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 przekaże 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 Wyłączną 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 należycie 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 bezwzględnie 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) nadzorczemu(-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

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 jakiejkolwiek 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 jakiekolwiek 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. Powiadamiamy 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 przekażemy 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.

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