarzający(-e):**

Imię i nazwisko lub nazwa: Zoho Corporation B.V („Zoho”)

Adres: Beneluxlaan 4B, 3527 HT UTRECHT, Holandia

Podpis \_\_\_\_\_

Imię i nazwisko \_\_\_\_\_

Stanowisko \_\_\_\_\_

Data \_\_\_\_\_

Kontakt [privacy@eu.zohocorp.com](mailto:privacy@eu.zohocorp.com)

## **DODATEK II**

### **Opis przetwarzania**

#### ***Kategorie osób, których dane osobowe są przetwarzane:***

Przetwarzane dane osobowe związane są z następującymi kategoriami osób, których dane dotyczą:

Zoho może przetwarzać wszelkie dane wprowadzone przez upoważnionych użytkowników narzędzi Zoho do współpracy i zarządzania online. Będzie to przede wszystkim dotyczyć realnych osób będących:

- użytkownikami upoważnionymi przez Zamawiającego do korzystania z usług;
- pracownikami, przedstawicielami, wykonawcami i kontaktami Zamawiającego;
- potencjalnymi klientami, klientami, partnerami biznesowymi i dostawcami Zamawiającego;
- doradcami i profesjonalnymi ekspertami Zamawiającego;
- pracownikami, przedstawicielami, wykonawcami i kontaktami potencjalnych klientów, klientów, partnerów biznesowych, dostawców, doradców i profesjonalnych ekspertów Zamawiającego.

#### ***Kategorie przetwarzanych danych osobowych:***

Kategorie przetwarzanych danych osobowych mogą obejmować między innymi:

- imię i nazwisko, dane kontaktowe, adres;
- dane związane z zatrudnieniem;
- informacje finansowe.

*Przetwarzane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa:*

Zoho zapewnia opcje szyfrowania danych wrażliwych w stanie spoczynku. Zdolność szyfrowania danych w stanie spoczynku jest inna w każdej usłudze Zoho i opcja ta może nie być domyślnie włączona. Szczegóły dotyczące możliwości szyfrowania w usługach Zoho są albo

publikowane przez Zoho na stronach internetowych Zoho, albo udostępniane Zamawiającemu na żądanie. W oparciu o charakter przetwarzanych wrażliwych danych osobowych Zamawiający ustala odpowiedniość lub adekwatność możliwości szyfrowania zapewnianych przez usługę(-i) Zoho i włącza szyfrowanie.

***Charakter przetwarzania:*** Charakter przetwarzania przez Zoho będzie obejmował świadczenie usług Zoho zgodnie z warunkami Umowy Serwisowej, niniejszej UPD lub jakiegokolwiek innej umowy pomiędzy Zamawiającym a Zoho.

***Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora:*** W celu świadczenia usług Zoho zgodnie z poleceniami przekazanymi przez Zamawiającego, opisanymi w punkcie 1 niniejszej UPD.

***Czas trwania przetwarzania:*** Okres obowiązywania Umowy Serwisowej.

*W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania:*

Zgodnie z punktem 3 Podmiot(y) Podprzetwarzający(-e) będą przetwarzać dane osobowe przez okres obowiązywania Umowy Serwisowej.

## **Dodatek III**

### **Techniczne i organizacyjne środki bezpieczeństwa mające zastosowanie do Manage Engine Service Desk Plus**

#### **Wstęp**

ManageEngine tworzy rozwiązania do zarządzania IT, które umożliwiają administratorom IT radzenie sobie w sposób proaktywny ze stojącymi przed nimi wyzwaniami informatycznymi. Poprawiamy stan bezpieczeństwa naszych klientów i traktujemy priorytetowo ich bezpieczeństwo danych oraz prywatność. W ramach niniejszego artykułu dokumentujemy nasze procesy bezpieczeństwa na poziomach organizacyjnym i produktowym.

#### **I. Bezpieczeństwo organizacji**

Wdrożyliśmy System Zarządzania Bezpieczeństwem Informacji (SZBI), który uwzględnia nasze cele w zakresie bezpieczeństwa, jak również ryzyka i działania minimalizujące dotyczące wszystkich zainteresowanych stron. Stosujemy ścisłe polityki i procedury obejmujące bezpieczeństwo, dostępność, przetwarzanie, integralność i poufność danych klientów.

##### **Kontrola przeszłości pracowników**

Przeszłość każdego pracownika poddawana jest procesowi weryfikacji. Przeprowadzenie tej kontroli w naszym imieniu zlecamy renomowanym agencjom zewnętrznym. Ma to na celu sprawdzenie rejestrów karnych pracowników, ich ewentualnej historii zatrudnienia oraz wykształcenia. Do czasu przeprowadzenia tej kontroli pracownikowi nie przydziela się zadań, które mogą wiązać się z ryzykiem dla użytkowników.

##### **Świadomość w zakresie bezpieczeństwa**

Po wprowadzeniu każdy pracownik podpisuje umowę o zachowaniu poufności i politykę dozwolonego korzystania, po czym przechodzi szkolenie w zakresie bezpieczeństwa informacji, prywatności i zgodności. Ponadto poziom świadomości pracowników oceniany jest przy pomocy testów i quizów, tak aby ustalić, z jakich tematów wymagane jest dalsze szkolenie. Zapewniamy szkolenia dotyczące konkretnych aspektów bezpieczeństwa, których pracownicy mogą potrzebować w zależności od pełnionych przez nich ról. Stale edukujemy naszych pracowników na temat bezpieczeństwa informacji, prywatności i zgodności w ramach naszej wewnętrznej społeczności, którą pracownicy regularnie odwiedzają, tak aby byli oni na bieżąco z praktykami bezpieczeństwa w organizacji. Aby podnosić świadomość i motywować do innowacyjności w zakresie bezpieczeństwa i prywatności organizujemy również wydarzenia wewnętrzne.

##### **Dedykowane zespoły ds. bezpieczeństwa i prywatności**

Posiadamy dedykowane zespoły ds. bezpieczeństwa i prywatności, które wdrażają nasze programy w zakresie bezpieczeństwa i prywatności oraz zarządzają nimi. Zespoły te regulują i utrzymują systemy obrony, opracowują procesy przeglądu pod kątem bezpieczeństwa i stale monitorują nasze sieci w celu wykrywania podejrzanej aktywności. Zapewniają one naszym zespołom inżynierów usługi doradcze i wskazówki w zakresie poszczególnych domen.

##### **Audyt wewnętrzny i zgodność**

Posiadamy dedykowany zespół ds. zgodności, który dokonuje przeglądu procedur i polityk w ManageEngine, tak aby dostosowywać je do standardów oraz ustalić, jakie procedury kontroli, procesy i systemy są potrzebne w celu spełnienia tych standardów. Zespół ten przeprowadza również okresowe audyty wewnętrzne oraz ułatwia prowadzenie niezależnych audytów i ocen przez strony trzecie. Aby uzyskać więcej informacji, prosimy zapoznać się z naszym [portfolio zgodności](#).

### **Bezpieczeństwo punktów końcowych**

Wszystkie stacje robocze wydawane pracownikom ManageEngine mają aktualne wersje systemu operacyjnego i zostały skonfigurowane z oprogramowaniem antywirusowym. Są one skonfigurowane w taki sposób, aby zachować zgodność z naszymi standardami bezpieczeństwa, które wymagają, aby wszystkie stacje robocze były odpowiednio skonfigurowane, posiadały zainstalowane poprawki oraz były śledzone i monitorowane przez rozwiązania do zarządzania punktami końcowymi ManageEngine. Omawiane stacje robocze posiadają domyślne zabezpieczenia – zostały bowiem skonfigurowane w taki sposób, aby szyfrować dane w stanie spoczynku, mają silne hasła i są blokowane podczas bezczynności. Urządzenia mobilne używane do celów służbowych są rejestrowane w systemie zarządzania urządzeniami mobilnymi, tak aby zapewnić, że spełniają one nasze standardy bezpieczeństwa.

## **II. Bezpieczeństwo aplikacji**

ServiceDesk Plus to platforma do zarządzania helpdeskiem obejmująca podstawowe aplikacje do zarządzania helpdeskiem oraz zarządzania IT, a także zarządzanie projektami, zarządzanie umowami, zarządzanie zasobami, bazę danych zarządzania konfiguracją (CMDB) oraz funkcje zapewniające zgodność z ITIL (Information Technology Infrastructure Library). Oprogramowanie ServiceDesk Plus jest obecnie wykorzystywane przez różne organizacje; niektóre spośród nich zainstalowały i skonfigurowały ServiceDesk Plus w ramach swojej sieci, a kilka innych zainstalowało i skonfigurowało ServiceDesk Plus w taki sposób, aby uzyskiwać do niego dostęp przez Internet. Jakikolwiek kompromis w zakresie bezpieczeństwa danych klientów narazi zatem organizacje na poważne ryzyko. Dlatego oprogramowanie ServiceDesk Plus zostało zaprojektowane z myślą o zapewnieniu maksymalnego bezpieczeństwa w każdym czasie, w tym podczas instalacji aplikacji, uwierzytelniania użytkowników, transmisji danych, przechowywania danych i zwykłego korzystania.

### **Bezpieczeństwo na etapie projektowania (secure by design)**

Nasz Model Cyklu Życia Tworzenia Oprogramowania (SDLC) zobowiązuje zespół inżynierów ServiceDesk Plus do ścisłego przestrzegania naszych standardów bezpiecznego kodowania. Ponadto standardów bezpieczeństwa przestrzegamy w całym procesie SDLC.

### **Standard bezpieczeństwa w fazie analizy i projektowania**

- Nasz zespół inżynierów gromadzi i analizuje wymagania, co ma na celu identyfikację wszelkich wad zabezpieczeń i luk w nowych funkcjach.
- Przygotowuje plan oceny podatności, odpowiadając na obawy dotyczące bezpieczeństwa zgłaszane przez użytkowników i analityków bezpieczeństwa, odnoszące się do poprzednich wydań/wersji.
- Opracowuje prototyp produktu lub funkcji, w tym zmiany, i przekazuje je do zatwierdzenia organowi zarządzania zmianami.

### **Standard bezpieczeństwa w fazie tworzenia**

- Zespół programistów postępuje zgodnie z wytycznymi w zakresie bezpieczeństwa przekazanymi przez zespół ds. bezpieczeństwa produktu.
- Kod źródłowy jest okresowo przeglądany przez koordynatora ds. bezpieczeństwa i kierownika zespołu.
- Przed skorzystaniem z wszelkich zależności kodu i bibliotek stron trzecich nasze zespoły ds. prawnych i bezpieczeństwa zweryfikują, czy biblioteki stron trzecich mają jakiegokolwiek znane problemy z zabezpieczeniami, czy też nie.
- Tylko upoważnieni inżynierowie mają dostęp do repozytorium kodu źródłowego.
- Dla zmodyfikowanych źródeł włączony jest proces zatwierdzania/przeglądu.

### **Standard bezpieczeństwa w fazie zapewnienia jakości (QA)/wydania**

- Wykonanie testów integracyjnych, automatycznych i penetracyjnych w celu zapewnienia, aby nowe funkcje lub moduły były zabezpieczone przed potencjalnymi podatnościami/wadami.
- Ciągłe testy dymne w celu zapewnienia, aby podstawowa funkcjonalność produktu pozostała nienaruszona, bez otwierania nowych luk w zabezpieczeniach.
- Generowanie raportów oceny bezpieczeństwa w celu zidentyfikowania kolejnych obszarów wymagających poprawy.
- Przeprowadzanie ciągłego skanowania podatności po wydaniu w celu szybkiej identyfikacji podatności i wprowadzania odnośnych poprawek.

### **Proces przeglądu bezpieczeństwa**

Posiadamy zespół ds. bezpieczeństwa, którego zadaniem jest zapewnienie, by wydana kompilacja/produkt były wolne od podatności w zakresie bezpieczeństwa. Podczas procesu przeglądu bezpieczeństwa zespół będzie postępować zgodnie z poniższym procesem.

- Stosuje zautomatyzowane narzędzie audytu bezpieczeństwa do nowych funkcji.
- Realizuje program audytu bezpieczeństwa dla wszystkich funkcji i poprawek błędów.
- Analizuje sposób wykorzystania plików stron trzecich i jego znane podatności.
- Zbiera zwięzłe informacje o funkcjach/poprawkach błędów od programistów w celu wykrycia ewentualnych podatności.
- Tworzy sprawozdania na temat bezpieczeństwa zarówno dla programistów, jak i zespołu wsparcia technicznego, tak aby klientom zapewnione zostało natychmiastowe rozwiązanie.
- Monitoruje niedawno wykryte podatności.
- W ramach końcowej kontroli zespół ds. bezpieczeństwa przeprowadza również testy strukturalne (white box testing), tj. manualny przegląd kodu źródłowego, co ma na celu wykrycie wszelkich defektów w kompilacji. Na tym etapie zespół ds. bezpieczeństwa opracowuje przypadki testowe w celu weryfikacji poprawności działania wszystkich funkcjonalności oraz obsługi błędów w stworzonej funkcji.
- Po rozwiązaniu wszystkich problemów i utworzeniu nowej kompilacji zespół ds. bezpieczeństwa zatwierdzi kompilację jako ostateczną.

### **Inne standardy bezpieczeństwa**

- Nasze repozytorium i infrastruktura kompilacji są zabezpieczone protokołem SSH/HTTPS i umieszczone w bezpiecznej, podzielonej na segmenty sieci z bardziej rygorystycznymi procedurami uwierzytelniania i kontroli dostępu.
- Nasze struktury bezpieczeństwa i kodu są zgodne ze standardami OWASP i wdrożone w warstwie aplikacji.
- Wszystkie zmiany kodu, zależności stron trzecich, pakiety wydań i pakiety uaktualnień podlegają wielu poziomom wewnętrznego przeglądu bezpieczeństwa, automatyzacji i testów penetracyjnych, a także skanowaniu podatności, co ma na celu zapewnienie ich dobrego zabezpieczenia przed błędami logicznymi i problemami z bezpieczeństwem.
- Każda aktualizacja i nowa funkcja w ServiceDesk Plus podlega wewnętrznym politykom zarządzania zmianami i regularnym ocenom podatności, a zmiany są wdrażane do środowiska produkcyjnego tylko po zatwierdzeniu przez zainteresowane organy zarządzania zmianami i bezpieczeństwem.
- Pliki binarne są podpisywane certyfikatem do podpisywania kodu, a klucz prywatny jest bezpiecznie przechowywany w podzielonej na segmenty sieci z ograniczonym dostępem.
- Dla wzmocnienia naszego stanu bezpieczeństwa zespół inżynierów ServiceDesk Plus ściśle współpracuje z wewnętrznymi zespołami ds. bezpieczeństwa, tak aby zasięgać ich opinii oraz identyfikować obszary wymagające poprawy.

Oprócz opisanych powyżej środków bezpieczeństwa podejmujemy stałe wysiłki na rzecz większego bezpieczeństwa aplikacji. W poniższej sekcji podano szczegółowe informacje na temat specyfikacji bezpieczeństwa ManageEngine ServiceDesk Plus.

### **ServiceDesk Plus: specyfikacje bezpieczeństwa**

Prosimy skorzystać z poniższego linku, aby dowiedzieć się więcej o specyfikacjach bezpieczeństwa produktu.

<https://www.manageengine.com/products/service-desk/servicedesk-plus-security-specifications.html>

## **III. Bezpieczeństwo operacyjne**

### **Ochrona danych klientów w ServiceDesk Plus**

ServiceDesk Plus jest produktem instalowalnym, zatem wszystkie dane znajdują się w środowisku klienta. W związku z tym w wersji ServiceDesk Plus On Premises naruszenie bezpieczeństwa danych nie jest możliwe. W naszym portalu wsparcia klienta przechowywane są jedynie zgłoszenia wsparcia klienta i pliki dziennika.

- Pliki przesłane przez klientów są bezpiecznie przechowywane w portalu wsparcia klienta.
- Przesłane pliki są dostępne tylko dla upoważnionych techników wsparcia.
- W przypadku danych przesłanych na serwer zostanie zachowana ich poufność i będą one wykorzystywane wyłącznie na potrzeby debugowania.
- Przesłane pliki można pobierać tylko na określonych serwerach, a dane uwierzytelniające serwera nie są nikomu udostępniane.
- Przesłane pliki zostaną usunięte automatycznie w następujących warunkach.
  - Podczas zamykania zgłoszenia zapewniamy usunięcie plików dziennika i danych na serwerze.
  - Plik przesłany na serwer zostanie usunięty automatycznie po 25 dniach.



## **Proces kompilacji i wprowadzania poprawek**

- Aby zapewnić całkowitą niezawodność najnowszych kompilacji zespół ServiceDesk Plus ściśle współpracuje z MESRC, co ma na celu przeprowadzanie obowiązkowych skanowań podatności i testów penetracyjnych przed każdym głównym wydaniem. Ponadto zespół przeprowadza ciągłe oceny podatności tych kompilacji, tak aby były one wolne od wszelkich nowych podatności.
- Gdy pojawi się nowa poprawka bezpieczeństwa lub aktualizacja, użytkownicy są bezzwłocznie powiadamiani o konieczności uaktualnienia produktu do najnowszej wersji.
- W przypadku wystąpienia obaw dotyczących bezpieczeństwa lub eskalacji, od użytkowników wymaga się przesłania szczegółowego raportu na temat odnośnej podatności lub odnośnego błędu w zabezpieczeniach. W międzyczasie zespół ds. produktu ocenia istotność błędu i ryzyko z nim związane oraz określa priorytet wydania na podstawie wagi błędu.

## **Rejestrowanie i monitorowanie**

Produkt rejestruje pewne dane w celu debugowania oraz zapobiegania niewłaściwemu korzystaniu. Pliki dziennika generowane przez ServiceDesk Plus są przechowywane na urządzeniach klientów. Możliwe jest przechowywanie maksymalnie 50 plików dziennika, a rozmiar każdego pliku ograniczony jest do 10 MB. Po osiągnięciu tego limitu pliki dziennika są rolowane; starsze pliki są usuwane z urządzeń użytkowników. Nie mamy dostępu do plików dziennika, chyba że użytkownik udostępni je w celu skorzystania z usług wsparcia. W takim przypadku dostęp do plików dziennika ma tylko personel wsparcia i zespół programistów, w zakresie ograniczonym do pełnionych przez nich ról. Po zidentyfikowaniu problemu pliki dziennika są usuwane.

## **Zapewnienie ciągłości działania**

W celu zapewnienia ciągłości działania posiadamy zasilanie awaryjne, systemy kontroli temperatury oraz systemy gaśnicze i przeciwpożarowe. Istnieją dedykowane plany zapewnienia ciągłości działania w zakresie głównych operacji takich, jak zarządzanie infrastrukturą i wsparcie techniczne. Posiadamy dobrze przygotowany plan zapewnienia ciągłości działania i usuwania skutków awarii, który ma nam pomóc w przypadku przedłużających się przerw w świadczeniu usług, wpływających tym samym na usługi świadczone klientom, wynikających z czynników od nas niezależnych, np. klęsk żywiołowych, katastrof spowodowanych przez człowieka itp., tak abyśmy mogli wznowić operacje zarządzania punktami końcowymi w maksymalnym możliwym zakresie w jak najkrótszym czasie. W celu zapewnienia ciągłości świadczenia usług naszym klientom powyższym planem objęte zostały wszystkie nasze wewnętrzne operacje. Utworzyliśmy trzy zespoły awaryjne, a mianowicie Zespół Zarządzania Kryzysowego (EMT), Zespół ds. Usuwania Skutków Awarii (DRT) i Zespół Usług Technicznych IT (IT), które mają za zadanie zapewnienie lepszej koordynacji i wsparcia między różnymi zespołami.

## **IV. Zarządzanie incydentami**

### **Raportowanie**

Mamy dedykowany zespół ds. zarządzania incydentami. Powiadamy Państwa o incydentach w naszym środowisku, które Państwa dotyczą, informując również o odpowiednich działaniach, których podjęcie przez Państwa może być potrzebne. Śledzimy i zamykamy incydenty, podejmując odpowiednie działania naprawcze. W stosownych przypadkach prześlemy Państwu niezbędne dowody odnoszące się do incydentów, które Państwa dotyczą. Ponadto wdrażamy procedury kontrolne, aby zapobiec powtórzeniu się podobnych sytuacji. Priorytetowo odpowiadamy na incydenty związane z bezpieczeństwem lub prywatnością zgłaszane nam przez Państwa na adres

e-mail incidents@zohocorp.com. W przypadku incydentów ogólnych powiadomimy użytkowników za pośrednictwem naszych blogów, forów i mediów społecznościowych. W przypadku incydentów dotyczących konkretnego użytkownika indywidualnego lub konkretnej organizacji powiadomimy zainteresowaną stronę za pośrednictwem poczty elektronicznej (na zarejestrowany u nas podstawowy adres e-mail administratora Organizacji).

#### **Zawiadomienie o naruszeniu**

Jako administratorzy danych zawiadamiamy odpowiedni Organ Ochrony Danych o naruszeniu w ciągu 72 godzin po jego stwierdzeniu, zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO). W razie potrzeby, w zależności od konkretnych wymagań, powiadamiamy klientów.

#### **V. Odpowiedzialne ujawnianie**

Posiadamy program zgłaszania podatności o nazwie „Bug Bounty”, którego celem jest okazanie uznania dla pracy badaczy bezpieczeństwa w zakresie identyfikowania podatności i nagrodzenie tej pracy. Jesteśmy zaangażowani we współpracę ze społecznością na rzecz weryfikacji, odtwarzania, reakcji, naprawy i wdrażania odpowiednich rozwiązań w zakresie zgłoszonych podatności. W przypadku odkrycia takich problemów prosimy o zgłoszenie ich na stronie internetowej <https://bugbounty.zoho.com>. Jeśli chcą Państwo zgłosić nam podatności bezpośrednio, prosimy o wiadomość e-mail na adres support@servicedeskplus.com

## **Techniczne i organizacyjne środki bezpieczeństwa mające zastosowanie do OP Manager Plus**

### **I. Bezpieczeństwo organizacji**

Wdrożyliśmy System Zarządzania Bezpieczeństwem Informacji (SZBI), który uwzględnia nasze cele w zakresie bezpieczeństwa, jak również ryzyka i działania minimalizujące dotyczące wszystkich zainteresowanych stron. Stosujemy ścisłe polityki i procedury obejmujące bezpieczeństwo, dostępność, przetwarzanie, integralność i poufność danych klientów.

#### **Kontrola przeszłości pracowników**

Przeszłość każdego pracownika poddawana jest procesowi weryfikacji. Przeprowadzenie tej kontroli w naszym imieniu zlecamy renomowanym agencjom zewnętrznym. Ma to na celu sprawdzenie rejestrów karnych pracowników, ich ewentualnej historii zatrudnienia oraz wykształcenia. Do czasu przeprowadzenia tej kontroli pracownikowi nie przydziela się zadań, które mogą wiązać się z ryzykiem dla użytkowników.

#### **Świadomość w zakresie bezpieczeństwa**

Po wprowadzeniu każdy pracownik podpisuje umowę o zachowaniu poufności i politykę dozwolonego korzystania, po czym przechodzi szkolenie w zakresie bezpieczeństwa informacji, prywatności i zgodności. Ponadto poziom świadomości pracowników oceniany jest przy pomocy testów i quizów, tak aby ustalić, z jakich tematów wymagane jest dalsze szkolenie. Zapewniamy szkolenia dotyczące konkretnych aspektów bezpieczeństwa, których pracownicy mogą potrzebować w zależności od pełnionych przez nich ról. Stale edukujemy naszych pracowników na temat bezpieczeństwa informacji, prywatności i zgodności w ramach naszej wewnętrznej społeczności, którą pracownicy regularnie odwiedzają, tak aby byli oni na bieżąco z praktykami bezpieczeństwa w organizacji. Aby podnosić świadomość i motywować do innowacyjności w zakresie bezpieczeństwa i prywatności organizujemy również wydarzenia wewnętrzne.

#### **Dedykowane zespoły ds. bezpieczeństwa i prywatności**

Posiadamy dedykowane zespoły ds. bezpieczeństwa i prywatności, które wdrażają nasze programy w zakresie bezpieczeństwa i prywatności oraz zarządzają nimi. Zespoły te regulują i utrzymują systemy obrony, opracowują procesy przeglądu pod kątem bezpieczeństwa i stale monitorują nasze sieci w celu wykrywania podejrzanej aktywności. Zapewniają one naszym zespołom inżynierów usługi doradcze i wskazówki w zakresie poszczególnych domen.

#### **Audyt wewnętrzny i zgodność**

Posiadamy dedykowany zespół ds. zgodności, który dokonuje przeglądu procedur i polityk w ManageEngine, tak aby dostosowywać je do standardów oraz ustalić, jakie procedury kontroli, procesy i systemy są potrzebne w celu spełnienia tych standardów. Zespół ten przeprowadza również okresowe audyty wewnętrzne oraz ułatwia prowadzenie niezależnych audytów i ocen przez strony trzecie.

Aby uzyskać więcej informacji, prosimy zapoznać się z naszym [portfolio zgodności](#).

### **Bezpieczeństwo punktów końcowych**

Wszystkie stacje robocze wydawane pracownikom ManageEngine mają aktualne wersje systemu operacyjnego i zostały skonfigurowane z oprogramowaniem antywirusowym. Są one skonfigurowane w taki sposób, aby zachować zgodność z naszymi standardami bezpieczeństwa, które wymagają, aby wszystkie stacje robocze były odpowiednio skonfigurowane, posiadały zainstalowane poprawki oraz były śledzone i monitorowane przez rozwiązania do zarządzania punktami końcowymi ManageEngine. Omawiane stacje robocze posiadają domyślne zabezpieczenia – zostały bowiem skonfigurowane w taki sposób, aby szyfrować dane w stanie spoczynku, mają silne hasła i są blokowane podczas bezczynności. Urządzenia mobilne używane do celów służbowych są rejestrowane w systemie zarządzania urządzeniami mobilnymi, tak aby zapewnić, że spełniają one nasze standardy bezpieczeństwa.

## **II. Bezpieczeństwo aplikacji**

### **i. Bezpieczeństwo na etapie projektowania (secure by design)**

Przestrzegamy wytycznych bezpiecznego kodowania w ramach Cyklu Życia Tworzenia Oprogramowania (SDLC); wytyczne te udostępniane są wszystkim programistom. W następnym kroku, w celu ustalenia potencjalnych problemów z bezpieczeństwem weryfikujemy zmiany kodu, najpierw manualnie go przeglądając, a następnie korzystając z naszego analizatora kodu i narzędzi do skanowania podatności. Cały ten proces przeprowadzany jest przed wydaniem każdej nowej funkcji. W przypadku wykrycia jakichkolwiek problemów są one bezzwłocznie sprawdzane i naprawiane. Ponadto w warstwie aplikacji wdrożona została solidna struktura bezpieczeństwa, oparta na standardach OWASP. Przedmiotowa struktura zapewnia środki służące minimalizacji zagrożeń takich, jak ataki typu SQL Injection, Cross-Site Scripting oraz DoS w warstwie aplikacji. Co więcej, przeprowadzamy regularne sesje edukacyjne dla programistów na temat praktyk bezpiecznego kodowania.

### **ii. Tożsamość i kontrola dostępu**

#### **• Kontrola dostępu oparta na rolach**

Kontrola dostępu oparta na rolach pozwala na dostęp do określonej funkcji tylko upoważnionym użytkownikom.

Użytkownikom wyznacza się określone role, a ich dostęp do poszczególnych funkcjonalności zależy od przyznanych im uprawnień.

### iii. Szyfrowanie

- **W tranzycie:**

- Każdy transfer danych z aplikacji pośredniczącej (agent application) na serwer odbywa się za pomocą silnego protokołu szyfrowania – HTTPS. Użytkownicy mogą ustawić HTTPS jako domyślny protokół dla całej komunikacji z poziomu konsoli internetowej.
- Użytkownicy mogą wyłączyć starszą wersję TLS w pliku server.xml. Obsługa starszej wersji TLS zapewniana jest w celu umożliwienia użytkownikom zarządzania ich pracą na starszych wersjach systemu Windows. Dodatkowo, dla najnowszych systemów obsługiwane są silne szyfry oraz TLS 1.2.

To zapewnia, że podczas przesyłania danych są one zawsze szyfrowane.

- **W stanie spoczynku:** Dane wrażliwe, takie jak hasła, tokeny uwierzytelniania itp., które są przechowywane w bazach danych, są szyfrowane przy pomocy 256-bitowego standardu Advanced Encryption Standard (AES).

**Ochrona bazy danych:** Dostęp do bazy danych produktu można uzyskać tylko poprzez podanie specyficznych dla danej instancji danych uwierzytelniających i jest on ograniczony do dostępu lokalnego hosta. Przechowywane hasła są haszowane jednokierunkowo za pomocą funkcji bcrypt i są filtrowane ze wszystkich naszych logów. Ponieważ stosowany jest algorytm haszujący bcrypt z ciągiem zaburzającym dla poszczególnych użytkowników (per-user-salt), odtworzenie haseł wiązałoby się z nadmiernymi trudnościami i byłoby bardzo czasochłonne, a przy tym baza danych rezyduje tylko w konfiguracji klienta.

### 3. Bezpieczeństwo operacyjne

- a. **Bezpieczeństwo danych klientów:** Ponieważ produkt jest rozwiązaniem lokalnym (on-premise), dane klienta znajdują się wyłącznie w jego środowisku.

**Uwaga:** W przypadku, gdy klient potrzebuje pomocy w rozwiązaniu problemu, możemy wymagać dostarczenia plików dziennika klienta. Klient przesyła pliki dziennika przez bezpieczny, należący do nas portal, do którego dostęp uzyskać może tylko upoważniony personel, i przyznaje nam uprawnienia do dostępu do tych plików. Pliki dziennika zostaną automatycznie usunięte po pięciu dniach od czasu ich przesłania. Ponadto klient zostanie powiadomiony o wystąpieniu wszelkich naruszeń.

- b. **Zarządzanie podatnościami i poprawkami:**

Posiadamy dedykowany proces w zakresie podatności, w ramach którego przeprowadzane jest aktywne skanowanie w poszukiwaniu zagrożeń bezpieczeństwa lub podatności. Odbywa się to przy pomocy kombinacji certyfikowanych narzędzi skanujących stron trzecich oraz narzędzi wewnętrznych. Następnie wykonywane są testy automatyczne i manualne. Ponadto zespół ds. bezpieczeństwa aktywnie przegląda przychodzące raporty na temat bezpieczeństwa i monitoruje publiczne listy mailingowe, posty na blogach i serwisy wiki w celu identyfikacji incydentów bezpieczeństwa mogących mieć wpływ na spółkę. Po zidentyfikowaniu podatności wymagającej naprawy, jest ona rejestrowana, otrzymuje priorytet zależny od jej wagi i przypisywana jest do niej osoba odpowiedzialna. W dalszej kolejności identyfikujemy powiązane ryzyka i minimalizujemy je bądź poprzez wprowadzenie poprawek do systemów z podatnościami, bądź poprzez stosowanie odpowiednich procedur kontrolnych.

Po ocenie wagi podatności na podstawie analizy wpływu angażujemy się na rzecz rozwiązania problemu w ramach naszej zdefiniowanej umowy o gwarantowanym poziomie usług (SLA). W zależności od wagi problemu wysyłamy ostrzeżenia o zagrożeniu bezpieczeństwa wszystkim naszym klientom, opisując podatność, poprawkę i kroki, które powinien podjąć klient.

#### **c. Zapewnienie ciągłości działania:**

- W celu zapewnienia ciągłości działania posiadamy zasilanie awaryjne, systemy kontroli temperatury oraz systemy gaśnicze i przeciwpożarowe. Istnieją dedykowane plany zapewnienia ciągłości działania w zakresie głównych operacji takich, jak zarządzanie infrastrukturą i wsparcie techniczne.

- Posiadamy dobrze przygotowany plan zapewnienia ciągłości działania i usuwania skutków awarii, który ma nam pomóc w przypadku przedłużających się przerw w świadczeniu usług, wpływających tym samym na usługi świadczone klientom, wynikających z czynników od nas niezależnych, np. klęsk żywiołowych, katastrof spowodowanych przez człowieka itp., tak abyśmy mogli wznowić operacje zarządzania punktami końcowymi w maksymalnym możliwym zakresie w jak najkrótszym czasie. W celu zapewnienia ciągłości świadczenia usług naszym klientom powyższym planem objęte zostały wszystkie nasze wewnętrzne operacje. Utworzyliśmy trzy zespoły awaryjne, a mianowicie Zespół Zarządzania Kryzysowego (EMT), Zespół ds. Usuwania Skutków Awarii (DRT) i Zespół Usług Technicznych IT (IT), które mają za zadanie zapewnienie lepszej koordynacji i wsparcia między różnymi zespołami.

#### **d. Odpowiedzialne ujawnianie**

Posiadamy program zgłaszania podatności „Bug Bounty”, który odwołuje się do społeczności badaczy bezpieczeństwa i którego celem jest okazanie uznania dla ich pracy oraz jej nagrodzenie. Jesteśmy zaangażowani we współpracę ze społecznością na rzecz weryfikacji, odtwarzania, reakcji, naprawy i wdrażania odpowiednich rozwiązań w zakresie zgłoszonych

podatności. W przypadku odkrycia takich problemów prosimy o zgłoszenie ich na stronie internetowej <https://bugbounty.zoho.com> lub pocztą elektroniczną na adres: [opmanager-support@manageengine.com](mailto:opmanager-support@manageengine.com).

#### **e. Kontrola bezpieczeństwa po stronie klientów**

Powyżej omówiliśmy działania, jakie podejmujemy, aby zapewnić naszym klientom bezpieczeństwo na różnych odcinkach.

Oto działania, które możecie Państwo podjąć jako klienci, aby ze swojej strony zapewnić sobie bezpieczeństwo:

- Wybrać unikalne i skomplikowane hasło.
- Zabezpieczyć foldery współdzielone w sieci.
- Korzystać z zaufanych certyfikatów stron trzecich, zapewniając zabezpieczenie połączeń.
- Sprawdzać dostępność najnowszych poprawek i regularnie aktualizować swoje punkty końcowe.
- <https://www.manageengine.com/network-monitoring/service-packs.html>