UMOWA O PRZETWARZANIE DANYCH

Niniejsza Umowa o Przetwarzanie Danych (dalej „Umowa") zostaje zawarta pomiędzy spółką Siemens Product Lifecycle Management Software Inc., występującą także pod nazwą Siemens Industry Software (dalej „SISW"), a klientem, który potwierdził podpisem akceptację warunków Umowy (dalej „Klient"). SISW zachowuje prawo do korzystania z usług jednostek powiązanych w celu realizacji swoich praw i obowiązków wynikających z niniejszej Umowy. W związku z powyższym termin „SISW" użyty w niniejszej Umowie może także dotyczyć jednostek powiązanych, bezpośrednio lub pośrednio należących do spółki nadrzędnej Siemens Product Lifecycle Management Software Inc. lub przez nią kontrolowanych, które zostały upoważnione przez spółkę Siemens Product Lifecycle Management Software Inc. do dystrybucji usług chmury SISW („Usługa Chmury").

Klient ponosi wyłączną odpowiedzialność za ustalenie typu danych i osób, których dotyczy przetwarzanie danych, a także zobowiązany jest zapewnić legalność takiego przetwarzania za pomocą Usługi Chmury. Klient odpowiada również za dokonanie korygowanie, usuwanie lub blokowanie danych osobowych za pomocą funkcji oferowanych w ramach Usługi Chmury. Klient ma prawo eksportować i usuwać swoje dane, w tym dane osobowe, za pomocą funkcji oferowanych w ramach Usługi Chmury. Po rozwiązaniu niniejszej Umowy Klient ma 30 dni na przesłanie do SISW pisemnego wniosku o udostępnienie Klientowi Danych Klienta do pobrania. Po upływie okresu wskazanego przez SISW w odpowiedzi na taki wniosek pozostałe dane Klienta podlegają usunięciu i nie będą już dla niego dostępne. SISW i Klient uzgadniają, że w ramach Usługi Chmury prawo Klienta do wydawania poleceń realizowane będzie wyłącznie za pośrednictwem funkcji oferowanych w ramach Usługi Chmury. Dodatkowe polecenia dotyczące danych Klienta wymagają zawarcia odrębnej umowy na piśmie pomiędzy SISW a Klientem, określającej także wysokość dodatkowych opłat, jakie Klient będzie ponosić za realizację takich poleceń. Klient zobowiązuje się, że nie będzie wprowadzał do Usługi Chmury ani przechowywał w ramach tej usługi objętych ochroną informacji o stanie zdrowia (ang. protected health information, PHI), chyba że SISW i Klient zawarli na piśmie odrębną umowę, która wprost zezwala na przechowywanie informacji PHI w Usłudze Chmury.

W ramach świadczenia Usługi Chmury i w odniesieniu do systemu produkcyjnego SISW zobowiązuje się przedsięwziąć środki techniczne i organizacyjne, o których mowa w Załączniku 2 do Dodatku A do niniejszej Umowy. Systemy nieprodukcyjne związane z Usługą Chmury nie muszą być zgodne ze środkami opisanymi w Załączniku 2 do Dodatku A. SISW może też w dowolnym terminie zmienić środki techniczne i organizacyjne dotyczące systemu produkcyjnego, o ile zmiany takie nie obniżą istotnie poziomu ochrony oferowanej przez takie środki. SISW ograniczy zbieranie, przetwarzanie i wykorzystywanie danych osobowych przez swoich pracowników bez upoważnienia i zobowiązuje się zatrudniać do przetwarzania danych osobowych Klienta wyłącznie pracowników, którzy przeszli odpowiedni instruktaż zgodnie z wymaganiami dotyczącymi ochrony prywatności danych.

SISW ma prawo powierzyć realizację Usługi Chmury podwykonawcom przetwarzania, tj. podmiotom realizującym dalsze przetwarzanie danych. W zakresie, w jakim nie można wyłączyć dostępu podwykonawców przetwarzania do danych osobowych Klienta, SISW przekaże Klientowi na żądanie wykaz takich podmiotów wraz z ich lokalizacjami, a także odpowiednio uaktualni taki wykaz przed udzieleniem nowym podwykonawcom przetwarzania dostępu do danych osobowych należących do Klienta. Jeśli Klient z uzasadnionych powodów nie zgadza się na wprowadzenie nowego podwykonawcy przetwarzania, ma obowiązek niezwłocznie zawiadomić o tym SISW, a jeśli SISW nalega na zaangażowanie tego podmiotu, Klient ma uzasadniony powód, by wypowiedzieć niniejszą Umowę. W zakresie, w jakim zaangażowanie nowego podwykonawcy przetwarzania wymaga transgranicznego przekazywania danych, SISW podejmie starania, aby podwykonawca przetwarzania utrzymywał odpowiedni poziom ochrony takich danych osobowych.

SISW będzie regularnie weryfikować stosowanie odpowiednich środków technicznych i organizacyjnych oraz na uzasadniony wniosek Klienta potwierdzi, że środki takie są stosowane. Jeśli Klient ma powody, by przypuszczać, że potwierdzenie wystawione przez SISW jest niezgodne z prawdą, ma prawo potwierdzić zastosowanie wspomnianych środków technicznych i organizacyjnych w formie audytu SISW, pod warunkiem wcześniejszego zawiadomienia SISW o nim w odpowiednim terminie. Audyt taki zostanie przeprowadzony na koszt Klienta.

SISW i Klient uzgadniają, że jakiekolwiek wypadki przekazywania danych osobowych Klienta z krajów Unii Europejskiej (UE) do krajów spoza UE, co do których UE uznaje, że nie zapewniają odpowiedniego poziomu ochrony danych osobowych, realizowane będą zgodnie ze standardowymi klauzulami umownymi UE w tym zakresie, wskazanymi w Dodatku A i stanowiącymi część niniejszej Umowy. W razie sprzeczności między warunkami niniejszej Umowy a standardowymi klauzulami umownymi pierwszeństwo mają standardowe klauzule umowne. Standardowe klauzule umowne podlegają prawu państwa członkowskiego UE, w którym eksporter danych prowadzi działalność gospodarczą (zgodnie z definicją w Dodatku A).

Dodatek A
Standardowe klauzule umowne UE

Na potrzeby art. 26 ust. 2 dyrektywy 95/46/WE w odniesieniu do przekazywania danych osobowych przetwarzającym prowadzącym działalność w państwach trzecich, które nie zapewniają odpowiedniego poziomu ochrony danych

uzgodnione pomiędzy

Klientem i (lub) jednostką powiązaną Klienta prowadzącą działalność w UE

(dalej „**eksporter danych**")

a

spółką Siemens Product Lifecycle Management Software Inc., występującą także pod nazwą Siemens Industry Software, w tym każdą z jej jednostek powiązanych, bezpośrednio lub pośrednio należących do spółki nadrzędnej Siemens Product Lifecycle Management Software Inc. lub przez nią kontrolowanych, która została upoważniona przez spółkę Siemens Product Lifecycle Management Software Inc. do przetwarzania danych w jej imieniu

(dalej „**importer danych**");

każda z nich zwana jest osobno „stroną", a łącznie zwane są one „stronami".

STRONY UZGODNIŁY następujące Klauzule Umowne („Klauzule") w celu wskazania odpowiednich zabezpieczeń odnośnie do ochrony prywatności oraz podstawowych praw i wolności osób w zakresie przekazywania przez eksportera danych importerowi danych określonych w Załączniku 1 danych osobowych.

Art. 1. Definicje

Na potrzeby niniejszych Klauzul

(a) terminy „dane osobowe", „szczególne kategorie danych", „przetwarzanie,", „administrator", „przetwarzający", „podmiot danych" oraz „organ nadzorczy" mają znaczenia nadane im w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych;

(b) „eksporter danych" oznacza administratora przekazującego dane osobowe;

(c) „importer danych" oznacza przetwarzającego, który zgodził się odebrać od eksportera danych dane osobowe przeznaczone do przetworzenia w jego imieniu po ich przekazaniu zgodnie z jego poleceniami i postanowieniami niniejszych klauzul, oraz który nie jest objęty systemem państwa trzeciego zapewniającym odpowiedni stopień ochrony w rozumieniu art. 25 ust. 1 dyrektywy 95/46/WE;

(d) „podwykonawca przetwarzania" („podprzetwarzający") oznacza każdego przetwarzającego dane zaangażowanego przez importera danych lub przez jego podwykonawcę przetwarzania, który zgadza się odebrać od importera danych lub innego podwykonawcy przetwarzania importera danych dane osobowe przeznaczone wyłącznie do przetwarzania w imieniu eksportera danych po ich przekazaniu zgodnie z jego poleceniami, warunkami niniejszych klauzul oraz warunkami pisemnej umowy o podwykonawstwo;

(e) „obowiązujące prawo w zakresie ochrony danych" oznacza przepisy prawa chroniące prawa podstawowe i wolności osób, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych, które obowiązują administratora danych w państwie członkowskim, w którym eksporter danych prowadzi działalność gospodarczą;

(f) „techniczne i organizacyjne środki bezpieczeństwa" oznaczają środki, których celem jest ochrona danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, zmianą, nieupoważnionym ujawnieniem lub dostępem, w szczególności gdy przetwarzanie obejmuje transmisję danych w sieci, a także przed wszelkimi innymi bezprawnymi formami przetwarzania.

Art. 2. Szczegółowe informacje dotyczące przekazywania danych

Szczegółowe informacje dotyczące przekazywania danych, a przede wszystkim, w stosownych wypadkach, szczególne kategorie danych osobowych, podane są w Załączniku 1, który stanowi integralną część niniejszych klauzul.

Art. 3. Klauzula dotycząca beneficjentów będących osobami trzecimi

1. Podmiot danych może egzekwować względem eksportera danych postanowienia niniejszej klauzuli, klauzuli 4 lit. od b) do i), klauzuli 5 lit. od a) do e) oraz od g) do j), klauzuli 6 ust. 1 i 2, klauzuli 7, klauzuli 8 ust. 2 oraz klauzul od 9 do 12 jako beneficjent będący osobą trzecią.

2. Podmiot danych może egzekwować względem importera danych postanowienia niniejszej klauzuli, klauzuli 5 lit. od a) do e) oraz lit. g), klauzuli 6, klauzuli 7, klauzuli 8 ust. 2 oraz klauzul od 9 do 12 w wypadku, gdy eksporter danych faktycznie zniknął lub przestał występować w obrocie prawnym, chyba że podmiot będący jego spadkobiercą przejął całość obowiązków prawnych eksportera danych z mocy umowy lub obowiązującego prawa, w wyniku czego przejmuje on prawa i obowiązki eksportera danych; w takim wypadku podmiot danych może egzekwować ich realizację względem takiego podmiotu.

3. Podmiot danych może egzekwować względem podwykonawcy przetwarzania postanowienia niniejszej klauzuli, klauzuli 5 lit. od a) do e) oraz lit. g), klauzuli 6, klauzuli 7, klauzuli 8 ust. 2 oraz klauzul od 9 do 12 w wypadku, gdy zarówno eksporter danych, jak i importer danych faktycznie zniknęli lub przestali występować w obrocie prawnym albo zostali postawieni w stan upadłości, chyba że jakikolwiek podmiot prawny będący spadkobiercą przejął całość obowiązków prawnych eksportera danych z mocy umowy lub obowiązującego prawa, w wyniku czego przejął prawa i obowiązki eksportera danych; w takim wypadku podmiot danych może egzekwować ich realizację względem takiego podmiotu. Odpowiedzialność cywilna podwykonawcy przetwarzania na podstawie niniejszych klauzul w tym zakresie ograniczona jest do wykonywanych przez niego czynności przetwarzania.

4. Strony nie zgłaszają sprzeciwu wobec reprezentowania podmiotu danych przez stowarzyszenie lub inny organ w wypadku, gdy podmiot danych tego sobie życzy oraz gdy zezwala na to prawo krajowe.

Art. 4. Obowiązki eksportera danych

Eksporter danych potwierdza i oświadcza, że:

(a) czynność przetwarzania danych osobowych, w tym samo ich przekazywanie, jest i będzie realizowana zgodnie z odpowiednimi postanowieniami obowiązujących przepisów w zakresie ochrony danych (i w stosownych wypadkach została zgłoszona właściwym organom państwa członkowskiego, w którym eksporter danych ma siedzibę) i nie stanowi naruszenia odpowiednich przepisów prawa tego państwa;

(b) polecił i przez cały czas realizowania usług przetwarzania danych osobowych będzie polecał importerowi danych przetwarzanie przekazanych danych osobowych wyłącznie w imieniu eksportera danych i zgodnie z obowiązującymi przepisami w zakresie ochrony danych oraz niniejszymi klauzulami;

(c) importer danych udzieli wystarczających gwarancji w zakresie technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w Załączniku 2 do niniejszej umowy;

(d) po zakończeniu analizy wymagań wynikających z obowiązujących przepisów w zakresie ochrony danych zastosowane zostaną środki bezpieczeństwa odpowiednie do celu ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem lub przypadkową utratą, zmianą, nieupoważnionym ujawnieniem lub dostępem, w szczególności jeśli przetwarzanie obejmuje transmisję danych w sieci, a także przed wszelkimi pozostałymi bezprawnymi formami przetwarzania, oraz że środki te zapewnią poziom bezpieczeństwa odpowiadający ryzyku towarzyszącemu przetwarzaniu i charakterowi podlegających ochronie danych z uwzględnieniem obecnego stanu wiedzy i kosztu ich wdrożenia;

(e) zapewni zgodność z zastosowanymi środkami bezpieczeństwa;

(f) jeśli przekazaniu podlegają szczególne kategorie danych, podmiot danych został lub zostanie poinformowany przed przekazaniem danych lub możliwie szybko po ich przekazaniu, że jego dane mogą być przekazywane do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony w rozumieniu dyrektywy 95/46/WE;

(g) przekaże jakiekolwiek zawiadomienia otrzymane od importera danych lub podwykonawcy przetwarzania zgodnie z klauzulą 5 lit. b) oraz klauzulą 8 ust. 3 do organu nadzorczego ochrony danych, jeśli eksporter danych podejmie decyzję o kontynuowaniu przekazywania danych lub o przerwaniu zawieszenia ich przekazywania;

(h) udostępni podmiotom danych na żądanie kopię niniejszych klauzul z wyjątkiem Załącznika 2, a także ogólny opis przewidzianych środków bezpieczeństwa wraz z kopią umowy o usługi dalszego przetwarzania, która musi zostać zawarta zgodnie z niniejszymi klauzulami, chyba że klauzule lub wspomniana umowa zawierają informacje handlowe; w takim wypadku może usunąć takie informacje;

(i) w razie dalszego przetwarzania czynność przetwarzania realizowana będzie przez podwykonawcę przetwarzania zgodnie z postanowieniami klauzuli 11, a podwykonawca przetwarzania zapewni co najmniej ten sam poziom ochrony danych osobowych i praw podmiotów danych, do którego zapewnienia importer danych jest zobowiązany na podstawie niniejszych klauzul; oraz

(j) zapewni zgodność z klauzulą 4 lit. od a) do i).

Art. 5. Obowiązki importera danych

Importer danych potwierdza i zapewnia, że:

(a) przetwarza dane osobowe wyłącznie w imieniu eksportera danych i zgodnie z poleceniami i postanowieniami niniejszych klauzul, a jeśli nie jest w stanie osiągnąć zgodności w tym zakresie z jakichkolwiek przyczyn, niezwłocznie poinformuje eksportera danych o niemożności zachowania takiej zgodności; w takim wypadku eksporter danych ma prawo zawiesić przekazywanie danych i (lub) wypowiedzieć umowę;

(b) nie ma powodów, by przypuszczać, że obowiązujące go przepisy uniemożliwiają mu spełnienie poleceń eksportera danych oraz obowiązków wynikających z umowy, oraz że w razie zmiany przepisów, która z dużym prawdopodobieństwem będzie mieć znaczący, negatywny wpływ na oświadczenia i zobowiązania złożone na podstawie niniejszych klauzul, niezwłocznie po uzyskaniu o tym informacji powiadomi o zmianie eksportera danych; eksporter danych ma w takim wypadku prawo zawiesić przekazywanie danych i (lub) wypowiedzieć umowę;

(c) przed przetwarzaniem przekazywanych danych osobowych wdrożył techniczne i organizacyjne środki bezpieczeństwa, o których mowa w Załączniku 2;

(d) niezwłocznie poinformuje eksportera danych o:

i) każdym wiążącym prawnie wniosku o ujawnienie danych osobowych złożonym przez organy władzy wykonawczej, chyba że ujawnienie takie jest zabronione na mocy innych przepisów, np. wynikającego z prawa karnego zakazu pozwalającego chronić poufność śledztwa w ramach egzekwowania prawa;
ii) każdym przypadkowym lub nieupoważnionym dostępie; a także
iii) każdym wniosku otrzymanym bezpośrednio od podmiotów danych bez odpowiadania na taki wniosek, chyba że został osobno do tego upoważniony;

(e) będzie niezwłocznie i odpowiednio obsługiwać wszelkie zapytania od eksportera danych dotyczące przetwarzania przez niego przekazywanych danych osobowych, a także stosować się do wskazówek organu nadzorczego w odniesieniu do przetwarzania przekazywanych danych;

(f) na wniosek eksportera danych udostępni swoje obiekty przetwarzania danych na potrzeby audytu czynności przetwarzania objętych postanowieniami niniejszych klauzul, który realizowany będzie przez eksportera danych lub organ kontroli składający się z niezależnych członków posiadających wymagane kwalifikacje zawodowe i objętych zobowiązaniem do zachowania poufności, wybranych przez eksportera danych, w stosownych wypadkach w porozumieniu z organem nadzorczym;

(g) udostępni na żądanie podmiotom danych kopię niniejszych klauzul i obowiązującej umowy o dalsze przetwarzanie danych, chyba że niniejsze klauzule lub umowa zawierają informacje handlowe; w takim wypadku ma prawo usunąć takie informacje handlowe, z wyjątkiem Załącznika 2, który zostanie zastąpiony przez ogólny opis środków bezpieczeństwa, jeśli podmiot danych nie może uzyskać kopii od eksportera danych;

(h) w razie dalszego przetwarzania danych poinformował eksportera danych o tym fakcie i uzyskał jego uprzednią zgodę na piśmie;

(i) czynności przetwarzania wykonywane przez podwykonawcę przetwarzania będą realizowane zgodnie z postanowieniami klauzuli 11;

(j) niezwłocznie prześle eksporterowi danych zawartą na podstawie niniejszych klauzul umowę o dalsze przetwarzanie.

Art. 6. Odpowiedzialność

1. Strony uzgadniają, że każdy podmiot danych, których poniósł szkodę w wyniku naruszenia zobowiązań, o których mowa w klauzuli 3 lub w klauzuli 11, przez którąkolwiek ze stron lub podwykonawcę przetwarzania, jest upoważniony do otrzymania od eksportera danych odszkodowania za poniesioną szkodę.

2. Jeśli podmiot danych nie jest w stanie wnieść przeciwko eksporterowi danych roszczenia o odszkodowanie zgodnie z ust. 1, w związku z naruszeniem przez importera danych lub jego podwykonawcę przetwarzania jakichkolwiek zobowiązań, o których mowa w klauzuli 3 lub klauzuli 11, ponieważ eksporter danych faktycznie zniknął lub przestał występować w obrocie prawnym albo został postawiony w stan upadłości, importer danych wyraża zgodę na to, że podmiot danych może wystąpić z roszczeniem wobec importera danych w zastępstwie eksportera danych, chyba że podmiot będący spadkobiercą przejął całość zobowiązań prawnych eksportera danych wynikających z umów lub z mocy prawa; w takim wypadku podmiot danych może egzekwować swoje prawa wobec takiego podmiotu.

   Importer danych nie może powoływać się na naruszenie przez podwykonawcę przetwarzania jego zobowiązań w celu uniknięcia realizacji własnych zobowiązań.

3. Jeśli podmiot danych nie jest w stanie wnieść roszczenia przeciwko eksporterowi danych lub importerowi danych, o których mowa w ust. 1 i 2, w związku z naruszeniem przez podwykonawcę przetwarzania jakichkolwiek jego zobowiązań, o których mowa w klauzuli 3 lub klauzuli 11, ponieważ eksporter danych oraz importer danych faktycznie zniknęli lub przestali występować w obrocie prawnym albo zostali postawieni w stan upadłości, podwykonawca przetwarzania wyraża zgodę na to, że podmiot danych może wystąpić wobec podwykonawcy przetwarzania z roszczeniem dotyczącym czynności przetwarzania tego ostatniego realizowanych na podstawie niniejszych klauzul, jak gdyby podwykonawca przetwarzania był eksporterem danych lub importerem danych, chyba że podmiot będący spadkobiercą przejął całość zobowiązań prawnych eksportera danych lub importera danych wynikających z umów lub z mocy prawa; w takim wypadku podmiot danych może egzekwować swoje prawa wobec takiego podmiotu. Odpowiedzialność podwykonawcy przetwarzania ogranicza się do wykonywanych przez niego czynności przetwarzania na podstawie niniejszych klauzul.

Art. 7. Mediacja i jurysdykcja

1. Importer danych potwierdza, że jeśli podmiot danych będzie dochodzić względem niego praw beneficjenta będącego osobą trzecią i (lub) wystąpi z roszczeniem o odszkodowanie na podstawie niniejszych klauzul, importer danych zaakceptuje decyzję podmiotu danych w zakresie:

   (a) przekazania sporu do mediacji, której podejmie się niezależna osoba lub w stosownych wypadkach organ nadzorczy;

   (b) przekazania sporu do sądu w państwie członkowskim, w którym eksporter danych prowadzi działalność gospodarczą.

2. Strony uzgadniają, że wybór podmiotu danych nie powoduje uszczerbku dla jego praw materialnych lub procesowych w zakresie środków zaradczych na podstawie innych przepisów prawa krajowego lub międzynarodowego.

Art. 8. Współpraca z organami nadzorczymi

1. Eksporter danych zgadza się złożyć kopię niniejszej umowy do organu nadzorczego, o ile wystąpi on z takim wnioskiem lub jeśli takie przekazanie wymagane jest na podstawie obowiązujących przepisów w zakresie ochrony danych.

2. Strony uzgadniają, że organ nadzorczy ma prawo przeprowadzić audyt importera danych oraz jakiegokolwiek podwykonawcy przetwarzania, a zakres i warunki tego audytu winny być identyczne jak w wypadku audytu eksportera danych na podstawie obowiązujących przepisów w zakresie ochrony danych.

3. Importer danych zobowiązany jest niezwłocznie zawiadomić eksportera danych o istnieniu obowiązujących go lub każdego podwykonawcę przetwarzania przepisów prawa, które uniemożliwiają przeprowadzenie audytu importera danych lub jego podwykonawcy przetwarzania zgodnie z ust. 2. W takim wypadku eksporter danych ma prawo podjąć działania przewidziane w klauzuli 5 lit. b).

Art. 9. Prawo właściwe

Niniejsze klauzule podlegają prawu państwa członkowskiego, w którym eksporter danych prowadzi działalność gospodarczą.

Art. 10. Zmiany umowy

Strony zobowiązują się nie zmieniać treści niniejszych klauzul. Nie uniemożliwia to stronom dodawania w wymaganych wypadkach klauzul dotyczących kwestii związanych z działalnością gospodarczą, o ile nie są one sprzeczne z istniejącymi klauzulami.

Art. 11. Dalsze przetwarzanie

1. Importer danych zobowiązuje się nie zlecać czynności przetwarzania realizowanych w imieniu eksportera danych na podstawie niniejszych klauzul bez uprzedniej pisemnej zgody eksportera danych. Jeśli importer danych zleca swoje obowiązki na podstawie niniejszych klauzul za zgodą eksportera danych, może je zlecić wyłącznie przez zawarcie z podwykonawcą przetwarzania pisemnej umowy narzucającej na podwykonawcę przetwarzania te same obowiązki, które są nałożone na importera danych na podstawie niniejszych klauzul. Jeśli podwykonawca przetwarzania nie realizuje swoich obowiązków w zakresie ochrony danych wynikających z powyższej pisemnej umowy, importer danych ponosi względem eksportera danych pełną odpowiedzialność za realizację obowiązków podwykonawcy przetwarzania.

2. Pisemna umowa zawarta pomiędzy importerem danych a podwykonawcą przetwarzania musi też zawierać klauzulę dotyczącą beneficjenta będącego osobą trzecią, zawartą w klauzuli 3 na wypadek, gdyby podmiot danych nie mógł wnieść wobec eksportera danych lub importera danych roszczenia o odszkodowanie, o którym mowa w ust. 1 klauzuli 6, ponieważ faktycznie zniknęli lub przestali występować w obrocie prawnym albo zostali postawieni w stan upadłości, a żaden podmiot będący spadkobiercą nie przejął całości zobowiązań prawnych eksportera danych lub importera danych wynikających z umów lub z mocy prawa. Odpowiedzialność cywilna podwykonawcy przetwarzania na podstawie niniejszych klauzul w tym zakresie ograniczona jest do wykonywanych przez niego czynności przetwarzania.

3. Postanowienia umowy, o której mowa w ust. 1, dotyczące kwestii ochrony danych przy dalszym przetwarzaniu podlegają prawu państwa członkowskiego, w którym eksporter danych prowadzi działalność gospodarczą.

4. Eksporter danych zobowiązany jest prowadzić wykaz umów o dalsze przetwarzanie zawartych na podstawie niniejszych klauzul i zgłoszonych przez importera danych na podstawie klauzuli 5 lit. j) oraz aktualizować taki wykaz co najmniej raz w roku. Wykaz musi być dostępny dla organu nadzorczego ochrony danych właściwego dla eksportera danych.

Art. 12. Obowiązki po zakończeniu świadczenia usług przetwarzania danych osobowych

1. Strony uzgadniają, że po zakończeniu świadczenia usług przetwarzania danych osobowych importer danych lub podwykonawca przetwarzania zobowiązani są, zgodnie z wyborem eksportera danych, zwrócić eksporterowi danych całość przekazanych danych osobowych i ich kopii lub zniszczyć całość tych danych osobowych i zaświadczyć eksporterowi danych, że tak postąpili, chyba że obowiązujące importera danych prawo uniemożliwia mu zwrot albo zniszczenie całości lub części przekazanych danych osobowych. W takim wypadku importer danych zagwarantuje poufność przekazanych danych osobowych i zaprzestanie ich aktywnego przetwarzania.

2. Importer danych i podwykonawca przetwarzania gwarantują, że na wniosek eksportera danych i (lub) organu nadzorczego udostępnią swoje obiekty służące do przetwarzania danych na potrzeby audytu środków, o których mowa w ust. 1.

ZAŁĄCZNIK 1 DO STANDARDOWYCH KLAUZUL UMOWNYCH

Eksporter danych
Eksporterem danych jest (krótko opisać czynności w zakresie przekazywania danych):

Klient jest abonentem świadczonej przez SISW Usługi Chmury, która umożliwia użytkownikom końcowym upoważnionym przez Klienta wprowadzanie, modyfikowanie, usuwanie, pobieranie i przetwarzanie w inny sposób Danych Klienta, które mogą obejmować dane osobowe, zgodnie z treścią Umowy oraz odpowiedniej dokumentacji dotyczącej Usługi Chmury.

Importer danych
Importerem danych jest (krótko opisać czynności w zakresie przekazywania danych):

spółka Siemens Product Lifecycle Management Software Inc., która samodzielnie i (lub) za pośrednictwem podwykonawców przetwarzania świadczy Usługę Chmury obejmującą: utrzymanie w Stanach Zjednoczonych Ameryki i Unii Europejskiej infrastruktury obliczeniowej, w której funkcjonuje Usługa Chmury; przechowywanie w tej infrastrukturze Danych Klienta wprowadzanych do Usługi Chmury przez Klienta; monitorowanie dostępności i bieżącego funkcjonowania Usługi Chmury oraz infrastruktury; a także utrzymanie bezpieczeństwa infrastruktury zgodnie z treścią Umowy i odpowiedniej dokumentacji dotyczącej Usługi Chmury.

Podmioty danych
Przekazywane dane osobowe dotyczą następujących kategorii podmiotów danych (podać):

O ile eksporter danych nie wskaże inaczej na piśmie, podmiotami danych mogą być użytkownicy końcowi upoważnieni przez Klienta do korzystania z Usługi Chmury oraz inni pracownicy Klienta, których dane osobowe przechowywane są w Usłudze Chmury.

Kategorie danych
Przekazywane dane osobowe obejmują następujące kategorie danych (podać):

Konkretne kategorie danych, które mają być przechowywane w Usłudze Chmury, podlegają w dużym stopniu konfiguracji przez Klienta, choć niektóre wspólne kategorie danych, które mogą być przechowywane w Usłudze Chmury, to między innymi: nazwisko, adres e-mail, nazwa firmy, numer telefonu, miejsce pracy, narodowość lub obywatelstwo oraz informacje dotyczące dostępu i korzystania z Usługi Chmury. W zależności od konfiguracji Usługi Chmury przez Klienta Dane Klienta mogą obejmować wiele innych kategorii danych.

Szczególne kategorie danych (jeśli ma to zastosowanie)
Przekazywane dane osobowe obejmują następujące szczególne kategorie danych (podać):

Szczególne kategorie danych przechowywanych w Usłudze Chmury będą uzgadniane między stronami w Umowie lub Zamówieniu albo w zakresie prac dotyczącym profesjonalnych usług świadczonych na rzecz Klienta w ramach uruchomienia przez niego Usługi Chmury.

Czynności przetwarzania
Przekazywane dane osobowe objęte są następującymi podstawowymi czynnościami przetwarzania (podać):

Dane osobowe mogą być przetwarzane: w ramach normalnego funkcjonowania Usługi Chmury, w zależności od konfiguracji Klienta, w formie przechowywania i (lub) archiwizacji w infrastrukturze komputerowej utrzymywanej przez eksportera danych, w środowiskach jednego lub wielu użytkowników, w formie dostępu lub transmisji na podstawie poleceń przekazanych do Usługi Chmury przez użytkownika końcowego upoważnionego przez Klienta do korzystania z Usługi Chmury oraz w ramach czynności utrzymania Usługi Chmury realizowanych przez eksportera danych.

ZAŁĄCZNIK 2 DO STANDARDOWYCH KLAUZUL UMOWNYCH

Niektóre oferty dotyczące Usług Chmury realizowane są na innych warunkach, które, jeśli mają zastosowanie, podane są w Zamówieniu. W innym wypadku importer danych zastosuje w odniesieniu do przechowywanych w Systemie danych osobowych zgodnie z klauzulą 4 lit. d) i klauzulą 5 lit. c) środki techniczne i organizacyjne wskazane poniżej.

Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez importera danych zgodnie z klauzulą 4 lit. d) i klauzulą 5 lit. c):

1. Kontrola fizycznego dostępu. Nieupoważnione osoby nie będą mogły uzyskać fizycznego dostępu do pomieszczeń, budynków ani obiektów, w których znajdują się systemy przetwarzania danych, w których przetwarzane są i (lub) wykorzystywane dane osobowe.

   Środki: wszystkie centra danych przestrzegają rygorystycznych procedur bezpieczeństwa wprowadzonych przez personel bezpieczeństwa, stosują sprzęt do monitoringu wizyjnego, czujki ruchu, mechanizmy kontroli dostępu i inne środki zapobiegające naruszeniu integralności wyposażenia i obiektów centrum danych. Dostęp do systemów i infrastruktury na terenie obiektów centrów danych mają wyłącznie upoważnieni przedstawiciele. Sprzęt służący do zapewniania bezpieczeństwa fizycznego (np. czujki ruchu, kamery, itd.) jest regularnie konserwowany, aby zagwarantować jego prawidłowe działanie. We wszystkich centrach danych stosuje się następujące szczegółowe środki bezpieczeństwa fizycznego:

   a. Budynki są co do zasady zabezpieczone systemami kontroli dostępu (system dostępowy korzystający z kart inteligentnych).
   b. Dane do uwierzytelnienia, w tym dane znajdujące się na karcie dostępu elektronicznego (unikatowej dla każdego pracownika, dostawcy lub wykonawcy) oraz kod PIN, przekazywane są upoważnionym użytkownikom w celu uzyskania przez nich fizycznego dostępu do obiektów centrum danych.
   c. Fizyczny dostęp do centrów danych w granicach systemu umożliwiany jest za pomocą elektronicznego systemu kontroli dostępu, który składa się z czytników kart i terminali PIN przy wejściach do budynku i pomieszczeń oraz samych czytników kart dla wyjść z budynku i pomieszczeń.
   d. W zależności od klasyfikacji bezpieczeństwa budynki, poszczególne strefy i otaczający je teren podlegają dodatkowej ochronie z wykorzystaniem dodatkowych środków. Należą do nich określone profile dostępowe, monitoring wideo, systemy alarmu przeciwwłamaniowego i biometryczne systemy kontroli dostępu.
   e. Prawo do dostępu udzielane jest upoważnionym pracownikom indywidualnie zgodnie ze środkami Kontroli Dostępu do Systemu i Danych wskazanymi poniżej. Dotyczy to także dostępu dla gości. Gośce i odwiedzający budynki SISW muszą zarejestrować się w recepcji i muszą im towarzyszyć upoważnieni pracownicy SISW. SISW i inni zewnętrzni dostawcy centrów danych rejestrują imiona i nazwiska osób oraz czasy wejścia/wyjścia osób na teren prywatny SISW na terenie centrów danych.
   f. Pracownicy i personel zewnętrzny SISW muszą nosić swoje identyfikatory we wszystkich lokalizacjach SISW.

2. Kontrola dostępu do systemu. Należy uniemożliwić korzystanie bez upoważnienia z systemów przetwarzania danych używanych do świadczenia Usługi Chmury.

   Środki:

   a. SISW lub podwykonawcy przetwarzania zarządzają środowiskiem w taki sposób, by spełnić wymagania normy NIST SP 800-53 Rev. 4 Access Control (AC) and Identification and Authentication (IA) (Kontrola dostępu (AC), identyfikacja i uwierzytelnianie (IA)).
   b. Do udzielenia dostępu do systemów szczególnie chronionych, w tym systemów do przechowywania i przetwarzania danych osobowych, wykorzystuje się wiele poziomów autoryzacji. Stosuje się procesy zapewniające, że do dodawania, usuwania i modyfikacji użytkowników uprawnieni są wyłącznie upoważnieni użytkownicy.
   c. Wszyscy użytkownicy mający dostęp do systemów SISW posiadają unikatowe nazwy użytkowników i hasła, które muszą spełniać określone minimalne kryteria złożoności.
   d. SISW i podwykonawcy przetwarzania stosują procedury gwarantujące, że zgłaszane zmiany w zakresie upoważnień realizowane są zgodnie z wytycznymi (na przykład nie udziela się praw bez upoważnienia). Jeśli użytkownik SISW zmienia swoją rolę lub odchodzi z firmy, realizowany jest proces odebrania prawa do dostępu do środowiska.
   e. SISW i podwykonawcy przetwarzania ustanowili zasady dotyczące haseł, zakazujące udostępniania haseł innym osobom, informujące o niezbędnych działaniach w razie ujawnienia hasła i wymagające regularnego zmieniania wszystkich haseł użytkownika oraz zmiany haseł domyślnych. Na potrzeby uwierzytelniania

użytkownikom przypisywane są osobiste identyfikatory. Wszystkie hasła muszą spełnić minimalne wymagania w zakresie złożoności i są przechowywane w formie zaszyfrowanej. W wypadku haseł do domen system wymusza zmianę hasła co 60 dni, a nowe hasło musi spełnić wymagania w zakresie minimalnej złożoności. Na każdym komputerze SISW działa wygaszacz ekranu chroniony hasłem.

f. SISW lub podwykonawcy przetwarzania automatycznie kontrolują następujące zdarzenia dotyczące kont: utworzenie, modyfikacja, aktywacja, dezaktywacja i usunięcie. Rejestry z takimi danymi kontroluje okresowo administrator systemu.
g. Sieci SISW i podwykonawców przetwarzania są zabezpieczone na wyjściu do publicznego internetu zaporą.
h. SISW i podwykonawcy przetwarzania stosują aktualne oprogramowanie antywirusowe w punktach dostępu do sieci firmowej, dla kont e-mailowych oraz na wszystkich serwerach plików i na wszystkich stacjach roboczych.
i. SISW i podwykonawcy przetwarzania wdrażają zarządzanie poprawkami bezpieczeństwa w celu zapewnienia wprowadzania odpowiednich uaktualnień na potrzeby bezpieczeństwa.
j. Pełen zdalny dostęp do sieci firmowej SISW i infrastruktury krytycznej chroniony jest silnym, wieloczynnikowym mechanizmem uwierzytelniania.

3. Kontrola dostępu do danych. Osoby upoważnione do korzystania z systemów przetwarzania danych uzyskiwać będą dostęp wyłącznie do danych osobowych, do których mają prawa dostępu, a takie dane osobowe nie mogą być odczytywane, kopiowane, modyfikowane ani usuwane bez upoważnienia w trakcie ich przetwarzania, użytkowania i przechowywania.

   Środki:

   a. dostęp do danych osobowych, poufnych lub szczególnie chronionych (drażliwych) udzielany jest na zasadzie dostępu koniecznego. Innymi słowy, pracownicy lub osoby z zewnątrz mają dostęp tylko do informacji wymaganych do realizacji swoich zadań służbowych. SISW wykorzystuje koncepcje uwierzytelniania, w ramach których dokumentowany jest sposób i zakres przypisywania uprawnień. Wszystkie dane osobowe, poufne lub szczególnie chronione z innych powodów są chronione zgodnie politykami i standardami bezpieczeństwa SISW.
   b. Wszystkie serwery produkcyjne jakiejkolwiek Usługi Chmury SISW funkcjonują w odpowiednich centrach danych. Środki bezpieczeństwa chroniące przetwarzanie danych osobowych, poufnych lub szczególnie chronionych z innych powodów podlegają regularnemu sprawdzaniu. W tym celu SISW przeprowadza też okresowe audyty zewnętrzne, których celem jest potwierdzenie, że środki te są w odpowiedni sposób stosowane.
   c. SISW nie zezwala na instalowanie w systemach używanych na potrzeby Usługi Chmury oprogramowania osobistego ani innego oprogramowania, które nie zostało zatwierdzone przez SISW.
   d. Jeśli wystąpi konieczność przekazania danych ze względu na awarię nośnika danych, na którym się znajdują, po zakończeniu tej czynności nośnik, który uległ awarii, podlega rozmagnesowaniu (w wypadku nośnika magnetycznego) lub zniszczeniu (w wypadku nośników półprzewodnikowych lub optycznych).

4. Kontrola transmisji danych. Dane osobowe podczas przekazywania nie mogą być odczytywane, kopiowane, modyfikowane lub usuwane bez upoważnienia.

   Środki:

   a. SISW lub podwykonawcy przetwarzania zarządzają infrastrukturą i konfiguracją w taki sposób, by spełnić wymagania normy NIST SP 800-53 Rev. 4 Systems and Communication Protection (SC) (Ochrona systemów i komunikacji (SC)). Obejmuje to systemy sieciowe zapobiegania włamaniom (NIPS) oraz zapory na granicach systemu, zapewniające ochronę przed zainfekowanymi danymi w ramach komunikacji na zewnętrznej granicy infrastruktury. Systemy NIPS i zapory konfigurowane są zgodnie z normami DISA STIG. Dane w trakcie przesyłania szyfrowane są za pomocą modułów kryptograficznych spełniających wymagania normy FIPS 140-2.
   b. W wypadku fizycznego transportu nośników danych na terenie SISW stosowane są odpowiednie środki zapewniające uzgodniony poziom usług (np. szyfrowanie i pojemniki wyłożone ołowiem).
   c. Transmisja danych osobowych w sieci wewnętrznej SISW chroniona jest w taki sposób, jak transmisja innych danych poufnych na podstawie zasad bezpieczeństwa SISW.
   d. W wypadku przenoszenia danych pomiędzy SISW a Klientem środki ochrony przekazywanych danych osobowych są identyczne jak wskazane w Umowie lub odpowiedniej dokumentacji Usługi Chmury. Dotyczy to przenoszenia danych zarówno w formie fizycznej, jak i w sieci. Klient przejmuje odpowiedzialność za przekazywanie danych z Punktu Granicznego SISW (np. zapora danych wychodzących z centrum danych, które świadczy hosting dla Usługi Chmury).

5. Kontrola wprowadzanych danych. Usługa Chmury umożliwi retrospektywne ustalenie, czy ktoś uzyskał dostęp do danych osobowych albo zmodyfikował lub usunął dane osobowe z infrastruktury używanej do świadczenia Usługi Chmury.

   Środki:
   a. SISW zezwala na dostęp do danych osobowych wyłącznie upoważnionym pracownikom i tylko w zakresie koniecznym do realizacji ich zadań. SISW stosuje system rejestrowania wprowadzania, modyfikacji i usuwania danych lub ich blokowania przez SISW lub podwykonawców przetwarzania w maksymalnym zakresie obsługiwanym przez Usługę Chmury.
   b. Ścieżka audytu zapewnia wystarczający poziom szczegółowości, by ułatwić rekonstrukcję zdarzeń, jeśli wystąpiło lub podejrzewa się wystąpienie nieautoryzowanych czynności lub awarii. W każdym rekordzie rejestru zdarzeń systemu operacyjnego rejestrowane są typ zdarzenia, sygnatura czasu, źródło zdarzenia, lokalizacja zdarzeń, skutek zdarzenia oraz użytkownik związany ze zdarzeniem.

6. Kontrola zadań. Dane osobowe przetwarzane będą wyłącznie zgodnie z warunkami Umowy i związanymi z nią poleceniami przekazanymi przez Klienta.

   Środki:
   a. SISW wykorzystuje środki kontroli i procesy w celu zapewnienia zgodności z treścią umów zawartych pomiędzy SISW a klientami, podwykonawcami przetwarzania lub innymi usługodawcami.
   b. Dane Klienta objęte są co najmniej takim samym poziomem ochrony, co informacje poufne zgodnie ze standardem klasyfikacji informacji SISW.
   c. Wszyscy pracownicy i kontrahenci SISW mają wynikający z umowy obowiązek przestrzegania poufności wszystkich informacji szczególnie chronionych, w tym tajemnic handlowych klientów i partnerów SISW.

7. Kontrola dostępności. Dane osobowe będą chronione przed przypadkowym lub nieupoważnionym zniszczeniem lub utratą.

   Środki:
   a. pracownicy SISW wykonują kopie zapasowe procesów i stosują inne środki zapewniające szybkie przywrócenie do działalności systemów o krytycznym znaczeniu dla działalności gospodarczej w sytuacji, gdy są one niezbędne.
   b. SISW korzysta z globalnych dostawców usług chmury, aby zapewnić dostępność mocy na potrzeby centrów danych.
   c. SISW ma zdefiniowane plany kryzysowe, a także strategię przywracania normalnej działalności w odniesieniu do Usług Chmury.

8. Kontrola separacji danych. Dane osobowe zebrane w różnych celach mogą być przetwarzane osobno.

   Środki:
   a. w stosownych wypadkach SISW wykorzystuje możliwości techniczne wdrożonego oprogramowania (na przykład środowisko wielu użytkowników lub osobny system) w celu odseparowania danych osobowych Klienta i danych innych klientów.
   b. SISW utrzymuje odrębne instancje (z separacją logiczną i fizyczną) dla każdego klienta.
   c. Klient (w tym jego podmioty powiązane) ma dostęp wyłącznie do swoich instancji.

9. Kontrola nienaruszalności danych. Zapewnia, że dane osobowe pozostaną nietknięte, kompletne i aktualne w trakcie czynności przetwarzania:

   Środki: SISW stosuje strategię obrony składającą się z kilku warstw, która stanowi zabezpieczenie przed nieupoważnionymi modyfikacjami. Obejmuje ona środki kontroli podane w punktach dotyczących środków kontroli powyżej. Konfiguracja zapór spowoduje powstanie wielu segmentów sieci, czego wynikiem jest separacja dostępu publicznego i prywatnego. Każda reguła zapory będzie obejmować określone środki kontroli dostępu, określające dozwoloną wymianę informacji między tymi segmentami.

   a. Centrum monitorowania bezpieczeństwa: oprócz innego oprogramowania i procesów wykorzystywanych na potrzeby bezpieczeństwa i na potrzeby dochodzeniowe stosowane jest także automatyczne oprogramowanie do

wykrywania włamań w celu ostrzegania, śledzenia i, w razie konieczności, zawiadamiania o incydencie bezpieczeństwa oraz wspomagania eliminacji jego skutków.

b. Oprogramowanie antywirusowe: wszystkie systemy będą mieć skonfigurowane aktualne definicje antywirusowe, by zapewniać ochronę przed wirusami, robakami, trojanami i innymi formami szkodliwego oprogramowania.
c. Kopie zapasowe i odzyskiwanie danych: wszystkie systemy będą mieć tworzone obrazy danych i konfiguracji na potrzeby tworzenia kopii zapasowych na poziomie bazowym. W stosownych wypadkach SISW i podwykonawcy przetwarzania będą także obsługiwać instancję klienta o konfiguracji zapewniającej wysoką dostępność, co pozwoli zagwarantować, że dane przechowywane są w dwóch odrębnych centrach danych znajdujących się wystarczająco daleko od siebie.
d. Regularne audyty zewnętrzne w celu wykazania prawidłowego działania środków bezpieczeństwa. SISW i podwykonawcy przetwarzania będą przechodzić okresowo audyty sprawdzające działanie wymienionych powyżej środków bezpieczeństwa.