SMLOUVA O ZPRACOVÁNÍ DAT

Tato smlouva o zpracování dat (dále jen „smlouva“) se uzavírá mezi společností Siemens Product Lifecycle Management Software Inc., známou také jako Siemens Industry Software (dále jen „SISW“), a zákazníkem, který vyjádřil svůj souhlas s podmínkami této smlouvy (dále jen „zákazník“). Společnost SISW si ponechává právo využívat své přidružené společnosti k prosazení jakýchkoli svých práv a splnění jakýchkoliv svých povinností na základě této smlouvy. Proto také může pojem „SISW“ použitý v tomto dokumentu odkazovat na přidružené společnosti, které jsou přímo či nepřímo vlastněny nebo kontrolovány nejvyšší nadřazenou společností společnosti Siemens Product Lifecycle Management Software Inc. a které společnost Siemens Product Lifecycle Management Software Inc. oprávnila k distribuci cloudových služeb SISW (dále jen „cloudové služby“).

Za určení typu údajů a osob dotčených zpracováním bude odpovědný výhradně zákazník, který zajistí oprávněnost takového zpracování prostřednictvím cloudových služeb. Zákazník bude také odpovědný za veškeré opravy, výmazy nebo zablokování osobních údajů za použití funkcí nabízených cloudovými službami. Zákazník může svá data včetně osobních údajů za použití funkcí nabízených cloudovými službami exportovat a mazat. Po skončení této smlouvy o zpracování dat bude mít zákazník 30 dnů na odeslání písemné žádosti společnosti SISW o to, aby data zákazníka byla zákazníkovi zpřístupněna ke stažení. Po uplynutí libovolného období stanoveného společností SISW v odpovědi na danou žádost budou zbývající data zákazníka vymazána a nebudou již pro zákazníka dostupná. Společnost SISW a zákazník souhlasí v rámci cloudové služby, že právo zákazníka vydávat pokyny bude uplatňováno výhradně pomocí funkcí nabízených cloudovou službou. Dodatečné pokyny týkající se dat zákazníka vyžadují samostatnou písemnou smlouvu mezi společností SISW a zákazníkem včetně smlouvy o dalších poplatcích, které zákazník zaplatí za provedení takových pokynů. Zákazník se zavazuje, že do cloudové služby neodešle ani neuloží jakékoliv chráněné zdravotní informace („PHI“), pokud společnost SISW a zákazník neuzavřeli samostatnou písemnou smlouvu, která výslovně povoluje ukládání informací PHI do cloudové služby.

Při poskytování cloudové služby bude společnost SISW s ohledem na výrobní systém dodržovat všechna technická a organizační opatření popsaná v dodatku č. 2 k příloze A této smlouvy o zpracování dat. Nevýrobní systémy související s cloudovou službou mohou nebo nemusí dodržovat opatření popsaná v dodatku č. 2 k příloze A. Kromě tohoto může společnost SISW příležitostně změnit technická a organizační opatření vztahující se na výrobní systém, pokud tyto změny nebudou mít zásadně nepříznivý dopad na úroveň ochrany, kterou tato opatření zajišťují. Společnost SISW zakáže svým pracovníkům shromažďovat, zpracovávat nebo používat osobní údaje bez oprávnění a bude při zpracování osobních údajů zákazníka nasazovat pouze takové pracovníky, kteří byli specificky vyškoleni v souladu s požadavky ochrany důvěrnosti dat.

Společnost SISW bude oprávněna použít při provádění cloudové služby dílčí zpracovatele. V rozsahu ve kterém nelze přístup dílčích zpracovatelů k osobním údajům vyloučit poskytne společnost SISW zákazníkovi na jeho žádost seznam těchto dílčích zpracovatelů a jejich umístění a předtím, než bude přístup k zákazníkovým osobním údajům udělen jakémukoli novému dílčímu zpracovateli, bude tento seznam dle potřeby aktualizovat. Pokud bude mít zákazník proti libovolnému novému dílčímu zpracovateli odůvodněné námitky, bude o těchto námitkách informovat společnost SISW a pokud bude společnost SISW na přijetí tohoto nového dílčího zpracovatele trvat, bude mít zákazník právo ukončit tuto smlouvu o zpracování dat pro odůvodněnost. Pokud zapojení jakéhokoliv takového dílčího zpracovatele zahrnuje přeshraniční přenos osobních údajů, zavazuje se společnost SISW zajistit, aby takový dílčí zpracovatel dodržoval s ohledem na takové osobní údaje odpovídající úroveň ochrany dat.

Společnost SISW bude pravidelně kontrolovat dodržování příslušných technických a organizačních opatření a na základě přiměřené žádosti zákazníka zákazníkovi potvrdí, že příslušná technická a organizační opatření jsou dodržována. Pokud má zákazník důvod se domnívat, že potvrzení vydaná společností SISW jsou nesprávná, je zákazník oprávněn ověřit si dodržování technických a organizačních opatření naplánováním kontroly u společnosti SISW na základě oznámení zaslaného s přiměřeným předstihem. Tato kontrola bude provedena na náklady a výdaje zákazníka.

Společnost SISW a zákazník souhlasí s tím, že jakékoliv převody osobních údajů zákazníka ze zemí v Evropské unii do zemí mimo EU, které EU považuje za země, které nemají odpovídající úroveň ochrany osobních údajů, budou prováděny podle ustanovení standardních smluvních doložek EU, které jsou uvedeny v příloze A a jsou tímto plně začleněny do této smlouvy. V případě rozporu mezi podmínkami této smlouvy o zpracování dat a podmínkami standardních smluvních doložek budou mít přednost ustanovení standardních smluvních doložek. Standardní smluvní doložky se budou řídit zákony členského státu EU, ve kterém je usazen vývozce dat (dle definice v příloze A).

Příloha A
Standardní smluvní doložky EU

ve smyslu čl. 26 odst. 2 směrnice 95/46/ES pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích, které nezajišťují odpovídající úroveň ochrany údajů
mezi

zákazníkem nebo přidruženou společností zákazníka sídlící v EU

(dále jen „**vývozce údajů**“)

a

společností Siemens Product Lifecycle Management Software Inc., známou také jako společnost Siemens Industry Software, včetně všech přidružených společností, které jsou přímo či nepřímo vlastněny nebo kontrolovány nejvyšší nadřazenou společností společnosti Siemens Product Lifecycle Management Software Inc. a které společnost Siemens Product Lifecycle Management Software Inc. oprávnila ke zpracování dat jejím jménem

(dále jen „**dovozce údajů**“)

jednotlivě „strana“; společně „strany“

SE DOHODLI v zájmu zajištění dostatečných ochranných opatření s ohledem na ochranu soukromí a základní práva a svobody osob při předávání osobních údajů uvedených v dodatku 1 vývozcem údajů dovozci údajů na těchto smluvních doložkách („doložky“).

Doložka 1. Definice

Pro účely doložek:

(a) „osobní údaje“, „zvláštní kategorie údajů“, „zpracovávat/zpracování“, „správce“, „zpracovatel“, „subjekt údajů“ a „orgán dozoru“ mají stejný význam jako ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;

(b) „vývozcem údajů“ se rozumí správce, který předává osobní údaje;

(c) „dovozcem údajů“ se rozumí zpracovatel, který se zavazuje přijímat od vývozce údajů osobní údaje určené ke zpracování jménem vývozce údajů po předání v souladu s jeho pokyny a s podmínkami těchto doložek a který nepodléhá systému třetí země zajišťující odpovídající ochranu ve smyslu čl. 25 odst. 1 směrnice 95/46/ES;

(d) „dílčím zpracovatelem“ se rozumí zpracovatel najatý dovozcem údajů nebo jiným dílčím zpracovatelem dovozce údajů, který se zavazuje přijímat od dovozce údajů nebo od jiného dílčího zpracovatele dovozce údajů osobní údaje určené výhradně pro činnosti spojené se zpracováním jménem vývozce údajů po předání v souladu s pokyny vývozce údajů, podmínkami stanovenými v příloze a podmínkami písemné smlouvy o dílčím zpracování;

(e) „právem rozhodným pro ochranu údajů“ rozumí právní předpisy ochraňující základní práva a svobody jednotlivců, a zejména jejich právo na soukromí ve vztahu ke zpracování osobních údajů, které se vztahují na správce údajů v členském státě, ve kterém je usazen vývozce údajů;

(f) „technickými a organizačními bezpečnostními opatřeními“ rozumí opatření zaměřená na ochranu osobních údajů před náhodným či protiprávním zničením nebo před náhodnou ztrátou, úpravou, neoprávněným zveřejněním či přístupem, zejména v případech, kdy v souvislosti se zpracováním dochází k předávání údajů po síti, nebo před všemi ostatními protiprávními způsoby zpracování.

Doložka 2. Podrobnosti předávání

Podrobnosti předávání a zejména případné zvláštní kategorie osobních údajů jsou uvedeny v dodatku 1, který tvoří nedílnou součást doložek.

Doložka 3. Doložka ve prospěch třetí strany

1. Subjekty údajů mohou vůči vývozci údajů uplatnit jako oprávněné třetí strany tuto doložku, doložku 4 písm. b) až i), doložku 5 písm. a) až e) a g) až j), doložku 6 odst. 1 a 2, doložku 7, doložku 8 odst. 2 a doložky 9 až 12.

2. Subjekty údajů mohou vůči dovozci údajů uplatnit tuto doložku, doložku 5 písm. a) až e) a g), doložku 6, doložku 7, doložku 8 odst. 2 a doložky 9 až 12 v případech, kdy vývozce údajů fakticky zmizel nebo kdy z právního hlediska zanikl, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů a v důsledku toho přijímá práva a povinnosti vývozce údajů, přičemž v tomto případě je subjekt údajů může uplatňovat vůči tomuto subjektu.

3. Subjekty údajů mohou vůči dílčímu zpracovateli uplatnit tuto doložku, doložku 5 písm. a) až e) a g), doložku 6, doložku 7, doložku 8 odst. 2 a doložky 9 až 12 v případech, kdy vývozce údajů i dovozce údajů fakticky zmizeli nebo kdy z právního hlediska zanikli nebo jsou v platební neschopnosti, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů a v důsledku toho přijímá práva a povinnosti vývozce údajů, přičemž v tomto případě je subjekt údajů může uplatňovat vůči tomuto subjektu. Tato odpovědnost dílčího zpracovatele vůči třetím stranám je omezena na jeho vlastní činnosti spojené se zpracováním údajů podle těchto doložek.

4. Strany nemají námitek proti tomu, aby byl subjekt údajů zastupován sdružením nebo jiným subjektem, je-li to jeho výslovným přáním a povoluje-li to vnitrostátní právo.

Doložka 4. Povinnosti vývozce údajů

Vývozce údajů se zavazuje a zaručuje, že:

(a) zpracování osobních údajů, včetně předávání samotného, bylo a bude i nadále prováděno v souladu se souvisejícími ustanoveními práva rozhodného pro ochranu údajů (a případně bylo oznámeno příslušným orgánům členského státu, ve kterém je vývozce údajů usazen) a že neporušuje související předpisy daného státu;

(b) nařídil a po celou dobu poskytování služeb zpracování osobních údajů bude dovozci údajů nařizovat, aby předávané osobní údaje byly zpracovávány pouze jménem vývozce údajů a v souladu s právem rozhodným pro ochranu údajů a s doložkami;

(c) dovozce údajů poskytne dostatečné záruky v souvislosti s technickými a organizačními bezpečnostními opatřeními uvedenými v dodatku 2 k této smlouvě;

(d) po vyhodnocení požadavků práva rozhodného pro ochranu údajů jsou bezpečnostní opatření dostatečná k zajištění ochrany osobních údajů před náhodným či protiprávním zničením nebo před náhodnou ztrátou, úpravou, neoprávněným zveřejněním či přístupem, zejména v případech, kdy v souvislosti se zpracováním dochází k předávání údajů po síti, nebo před všemi ostatními protiprávními způsoby zpracování, a že tato opatření zajišťují úroveň bezpečnosti odpovídající rizikům, která v souvislosti se zpracováním hrozí, a povaze údajů, jež mají být chráněny, s ohledem na stav techniky a nákladnost jejich zavedení;

(e) zajistí dodržování bezpečnostních opatření;

(f) budou-li součástí předávání i zvláštní kategorie údajů, subjekt údajů byl nebo bude informován před předáním nebo co nejdříve poté, že jeho údaje mohou být předávány do třetí země, která neposkytuje odpovídající ochranu ve smyslu směrnice 95/46/ES;

(g) předá oznámení obdržené od dovozce údajů nebo případného dílčího zpracovatele podle doložky 5 písm. b) a doložky 8 odst. 3 orgánu dozoru pro ochranu údajů, pokud se vývozce údajů rozhodne pokračovat v předávání nebo odvolat jeho pozastavení;

(h) na požádání poskytne subjektům údajů kopii doložek, s výjimkou dodatku 2 a souhrnného popisu bezpečnostních opatření, a rovněž kopii případné smlouvy o službách dílčího zpracování, kterou je nutno uzavřít v souladu s doložkami, pokud doložky nebo smlouva neobsahují obchodní informace, v tomto případě je možno tyto obchodní informace vynechat;

(i) v případě dílčího zpracování je činnost spojená se zpracováním údajů vykonávána v souladu s doložkou 11 dílčím zpracovatelem, který zajišťuje přinejmenším stejnou úroveň ochrany osobních údajů a práv subjektu údajů jako dovozce údajů podle doložek, a

(j) zajistí shodu s doložkou 4 písm. a) až i).

Doložka 5. Povinnosti dovozce údajů

Dovozce údajů se zavazuje a zaručuje, že:

(a) osobní údaje bude zpracovávat pouze jménem vývozce údajů a v souladu s jeho pokyny a s těmito doložkami; nebude-li moci dodržování pokynů a doložek z jakýchkoli důvodů zajistit, zavazuje se o tom neprodleně informovat vývozce údajů, který je v takovém případě oprávněn pozastavit předávání údajů a/nebo odstoupit od smlouvy;

(b) nemá důvod se domnívat, že mu právní předpisy, kterým podléhá, brání plnit pokyny vývozce údajů a jeho povinnosti vyplývající ze smlouvy a že v případě změny těchto právních předpisů, která by mohla mít výrazně nepříznivý dopad na ochranná opatření a závazky stanovené doložkami, oznámí neprodleně tuto změnu vývozci údajů, který je v takovém případě oprávněn pozastavit předávání údajů a/nebo odstoupit od smlouvy;

(c) před zpracováním předaných osobních údajů učinil organizační a technická bezpečnostní opatření uvedená v dodatku 2;

(d) oznámí vývozci údajů neprodleně:

(i) veškeré právně závazné požadavky na zveřejnění osobních údajů ze strany donucovacího orgánu, není-li to jinak zakázáno, například trestním právem, aby byla zajištěna důvěrnost vyšetřování v rámci výkonu práva,

(ii) veškeré případy získání náhodného nebo neoprávněného přístupu a;

(iii) veškeré žádosti obdržené přímo od subjektů údajů, aniž by na tyto žádosti reagoval, ledaže k tomu byl jinak oprávněn;

(e) vyřídí neprodleně a řádně veškeré dotazy vývozce údajů týkající se jím prováděného zpracování osobních údajů, které jsou předmětem přenosu, a že se bude řídit v souvislosti se zpracováním předávaných údajů názorem orgánu dozoru;

(f) na žádost vývozce údajů umožní přezkoumání činností spojených se zpracováním údajů podle doložek ve svých zařízeních na zpracování údajů, které provede vývozce údajů nebo kontrolní orgán složený z nezávislých členů s požadovanou odbornou kvalifikací, kteří budou vázáni povinností zachovat mlčenlivost a vybráni vývozcem údajů, popřípadě po dohodě s orgánem dozoru;

(g) na požádání poskytne subjektu údajů kopii doložek nebo případné existující smlouvy o dílčím zpracování, pokud doložky nebo smlouva neobsahují obchodní informace, v tomto případě je možno tyto obchodní informace vynechat, s výjimkou dodatku 2, který bude nahrazen souhrnným popisem bezpečnostních opatření v případech, kdy subjekt údajů není schopen získat kopii od vývozce údajů;

(h) v případě dílčího zpracování předem informoval vývozce údajů a obdržel jeho předchozí písemný souhlas;

(i) služby zpracování údajů poskytované dílčím zpracovatelem budou v souladu s doložkou 11;

(j) vývozci údajů zašle neprodleně kopii případné dohody s dílčím zpracovatelem, která se uzavírá podle těchto doložek.

Doložka 6. Odpovědnost

1. Strany se dohodly, že subjekt údajů, který utrpěl v důsledku porušení povinností uvedených v doložce 3 nebo doložce 11 škodu způsobenou kteroukoli ze stran nebo dílčím zpracovatelem, je oprávněn obdržet od vývozce údajů za utrpěnou škodu náhradu.

2. Nemůže-li subjekt údajů uplatňovat v souladu s odstavcem 1 nárok na odškodnění vůči vývozci údajů pro porušení některé z povinností dovozce údajů nebo jeho dílčího zpracovatele uvedených v doložce 3 a 11, protože vývozce údajů fakticky zmizel, z právního hlediska zanikl nebo je v platební neschopnosti, dovozce údajů se zavazuje, že subjekt údajů smí uplatňovat nároky vůči dovozci údajů, jako by byl vývozcem údajů, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů, přičemž v tomto případě může subjekt může uplatňovat svá práva vůči tomuto subjektu.

   Dovozce údajů se nemůže spoléhat na to, že dílčí zpracovatel poruší své povinnosti, aby se vyhnul vlastní odpovědnosti.

3. Nemůže-li subjekt údajů uplatňovat v souladu s odstavci 1 a 2 nárok vůči vývozci údajů a dovozci údajů pro porušení některé z povinností dílčího zpracovatele uvedených v doložkách 3 a 11, protože vývozce údajů i dovozce údajů fakticky zmizeli, z právního hlediska zanikli nebo jsou v platební neschopnosti, dílčí zpracovatel se zavazuje, že subjekt údajů smí uplatňovat nároky vůči dílčímu zpracovateli s ohledem na jeho vlastní činnosti spojené se zpracováním údajů podle těchto doložek, jako by byl vývozcem údajů nebo dovozcem údajů, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů nebo dovozce údajů, přičemž v tomto případě může subjekt údajů uplatňovat svá práva vůči tomuto subjektu. Odpovědnost dílčího zpracovatele je omezena na jeho vlastní činnosti spojené se zpracováním údajů podle těchto doložek.

Doložka 7. Mediace a soudní příslušnost

1. Dovozce údajů se zavazuje, že uplatní-li proti němu subjekt údajů práva ve prospěch třetí strany a/nebo uplatní-li nárok na náhradu škody podle těchto doložek, přistoupí dovozce údajů na rozhodnutí subjektu údajů:

(a) předat spor k mediaci prováděné nezávislou osobou nebo popřípadě orgánem dozoru;

(b) předat spor soudům v členském státě, ve kterém je vývozce údajů usazen.

2. Strany se dohodly, že rozhodnutím subjektu údajů nebudou dotčena jeho hmotná ani procesní práva při podávání soudních žalob v souladu s ostatními ustanoveními vnitrostátního nebo mezinárodního práva.

Doložka 8. Spolupráce s orgány dozoru

1. Vývozce údajů se zavazuje uložit kopii této smlouvy u orgánu dozoru, vyžaduje-li to tento orgán nebo právo rozhodné pro ochranu údajů.

2. Strany se dohodly, že orgán dozoru má právo provést přezkoumání u dovozce údajů a u případného dílčího zpracovatele, které bude mít stejný rozsah a bude podléhat stejným podmínkám jako přezkoumání u vývozce údajů uskutečněné v souladu s právem rozhodným pro ochranu údajů.

3. Dovozce údajů okamžitě informuje vývozce údajů o existenci právních předpisů, kterým on nebo dílčí zpracovatel podléhá, jež podle odstavce 2 brání provést přezkoumání dovozce údajů nebo dílčího zpracovatele. V tomto případě má vývozce údajů právo učinit opatření podle doložky 5 písm. b).

Doložka 9. Rozhodné právo

Doložky se řídí právem členského státu, ve kterém je usazen vývozce údajů.

Doložka 10. Změna smlouvy

Strany se zavazují, že v doložkách nebudou provádět žádné změny ani úpravy. Toto nevylučuje, aby strany v případě potřeby připojily další doložky, které se vztahují k předmětu obchodu, pokud tyto doložky nejsou v rozporu s těmito doložkami.

Doložka 11. Dílčí zpracování

1. Dovozce údajů nezadá externě žádnou ze svých činností spojených se zpracováním údajů, které jsou vykonávány jménem vývozce údajů na základě těchto doložek, bez předchozího písemného souhlasu vývozce údajů. Pokud dovozce údajů se souhlasem vývozce údajů zajišťuje plnění svých povinností podle těchto doložek subdodavatelsky, učiní tak pouze formou písemné dohody s dílčím zpracovatelem, která dílčímu zpracovateli ukládá stejné povinnosti, jako jsou povinnosti dovozce údajů podle těchto doložek (3). Neplní-li dílčí zpracovatel své povinnosti týkající se ochrany údajů na základě této písemné dohody, je dovozce údajů vůči vývozci údajů nadále plně odpovědný za splnění povinností dílčího zpracovatele podle takovéto dohody.

2. Předchozí písemná smlouva mezi dovozcem údajů a dílčím zpracovatelem zahrnuje rovněž doložku ve prospěch třetí strany stanovenou v doložce 3 pro případy, kdy subjekt údajů nemůže uplatňovat nárok na odškodnění podle odstavce 1 doložky 6 vůči vývozci údajů nebo dovozci údajů, protože ti fakticky zmizeli nebo z právního hlediska zanikli nebo jsou v platební neschopnosti, ledaže případný nástupnický subjekt převzal na základě smlouvy nebo právních předpisů veškeré právní povinnosti vývozce údajů nebo dovozce údajů. Tato odpovědnost dílčího zpracovatele vůči třetím stranám je omezena na jeho vlastní činnosti spojené se zpracováním údajů podle těchto doložek.

3. Ustanovení týkající se aspektů ochrany údajů u subdodavatelského zajišťování podle odstavce 1 se řídí právem členského státu, ve kterém je usazen vývozce údajů.

4. Vývozce údajů vede seznam dohod o dílčím zpracování, jež uzavřel podle těchto doložek a které dovozce údajů oznámil podle doložky 5 písm. j), který bude alespoň jednou ročně aktualizovat. Seznam musí být dán k dispozici orgánu dozoru pro ochranu údajů vývozce údajů.

Doložka 12. Povinnosti po ukončení poskytování služeb spojených se zpracováním osobních údajů

1. Strany se dohodly, že po ukončení poskytování služeb spojených se zpracováním údajů dovozce údajů a dílčí zpracovatel podle rozhodnutí vývozce údajů vrátí veškeré předávané osobní údaje a jejich kopie vývozci údajů, nebo provede zničení veškerých osobních údajů a předloží vývozci údajů potvrzení o jejich zničení, pokud právní předpisy vztahující se na dovozce údajů nezakazují dovozci vrácení či zničení všech nebo části předávaných osobních údajů. V takovém případě dovozce údajů zaručuje, že zajistí zachování důvěrnosti předávaných osobních údajů a že nebude přenášené osobní údaje již dále aktivně zpracovávat.

2. Dovozce údajů a dílčí zpracovatel zaručují, že na žádost vývozce údajů a/nebo orgánu dozoru dají k dispozici svá zařízení na zpracování údajů za účelem přezkoumání opatření uvedených v odstavci 1.

DODATEK Č. 1 STANDARDNÍ SMLUVNÍ DOLOŽKY

Vývozce údajů
Vývozce údajů je (popište, prosím, stručně své činnosti, které mají význam pro předávání):

Zákazník je předplatitelem cloudové služby poskytované společností SISW, která umožňuje koncovým uživatelům oprávněným zákazníkem, aby otevírali, upravovali, používali, odstraňovali, stahovali a jinak zpracovávali data zákazníka, která mohou obsahovat osobní údaje, jak je popsáno ve smlouvě a příslušné dokumentaci ke cloudové službě.

Dovozce údajů
Dovozce údajů je (popište, prosím, stručně své činnosti, které mají význam pro předávání):

Společnost Siemens Product Lifecycle Management Software Inc. sama za sebe nebo prostřednictvím svých dílčích zpracovatelů poskytuje cloudovou službu, která zahrnuje: udržování výpočetní infrastruktury ve Spojených státech a Evropské unii, ve které je cloudová služba provozována; ukládání dat zákazníka, která jsou odeslána zákazníkem do cloudové služby, do infrastruktury; monitorování dostupnosti a průběžného provozu cloudové služby a infrastruktury a udržování bezpečnosti infrastruktury, jak je stanoveno ve smlouvě a příslušné dokumentaci ke cloudové službě.

Subjekty údajů
Předávané osobní údaje se týkají těchto kategorií subjektů údajů (uveďte, prosím, podrobnosti):

Není-li vývozcem údajů výslovně písemně stanoveno jinak, mohou subjekty údajů zahrnovat koncové uživatele oprávněné zákazníkem používat cloudovou službu a ostatní pracovníky zákazníka, jejichž osobní údaje jsou uloženy v cloudové službě.

Kategorie údajů
Předávané osobní údaje se týkají těchto kategorií údajů (uveďte, prosím, podrobnosti):

Zvláštní kateorie údajů ukládaných do cloudové služby podléhají znační konfiguraci ze strany zákazníka, i když k některým společným kategoriím údajů, které lze v cloudové službě ukládat, patří mimo jiné například: jméno, e-mailová adresa, název společnosti, telefonní číslo, místo práce, národnost nebo občanství a informace týkající se přístupu ke cloudové službě a jejího používání. V závislosti na konfiguraci cloudové služby zákazníkem může být v datech zákazníka obsaženo mnoho dalších kategorií údajů.

Zvláštní kategorie údajů (jsou-li předmětem předávání)
Předávané osobní údaje se týkají těchto zvláštních kategorií údajů (uveďte, prosím, podrobnosti):

Případné zvláštní kategorie údajů, které budou uloženy v cloudové službě, budou mezi smluvními stranami sjednány ve smlouvě nebo objednávce, nebo budou stanoveny ve výkazu práce na odborné služby, který bude zákazníkovi předán jako součást zavedení cloudové služby.

Proces zpracování
Předávané osobní údaje budou předmětem těchto základních procesů zpracování (uveďte, prosím, podrobnosti):

Osobní údaje mohou být zpracovávány: jako součást běžného provozu cloudové služby, v závislosti na konfiguraci zákazníka; prostřednictvím uložení nebo archivace výpočetní infrastruktury spravované vývozcem údajů, v prostředí single-tenant nebo multi-tenant; prostřednictvím přístupu a přenosu podle pokynů vydaných cloudové službě koncovým uživatelem oprávněným zákazníkem k používání cloudové služby; a jako součást údržbových činností cloudové služby prováděné vývozcem údajů.

DODATEK Č. 2 KE STANDARDNÍM SMLUVNÍM DOLOŽKÁM

Některé nabídky cloudových služeb jsou poskytovány za odlišných podmínek, které budou v případě jejich použitelnosti uvedeny v objednávce. Jinak podnikne dovozce údajů v souvislosti s osobními údaji uloženými v systému níže popsaná technická a organizační opatření v souladu s doložkami 4(d) a 5(c) doložek.

Popis technických a organizačních bezpečnostních opatření zavedených dovozcem údajů v souladu s doložkou 4(d) a 5(c):

1. Kontrola fyzického přístupu. Neoprávněným osobám bude zamezen fyzický přístup do prostor, budov nebo místností, kde jsou umístěny systémy zpracování, které zpracovávají nebo používají osobní údaje.

   Opatření: Všechna datová centra dodržují přísné bezpečnostní postupy vykonávané bezpečnostními pracovníky, sledovacím zařízením, detektory pohybu, mechanismy kontroly přístupu a dalšími opatřeními, která brání narušení vybavení a zařízení datového centra. K systémům a infrastruktuře v zařízeních datového centra mají přístup pouze oprávnění zástupci. Pro zajištění řádného fungování je prováděna pravidelná údržba fyzického zabezpečovacího vybavení (např. pohybová čidla, kamery atd.). Pro přiblížení jsou ve všech datových centrech zavedena následující fyzická bezpečnostní opatření:

   a. Budovy jsou obecně zabezpečeny pomocí systémů kontroly přístupu (systém přístupu pomocí chytrých karet).
   b. Autorizační přihlašovací údaje, které zahrnují elektronický přístupový průkaz (pro každého zaměstnance, prodejce nebo dodavatele jedinečný) a PIN, jsou poskytovány oprávněným pracovníkům pro účely fyzického přístupu do zařízení datových center.
   c. Fyzický přístup do datových center v rámci hranic systému je prováděn pomocí elektronického systému kontroly přístupu, který se skládá ze čteček karet a klávesnic pro kód PIN pro vstup do budov a místností a pouze čteček karet pro odchod z budov a místností.
   d. Budovy, jednotlivé oblasti a okolní prostory jsou dále chráněny dalšími opatřeními v závislosti na bezpečnostní klasifikaci. Patří k nim specifické přístupové profily, video sledování, alarmové systémy proti narušitelům a systémy biometrické kontroly přístupu.
   e. Přístupová práva budou udělena oprávněným pracovníkům na individuální bázi podle níže uvedených opatření pro kontrolu přístupu k systému a datům. Totéž platí pro vstup návštěvníků. Hosté a návštěvníci budov společnosti SISW musí nahlásit svá jména na recepci a musí je doprovázet oprávnění pracovníci společnosti SISW. Společnost SISW a všichni externí poskytovatelé datových center (třetí strany) zapisují do protokolu jména a časové údaje osob vstupujících do soukromých prostor společnosti SISW v rámci datových center.
   f. Zaměstnanci a externí pracovníci společnosti SISW musí ve všech prostorách společnosti SISW nosit svou identifikační kartu.

2. Kontrola přístupu k systémům. Systémy zpracování dat používané k poskytování cloudových služeb musí být chráněny před neoprávněným použitím.

   Opatření:
   a. Společnost SISW nebo její dílčí zpracovatelé spravují prostředí tak, aby splňovalo požadavky na kontrolu přístupu (AC) předpisu NIST SP 800-53, rev. 4, a požadavky na identifikaci a ověření (IA).
   b. K udělení přístupu k citlivým systémům včetně systémů pro uložení a zpracovávání osobních údajů se používá více úrovní autorizace. Jsou zavedeny postupy k zajištění toho, aby příslušné oprávnění k přidávání, odstraňování nebo změně uživatelů měli pouze oprávnění uživatelé.
   c. Všichni uživatelé získávají přístup k systémům společnosti SISW pomocí jedinečného uživatelského jména a hesla, které musí splňovat určitá minimální kritéria komplexnosti.
   d. Společnost SISW a její dílčí zpracovatelé mají zavedeny postupy k zajištění toho, aby požadované změny oprávnění byly prováděny pouze v souladu s pravidly (např. žádná práva nejsou udělena bez autorizace). Pokud uživatel SISW změní funkci nebo společnost opustí, proběhne postup zrušení jeho přístupových práv do prostředí.
   e. Společnost SISW a dílčí zpracovatelé mají zavedena pravidla pro hesla, která zakazují sdílení hesel, upravují postup v případě prozrazení hesla, vyžadují pravidelnou změnu všech uživatelských hesel a vyžadují změnu výchozích hesel. Pro ověření jsou přidělena personalizovaná uživatelská identifikační čísla. Všechna hesla musí splňovat minimální požadavky na komplexnost a jsou uložena v zašifrované formě. V případě doménového hesla si systém vynutí každých 60 dnů změnu hesla, které splňuje minimální požadavky na složitost. Každý počítač společnosti SISW má heslem chráněný spořič obrazovky.
   f. Společnost SISW nebo její dílčí zpracovatelé automaticky provádějí kontrolu následujících událostí na účtu: vytvoření, změna, povolení, zákaz a odstranění. Správce systému pravidelně kontroluje záznamy.

g. Sítě společnosti SISW a jejích dílčích zpracovatelů jsou chráněny před veřejným internetem bránami firewall.
h. Společnost SISW a její dílčí zpracovatelé používají na všech přístupových bodech do firemní sítě, pro e-mailové účty a na všech souborových serverech a všech pracovních stanicích aktuální antivirový software.
i. Společnost SISW a její subdodavatelé zavádějí správu bezpečnostních oprav, aby zajistili používání příslušných bezpečnostních aktualizací.
j. Úplný vzdálený přístup k firemní síti společnosti SISW a kritické infrastruktuře je chráněn silným vícefaktorovým ověřováním.

3. Kontrola přístupu k datům. Pracovníci oprávnění používat systémy zpracování dat získají přístup pouze k osobním údajům, ke kterým mají právo získat přístup, a osobní údaje se nesmí v průběhu zpracování, používání a uložení číst, kopírovat, měnit ani odstraňovat bez oprávnění.

   Opatření:
   a. Přístup k osobním, důvěrným nebo citlivým informacím se poskytuje na základě potřeby znát tyto údaje. Jinými slovy, zaměstnanci nebo externí třetí osoby mají přístup k těm informacím, které potřebují k tomu, aby mohly vykonat svoji práci. Společnost SISW používá autorizační koncepty, které dokumentují, jak byla oprávnění přidělena a která oprávnění byla přidělena. Všechny osobní, důvěrné nebo jinak citlivé údaje jsou chráněny v souladu s bezpečnostními zásadami a standardy společnosti SISW.
   b. Všechny produkční servery jakékoliv cloudové služby společnosti SISW jsou provozovány v příslušných datových centrech. Bezpečnostní opatření, která chrání aplikace zpracovávající osobní, důvěrné a jiné citlivé informace, jsou pravidelně kontrolována. Společnost SISW za tímto účelem také zavádí pravidelné externí audity za účelem ověření, zda jsou tato opatření používána správným způsobem.
   c. Společnost SISW nedovoluje do systémů používaných pro cloudovou službu instalaci osobního softwaru nebo jiného softwaru, který nebyl společností SISW schválen..
   d. Pokud by nastal požadavek na předání dat kvůli závadě základových paměťových médií, po dokončení takového předání budou vadná paměťová média vymazána (v případě magnetického úložiště) nebo skartována (v případě pevných nebo optických úložišť).

4. Kontrola přenosu dat. Osobní údaje se nesmí během předání bez oprávnění číst, kopírovat, měnit ani odstraňovat.

   Opatření:
   a. Společnost SISW nebo její dílčí zpracovatelé budou spravovat infrastrukturu a konfiguraci tak, aby splňovaly požadavky na systém podle předpisu NIST SP 800-53, rev. 4, a požadavky na ochranu komunikací (SC). To zahrnuje systémy zabránění narušení prostřednictvím sítě (NIPS) a brány firewall na hranicích systému na ochranu před škodlivou komunikací na vnějších hranicích infrastruktury. NIPS a brány firewall jsou konfigurovány podle norem DISA STIG. Data jsou při přenosu šifrována pomocí kryptografických modulů, které splňují normu FIPS 140-2.
   b. Tam, kde jsou nosiče dat fyzicky přepravovány, má společnost SISW zavedena odpovídající opatření k zajištění sjednaných úrovní služby (např. šifrování a olovem vyložené přepravní obaly).
   c. Přenos osobních údajů prostřednictvím interních sítí společnosti SISW je chráněn stejným způsobem jako u ostatních důvěrných dat podle bezpečnostních zásad společnosti SISW.
   d. Při přenosu údajů mezi společností SISW a zákazníkem jsou opatření na ochranu osobních údajů pro přenášené osobní údaje stejná jako ve smlouvě nebo příslušné dokumentaci pro cloudovou službu. Platí to pro fyzické předání dat i předání dat prostřednictvím sítě. Zákazník přebírá odpovědnost za přenos dat od demarkačního bodu SISW (např. odchozí brána firewall datového centra, které je hostitelem cloudové služby).

5. Kontrola zadávání dat. Cloudová služba bude umožňovat zpětně určit, zda a kým byl proveden přístup k osobním údajům, jejich změna nebo odstranění z infrastruktury použité k poskytování cloudové služby.

   Opatření:
   a. Společnost SISW povoluje svým oprávněným pracovníkům přístup k osobním údajům pouze tak, jak to vyžaduje výkon jejich práce. Společnost SISW zavedla v nejširším možném rozsahu podporovaném cloudovou službou systém zaznamenávání pro vstupů, změn a odstranění nebo zablokování osobních údajů společností SISW nebo jejími dílčími zpracovateli.
   b. Kontrolní stopa průběhu zpracování je dostatečně podrobná k tomu, aby umožnila rekonstrukci událostí v případě neoprávněné aktivity nebo poruchy nebo podezření na ně. Každý záznam událostí operačního systému obsahuje typ události, časové razítko, zdroj události, místo události, výsledek události a uživatele spojeného s událostí.

6. Ovládání úlohy. Osobní údaje budou zpracovávány výhradně v souladu s podmínkami smlouvy a případnými souvisejícími pokyny poskytnutými zákazníkem.

   Opatření:
   a. Společnost SISW používá kontroly a procesy k zajištění dodržování smluv mezi společností SISW a jejími zákazníky, dílčími zpracovateli nebo jinými poskytovateli služeb.
   b. Data zákazníka budou podléhat přinejmenším stejné úrovni ochrany jako důvěrné informace podle normy společnosti SISW pro klasifikaci informací.
   c. Všichni zaměstnanci a smluvní partneři společnosti SISW jsou smluvně zavázáni respektovat důvěrnost všech citlivých informací včetně obchodních tajemství zákazníků a partnerů společnosti SISW.

7. Kontrola dostupnosti. Osobní údaje budou chráněny před náhodným nebo neoprávněným zničením nebo ztrátou.

   Opatření:
   a. Společnost SISW používá zálohovací postupy a další opatření, která zajišťují v případě potřeby rychlou obnovu systémů kritických pro podnikání.
   b. Společnost SISW se při zajištění dostupnosti napájení datových center spoléhá na globální poskytovatele cloudových služeb.
   c. Společnost SISW stanovila pro cloudové služby havarijní plány a také strategie obnovy po pohromách.

8. Kontrola oddělení dat. Osobní údaje shromažďované pro různé účely mohou být zpracovávány samostatně.

   Opatření:
   a. Společnost SISW v případě potřeby využije technické možnosti zapojeného softwaru (např. sdílení typu „multi-tenancy“ nebo samostatné systémové prostředí) k dosažení oddělení osobních údajů zákazníka a údajů ostatních zákazníků.
   b. Společnost SISW vede pro jednotlivé zákazníky vyhrazené instance (s logickým nebo fyzickým oddělením).
   c. Zákazník (včetně svých přidružených společností) má přístup pouze ke své vlastní zákaznické instanci (instancím).

9. Kontrola integrity dat. Zajišťuje, že osobní údaje zůstanou během zpracování nedotčené, úplné a aktuální:

   Opatření: Společnost SISW zavedla jako ochranu před neoprávněnými změnami vícevrstvou obrannou strategii. Jde o kontrolní prvky uvedené ve výše popsaných částech týkajících se kontroly a opatření. Konfigurace bran firewall povede k vícečetným síťovým segmentům, které oddělí veřejný a soukromý přístup. Každé nastavené pravidlo sítě firewall bude mít určité kontroly přístupu specifikující povolenou komunikaci mezi těmito segmenty.

   a. Centrum monitorování bezpečnosti: K upozornění, vyšetření a v případě potřeby vyrozumění a pomoci při nápravě případného bezpečnostního incidentu bude použit software automatického zjišťování narušení ve spojení s dalšími prostředky ochrany bezpečnosti a forenzním softwarem a postupy pro zajištění bezpečnosti.
   b. Antivirový software: všechny systémy budou mít aktuální definice virů na ochranu proti virům, červům, trojským koním a ostatním formám škodlivého softwaru.
   c. Zálohování a obnova: všechny systémy budou mít základní úroveň zálohovacích snímků dat a konfigurace. Kde to bude použitelné, společnost SISW a její dílčí zpracovatelé budou také obsluhovat instanci zákazníka s konfigurací vysoké dostupnosti, což zajistí, že data budou uložena ve dvou samostatných datových centrech dostatečně od sebe vzdálených.
   d. Pravidelné externí audity za účelem prověření bezpečnostních opatření. Společnost SISW a její dílčí zpracovatelé budou absolvovat pravidelné externí audity za účelem ověření výše uvedených bezpečnostních opatření.