CONTRATTO PER IL TRATTAMENTO DEI DATI

Il presente Contratto per il trattamento dei dati ("Contratto") è stipulato tra Siemens Product Lifecycle Management Software Inc., anche denominata Siemens Industry Software (nel presente documento indicata come “SISW”), e il cliente che ha dichiarato la propria accettazione ai termini e alle condizioni del presente Contratto ("Cliente"). SISW mantiene il diritto di servirsi delle proprie società affiliate nel perseguimento di qualsiasi dei propri diritti e nell'adempimento di qualsiasi dei propri obblighi derivanti dal presente Contratto. Pertanto, il termine "SISW" utilizzato nel presente documento può riferirsi anche alle società affiliate, di proprietà o controllate direttamente o indirettamente da Siemens Product Lifecycle Management Software Inc. e autorizzate da Siemens Product Lifecycle Management Software Inc. a distribuire i servizi cloud di SISW ("Servizio cloud).

Il Cliente sarà l'unico responsabile della determinazione del tipo di dati e delle persone interessate dal trattamento e dovrà assicurare la legittimità di tale trattamento per mezzo del Servizio cloud. Il Cliente sarà inoltre responsabile dell'eventuale correzione, eliminazione o blocco dei dati personali, utilizzando le funzionalità offerte dal Servizio cloud. Il Cliente può esportare ed eliminare i propri dati, inclusi i dati personali, utilizzando le funzionalità offerte dal Servizio cloud. Alla risoluzione del presente Contratto per il trattamento dei dati, il Cliente avrà 30 giorni per inviare una richiesta scritta a SISW per richiedere che i Dati del cliente vengano resi disponibili per il download da parte del Cliente. Alla scadenza del periodo stabilito da SISW in risposta a tale richiesta, i dati del cliente rimanenti verranno sottoposti a eliminazione e non saranno più disponibili per il Cliente. SISW e il Cliente accettano che, nell'ambito del Servizio cloud, il diritto del Cliente di inviare istruzioni verrà esercitato esclusivamente utilizzando le funzionalità offerte dal Servizio cloud. Istruzioni aggiuntive relative ai dati del Cliente richiedono un accordo scritto separato tra SISW e il Cliente, incluso un accordo sulle eventuali spese che il Cliente deve sostenere per adempiere a tali istruzioni. Il Cliente si impegna a non caricare né memorizzare alcuna informazione protetta sulla salute (PHI, Protected Health Information) nel Servizio cloud, a meno che SISW e il Cliente abbiano sottoscritto un accordo scritto separato che consente espressamente la memorizzazione di informazioni PHI nel Servizio cloud.

Nella fornitura del Servizio cloud, in relazione al sistema di produzione, SISW adempierà alle misure tecniche e organizzative descritte nell'Appendice 2 fino all'Exhibit A del presente Contratto per il trattamento dei dati. I sistemi non di produzione correlati con il Servizio cloud possono adempiere o meno alle misure descritte nell'Appendice 2 fino all'Exhibit A. Inoltre, SISW può modificare periodicamente le misure tecniche e organizzative applicabili al sistema di produzione, purché tali modifiche non incidano negativamente sul livello di protezione consentito da tali misure in modo sostanziale. SISW impedirà al proprio personale di raccogliere, elaborare o utilizzare dati personali senza autorizzazione e impiegherà per l'elaborazione dei dati personali del Cliente esclusivamente personale specificamente istruito in conformità ai requisiti di protezione della privacy dei dati.

SISW avrà diritto di assumere subincaricati per lo svolgimento del Servizio cloud. Nella misura in cui l'accesso di subincaricati ai dati personali del Cliente non può essere escluso, SISW fornirà al Cliente su richiesta un elenco di tali subincaricati e le loro rispettive ubicazioni, inoltre aggiornerà tale elenco secondo quanto richiesto prima di concedere l'accesso di ogni nuovo subincaricato ai dati personali del Cliente. In caso il Cliente ragionevolmente obietti a qualsiasi nuovo subincaricato, il Cliente dovrà informare SISW di tale obiezione e, se SISW insisterà con l'assunzione del nuovo subincaricato, il Cliente avrà il diritto di risolvere il presente Contratto per il trattamento dei dati per giusta causa. Nella misura in cui l'assunzione di tale subincaricato richieda un trasferimento internazionale di dati personali, SISW tenterà di fare sì che tale subincaricato mantenga un livello di protezione dei dati adeguato in relazione a tali dati personali.

SISW verificherà regolarmente il rispetto delle misure tecniche e organizzative applicabili e, su ragionevole richiesta del Cliente, confermerà al Cliente che le misure tecniche e organizzative applicabili sono state rispettate. In caso il Cliente abbia motivo di ritenere che una conferma emessa da SISW sia errata, il Cliente avrà il diritto di verificare il rispetto delle misure tecniche e organizzative pianificando un controllo con SISW, con ragionevole preavviso. Tale controllo verrà svolto a spese del Cliente.

SISW e il Cliente accettano che qualsiasi trasferimento di dati personali del Cliente da paesi dell'Unione Europea a paesi esterni all'UE che, in base al giudizio dell'UE, non dispongono di un livello adeguato di protezione dei dati personali verrà condotto in base alle clausole contrattuali standard dell'UE, stabilite nell'Exhibit A e completamente incorporate nel presente documento. In caso di conflitto tra i termini del presente Contratto per il trattamento dei dati e i termini delle clausole contrattuali standard, avranno la priorità le clausole contrattuali standard. Le clausole contrattuali standard saranno regolate dalle leggi dello stato membro dell'UE in cui ha sede l'esportatore dei dati (come definito nell'Exhibit A).

Exhibit A
Clausole contrattuali standard dell'UE

Ai fini dell'Articolo 26(2) della Direttiva 95/46/CE per il trasferimento dei dati personali a responsabili del trattamento dati con sedi in paesi terzi che non assicurano un livello adeguato di protezione dei dati

da parte e tra

il Cliente e/o una società affiliata del Cliente con sede nell'UE

(di seguito denominato "**esportatore di dati**")

e

Siemens Product Lifecycle Management Software Inc., anche denominata Siemens Industry Software, incluse eventuali società affiliate di proprietà o controllate direttamente o indirettamente dalla società principale del gruppo Siemens Product Lifecycle Management Software Inc. e autorizzate da Siemens Product Lifecycle Management Software Inc. a elaborare dati per suo conto

(di seguito denominata, "**importatore di dati**")

ognuna indicata come "parte" e insieme come "le parti",

HANNO ACCETTATO le seguenti clausole contrattuali ("Clausole") al fine di addurre garanzie adeguate in relazione alla protezione della privacy, dei diritti fondamentali e della libertà delle persone per il trasferimento dall'esportatore all'importatore dei dati personali specificati nell'Appendice 1.

Sezione 1. Definizioni

Ai fini delle Clausole:

(a) "dati personali", "categorie speciali di dati", "trattare/trattamento", "responsabile del controllo", "responsabile del trattamento", "persona interessata" e "autorità di controllo" hanno lo stesso significato che presentano nella Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 sulla protezione delle persone in merito al trattamento dei dati personali e alla libera circolazione di tali dati;

(b) per "esportatore dei dati" si intende il responsabile del controllo che trasferisce i dati personali;

(c) per "importatore dei dati" si intende il responsabile del trattamento che accetta di ricevere i dati dall'esportatore di dati i dati personali destinati al trattamento per suo conto dopo il trasferimento in conformità alle istruzioni e ai termini delle Clausole e che non è soggetto a un sistema di un paese terzo che garantisca una protezione adeguata come previsto dall'Articolo 25(1) della Direttiva 95/46/CE;

(d) per "subincaricato" 'si intende qualsiasi responsabile del trattamento assunto dall'importatore dei dati o un altro subincaricato dell'importatore dei dati che accetta di ricevere dall'importatore dei dati, o da qualsiasi altro suo subincaricato, dati personali destinati esclusivamente ad attività di trattamento da svolgere per conto dell'esportatore dei dati dopo il trasferimento in conformità alle sue istruzioni, ai termini delle Clausole e ai termini del contratto scritto di subappalto;

(e) per "legge per la protezione dei dati applicabile" si intendono le normative che proteggono i diritti fondamentali e la libertà delle persone e, in particolare, il loro diritto alla privacy in relazione al trattamento dei dati personali, applicabili a un responsabile del controllo dei dati nello stato membro in cui l'esportatore dei dati ha sede;

(f) per "misure tecniche e organizzative" si intendono le misure volte a proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla divulgazione o accesso non autorizzati, in particolare dove il trattamento include la trasmissione dei dati su una rete, e da tutte le altre forme illegali di trattamento.

Sezione 2. Dettagli del trasferimento

I dettagli del trasferimento e, in particolare, le speciali categorie dei dati personali, dove applicabili, sono specificati nell'Appendice 1, che costituisce una parte integrante delle Clausole.

Sezione 3. Clausola del terzo beneficiario

1. La persona interessata può applicare nei confronti dell'esportatore dei dati la presente Clausola, la Clausola 4 da (b) a (i), la Clausola 5 da (a) a (e) e da (g) a (j), la Clausola 6(1) e (2), la Clausola 7, la Clausola 8(2) e le Clausole da 9 a 12 come terzo beneficiario.

2. La persona interessata può applicare nei confronti dell'importatore dei dati la presente Clausola, la Clausola 5 da (a) a (e) e (g), la Clausola 6, la Clausola 7, la Clausola 8(2), e le Clausole da 9 a 12, nei casi in cui l'esportatore dei dati risulti di fatto scomparso o abbia cessato di esistere per la legge, a meno che un'entità successore ne abbia assunto per intero gli obblighi legali per contratto o a norma di legge e pertanto tale ente assume i diritti e gli obblighi dell'esportatore dei dati, nel qual caso la persona interessata può applicare tali clausole nei confronti di tale entità.

3. La persona interessata può applicare nei confronti del subincaricato la presente Clausola, la Clausola 5 da (a) a (e) e (g), la Clausola 6, la Clausola 7, la Clausola 8(2), e le Clausole da 9 a 12, nei casi in cui sia l'esportatore dei dati che l'importatore dei dati risultino di fatto scomparsi o abbiano cessato di esistere per la legge o siano diventati insolventi, a meno che un'entità successore ne abbia assunto per intero gli obblighi legali per contratto o a norma di legge e pertanto tale ente assume i diritti e gli obblighi dell'esportatore dei dati, nel qual caso la persona interessata può applicare tali clausole nei confronti di tale entità. Tale responsabilità del terzo del subincaricato sarà limitata alle relative operazioni di trattamento ai sensi delle Clausole.

4. Le parti non impediscono a una persona interessata di essere rappresentata da un'associazione o da un altro ente se la persona interessata lo desidera espressamente e se ciò è consentito dalla legge nazionale.

Sezione 4. Obblighi dell'esportatore di dati

L'esportatore di dati accetta e garantisce:

(a) che il trattamento, incluso il trasferimento stesso, dei dati personali è stato e continuerà a essere effettuato in conformità alle disposizioni relative della legge sulla protezione dei dati applicabile (e, dove applicabile, che la sede dell'esportatore dei dati è stata notificata alle autorità competenti dello stato membro) e che non viola le clausole relative di tale stato;

(b) di essere stato istruito e che, per l'intera durata dei servizi di trattamento dei dati personali, istruirà l'importatore dei dati per il trattamento dei dati personali trasferiti solo per conto dell'esportatore dei dati e in conformità alla legge sulla protezione dei dati applicabile e alle Clausole;

(c) che l'importatore dei dati fornirà garanzie sufficienti relativamente alle misure di sicurezza tecniche e organizzative specificate nell'Appendice 2 del presente contratto;

(d) che dopo la valutazione dei requisiti della legge sulla protezione dei dati applicabile, le misure di sicurezza risultano appropriate per proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla divulgazione o accesso non autorizzati, in particolare dove il trattamento include la trasmissione dei dati su una rete, e da tutte le altre forme illegali di trattamento e che tali misure assicurano un livello di sicurezza appropriato per i rischi presentati dal trattamento e dalla natura dei dati da proteggere, sulla base del livello tecnologico e del costo della loro implementazione;

(e) che assicurerà la conformità alle misure di sicurezza;

(f) che, se il trasferimento include categorie speciali di dati, la persona interessata ne è stata informata o verrà informata prima del trasferimento o dopo, non appena possibile, del fatto che i suoi dati possono venire trasmessi a un paese terzo che non fornisce una protezione adeguata in base a quanto previsto dalla Direttiva 95/46/CE;

(g) di inoltrare qualsiasi notifica ricevuta dall'importatore di dati o da qualsiasi subincaricato conformemente alla Clausola 5(b) e alla Clausola 8(3) all'autorità di controllo della protezione dei dati se l'esportatore dei dati decide di continuare il trasferimento o di revocare la sospensione;

(h) di rendere disponibile su richiesta alle persone interessate una copia delle Clausole, ad eccezione dell'Appendice 2, e una descrizione riepilogativa delle misure di sicurezza, nonché una copia di qualsiasi contratto di servizi di subincarico per il trattamento che sia stato stipulato in conformità alle Clausole, a meno che le clausole o il contratto contengano informazioni commerciali, nel qual caso può rimuovere tali informazioni commerciali;

(i) che, in caso di subincarico di trattamento, l'attività di trattamento verrà svolta in conformità alla Clausola 11 da parte di un subincaricato che fornisce almeno lo stesso livello di protezione dei dati personali e dei diritti della persona interessata fornito dall'importatore dei dati ai sensi delle Clausole e

(j) che assicurerà la conformità alla Clausola 4 da (a) a (i).

Sezione 5. Obblighi dell'importatore di dati

L'importatore di dati accetta e garantisce:

(a) di trattare i dati personali esclusivamente per conto dell'esportatore dei dati e in conformità alle sue istruzioni e alle Clausole; se non potesse fornire tale conformità per qualsiasi motivo, accetta di informare prontamente l'esportatore dei dati della sua mancata conformità, nel qual caso l'esportatore dei dati avrà il diritto di sospendere il trasferimento dei dati e/o di risolvere il contratto;

(b) che non ha motivo di ritenere che la legislazione applicabile gli impedisca di completare le istruzioni ricevute dall'esportatore dei dati e i propri obblighi in base al contratto e che nel caso di modifica di questa legislazione che possa avere un notevole effetto contrario sulle garanzie e sugli obblighi forniti dalle Clausole, notificherà prontamente la modifica all'esportatore dei dati non appena ne avrà conoscenza, nel qual caso l'esportatore avrà diritto di sospendere il trasferimento dei dati e/o risolvere il contratto;

(c) di aver implementato le misure di sicurezza tecniche e organizzative specificate nell'Appendice 2 prima di trattare i dati personali trasferiti;

(d) che informerà prontamente l'esportatore dei dati in caso di:

(i) qualsiasi richiesta legalmente vincolate di divulgazione di dati personali presentata da forze dell'ordine, se non diversamente proibito, ad esempio il divieto previsto dal diritto penale per mantenere la riservatezza di un'indagine di polizia,
(ii) qualsiasi accesso accidentale o non autorizzato e
(iii) qualsiasi richiesta ricevuta direttamente dalle persone interessate, senza rispondere a tale richiesta, a meno che sia stato diversamente autorizzato in tal senso;

(e) di trattare prontamente e adeguatamente tutte le richieste presentate dall'esportatore dei dati in relazione al trattamento dei dati personali soggetti al trasferimento e di attenersi a quanto consigliato dall'autorità di controllo in merito al trattamento dei dati trasferiti;

(f) alla richiesta dell'esportatore di dati di sottoporre le proprie strutture di trattamento dei dati al controllo delle attività di trattamento previste dalle Clausole che dovrà essere condotto dall'esportatore dei dati o da un ente di ispezione formato da membri indipendenti e in possesso delle qualifiche professionali richieste, vincolati da un obbligo di riservatezza, selezionati dall'esportatore dei dati, dove applicabile, in accordo con l'autorità di controllo;

(g) di rendere disponibile su richiesta alla persona interessata una copia delle Clausole, o di qualsiasi contratto esistente di subincarico di trattamento, a meno che le Clausole o il contratto contengano informazioni commerciali, nel qual caso potrà rimuovere tali informazioni commerciali, ad eccezione dell'Appendice 2 che sarà sostituita da una descrizione riepilogativa delle misure di sicurezza nei casi in cui la persona interessata non possa ottenere una copia dall'esportatore dei dati;

(h) di aver, in caso di subincarico di trattamento, precedentemente informato l'esportatore dei dati e di averne ottenuto il previo consenso scritto;

(i) che i servizi di trattamento forniti dal subincaricato verranno svolti in conformità alla Clausola 11;

(j) di inviare prontamente all'esportatore dei dati una copia di ogni contatto di subincarico che conclude ai sensi delle Clausole.

Sezione 6. Responsabilità

1. Le parti accettano che qualsiasi persona interessata che abbia subito danni a causa di una violazione, di qualsiasi parte o subincaricato, degli obblighi riportati nella Clausola 3 o nella Clausola 11 ha diritto a ricevere l'indennizzo dall'esportatore dei dati per i danni subiti.

2. Se una persona interessata non è in grado di presentare la richiesta di risarcimento in conformità al paragrafo 1 nei confronti dell'esportatore dei dati, in seguito alla violazione da parte dell'importatore dei dati o di un suo subincaricato di qualsiasi obbligo riportato nella Clausola 3 o nella Clausola 11, poiché l'esportatore dei dati è di fatto scomparso, ha cessato di esistere per la legge o è diventato insolvente, l'importatore dei dati accetta che la persona interessata può presentare una richiesta di risarcimento nei suoi confronti come se si trattasse dell'esportatore dei dati, a meno che un'entità successore abbia assunto per intero gli obblighi legali dell'esportatore dei dati per contratto o a norma di legge, nel qual caso la persona interessata può esercitare i suoi diritti nei confronti di tale entità.

   L'importatore dei dati non può fare affidamento su una violazione di un subincaricato dei suoi obblighi per evitare le proprie responsabilità.

3. Se una persona interessata non è in grado di presentare una richiesta di risarcimento nei confronti dell'esportatore dei dati o dell'importatore dei dati come indicato nei paragrafi 1 e 2 in seguito alla violazione da parte del subincaricato di qualsiasi dei suoi obblighi riportati nella Clausola 3 o nella Clausola 11 poiché sia l'esportatore che l'importatore dei dati sono di fatto scomparsi, hanno cessato di esistere per la legge o sono diventati insolventi, il subincaricato accetta che la persona interessata può presentare una richiesta di risarcimento nei confronti del subincaricato del trattamento dei dati in merito alle operazioni di trattamento da lui svolte ai sensi delle Clausole come se si trattasse dell'esportatore o dell'importatore dei dati, a meno che un'entità successore abbia assunto per intero gli obblighi legali dell'esportatore o dell'importatore dei dati per contratto o a norma di legge, nel qual caso la persona interessata può esercitare i suoi diritti nei confronti di tale entità. La responsabilità del subincaricato sarà limitata alle relative operazioni di trattamento ai sensi delle Clausole.

Sezione 7. Mediazione e giurisdizione

1. L'importatore di dati accetta che se la persona interessata esercita nei suoi confronti diritti di terzo beneficiario e/o richiede l'indennizzo per i dati ai sensi delle Clausole, l'importatore dei dati accetterà la decisione della persona interessata:

   (a) di sottoporre la controversia a mediazione, da parte di una persona indipendente o, dove applicabile, da parte dell'autorità di controllo;

   (b) di sottoporre la controversia ai tribunali dello stato membro in cui l'esportatore di dati ha sede.

2. Le parti accettano che la scelta decisa dalla persona interessata non pregiudicherà i suoi diritti sostanziali e procedurali di cercare tutele ai sensi di altre normative del diritto nazionale e internazionale.

Sezione 8. Cooperazione con le autorità di controllo

1. L'esportatore di dati accetta di depositare una copia del presente contratto presso l'autorità di controllo dietro sua richiesta o se tale deposito è richiesto ai sensi della legge per la protezione dei dati applicabile.

2. Le parti accettano che l'autorità di controllo abbia il diritto di effettuare un controllo dell'importatore dei dati e di qualsiasi subincaricato, il quale è soggetto alle stesse condizioni che sarebbero applicate a un controllo dell'esportatore dei dati ai sensi della legge sulla protezione dei dati applicabile.

3. L'importatore dei dati dovrà informare prontamente l'esportatore dei dati dell'esistenza di normative applicabili all'importatore dei dati o a qualsiasi subincaricato che impediscono lo svolgimento di un controllo dell'importatore dei dati o di qualsiasi subincaricato, come previsto al paragrafo 2. In tale caso, l'esportatore dei dati avrà il diritto di intraprendere le misure previste nella Clausola 5 (b).

Sezione 9. Legge applicabile

Le Clausole saranno regolate dalla legge dello stato membro in cui l'esportatore dei dati ha sede.

Sezione 10. Variazione del contratto

Le parti si impegnano a non variare né modificare le Clausole. Ciò non impedisce alle parti di aggiungere clausole su problemi relativi all'attività aziendale quando richiesto, purché non siano in conflitto con le Clausole.

Sezione 11. Subincarico di trattamento

1. L'importatore dei dati non potrà subappaltare alcuna delle operazioni di trattamento eseguite per conto dell'esportatore dei dati ai sensi delle Clausole senza il previo consenso scritto dell'esportatore dei dati. Nel caso in cui l'importatore dei dati subappalti i propri obblighi previsti dalle Clausole con il consenso dell'esportatore dei dati, dovrà redigere un contratto scritto con il subincaricato che gli impone gli stessi obblighi previsti per l'importatore dei dati ai sensi delle Clausole. Nel caso in cui il subincaricato non adempia ai suoi obblighi di protezione dei dati previsti da tale contratto scritto, l'importatore dei dati resterà completamente responsabile nei confronti dell'esportatore dei dati per l'adempimento degli obblighi del subincaricato ai sensi di tale contratto.

2. Il precedente contratto scritto tra l'importatore dei dati e il subincaricato dovrà anche prevedere una clausola di terzo beneficiario, come previsto dalla Clausola 3, per i casi in cui la persona interessata non sia in grado di presentare una richiesta di risarcimento come indicato nel paragrafo 1 della Clausola 6 nei confronti dell'esportatore o dell'importatore dei dati poiché essi sono di fatto scomparsi, hanno cessato di esistere per la legge o sono diventati insolventi e nessun'entità successore ha assunto per intero gli obblighi legali dell'esportatore o dell'importatore dei dati per contratto o a norma di legge. Tale responsabilità del terzo del subincaricato sarà limitata alle relative operazioni di trattamento ai sensi delle Clausole.

3. Le disposizioni relative agli aspetti di protezione dei dati per il subincarico di trattamento del contratto indicato al paragrafo 1 saranno regolate dalla legge dello stato membro in cui l'esportatore dei dati ha sede.

4. L'esportatore dei dati dovrà tenere un elenco dei contratti di subincaricato di trattamento stipulati ai sensi delle Clausole e notificati dall'importatore dei dati conformemente alla Clausola 5 (j) che dovrà essere aggiornato almeno una volta all'anno. L'elenco sarà disponibile all'autorità di controllo della protezione dei dati dell'esportatore dei dati.

Sezione 12. Obbligo dopo il termine dei servizi di trattamento dei dati personali

1. Le parti accettano che al termine della fornitura dei servizi di trattamento dei dati, l'importatore dei dati e il subincaricato dovranno, a scelta dell'esportatore dei dati, restituire tutti i dati personali trasferiti e le copie relative all'esportatore dei dato o distruggere tutti i dati personali e certificare all'esportatore dei dati tale operazione, a meno che le normative applicabili all'importatore dei dati non gli impediscano di restituire o distruggere, completamente o parzialmente i dati personali trasferiti. In tal caso, l'importatore dei dati assicura che garantirà la riservatezza dei dati personali trasferiti e che non li tratterà più attivamente.

2. L'importatore dei dati e il subincaricato garantiscono che, su richiesta dell'esportatore dei dati e/o dell'autorità di controllo, sottoporrà le proprie strutture di trattamento dei dati a un controllo delle misure indicate nel paragrafo 1.

APPENDICE 1 ALLE CLAUSOLE CONTRATTUALI STANDARD

Esportatore dei dati
L'esportatore dei dati è (specificare brevemente le attività relative al trasferimento):

Il Cliente è un sottoscrittore di un Servizio cloud fornito da SISW che consente agli utenti finali autorizzati dal Cliente di inserire, modificare, utilizzare, rimuovere, scaricare e diversamente trattare i Dati del cliente che possono includere dati personali, come descritto nel Contratto e nella documentazione relative per il Servizio cloud.

Importatore dei dati
L'importatore dei dati è (specificare brevemente le attività relative al trasferimento):

Siemens Product Lifecycle Management Software Inc., per conto proprio e/o tramite subincaricati, fornisce il Servizio cloud che include: mantenimento dell'infrastruttura di elaborazione negli Stati Uniti e nell'Unione Europea mediante cui il Servizio cloud è gestito; memorizzazione nell'infrastruttura dei Dati del cliente che vengono caricati nel Servizio cloud dal Cliente; monitoraggio della disponibilità e del funzionamento costante dell'infrastruttura e mantenimento della sicurezza dell'infrastruttura, come stabilito nel Contratto e nella documentazione relativa per il Servizio cloud.

Persone interessate
I dati personali trasferiti riguardano le seguenti categorie di persone interessate (specificare):

Se non diversamente specificato per iscritto dall'esportatore dei dati, le persone interessate includono gli utenti finali autorizzati dal Cliente a utilizzare il Servizio cloud e altro personale del Cliente i cui dati personali sono memorizzati nel Servizio cloud.

Categorie di dati
I dati personali trasferiti riguardano le seguenti categorie di dati (specificare):

Le categorie di dati specifiche da memorizzare nel Servizio cloud sono soggette a una notevole configurazione da parte del Cliente, tuttavia alcune categorie di comuni di dati che possono essere memorizzate nel Servizio cloud sono, in via esemplificativa: nome, indirizzo email, ragione sociale, numero di telefono, sede dell'azienda, nazionalità o cittadinanza e informazioni relative all'accesso e all'utilizzo del Servizio cloud. A seconda della configurazione del cliente del Servizio cloud, nei Dati del cliente possono essere presenti molte altre categorie di dati.

Categorie specifiche di dati (se applicabile)
I dati personali trasferiti riguardano le seguenti categorie speciali di dati (specificare):

Qualsiasi categoria speciale di dati da memorizzare nel Servizio cloud si atterrà a quanto concordato tra le parti nel Contratto in un Ordine o a quanto stabilito in una dichiarazione di lavoro per sevizi professionali da fornire al Cliente come parte della distribuzione del Servizio cloud.

Operazioni di trattamento
I dati personali trasferiti saranno soggetti alle seguenti attività di trattamento di base (specificare):

I dati personali possono essere trattati: come parte del normale funzionamento del Servizio cloud, a seconda della configurazione del Cliente; tramite memorizzazione e/o archiviazione sull'infrastruttura di elaborazione gestita dall'esportatore di dati, in ambienti single-tenant o multi-tenant; tramite accesso o trasmissione conformemente alle istruzioni inviate al Servizio cloud da un utente finale autorizzato dal Cliente a utilizzare il Servizio cloud; come parte delle operazioni di mantenimento del Servizio cloud effettuate dall'esportatore di dati.

APPENDICE 2 ALLE CLAUSOLE CONTRATTUALI STANDARD

Alcune offerte di Servizi cloud vengono fornite con termini diversi i quali, se applicabile, verranno stabiliti in un Ordine. In caso contrario, l'importatore dei dati adotterà le misure tecniche e organizzative descritte di seguito in merito ai dati personali memorizzati nel Sistema, conformemente alle Clausole 4(d) e 5(c) delle Clausole.

Descrizione delle misure di sicurezza tecniche e organizzative implementate dall'importatore dei dati conformemente alle Clausole 4(d) e 5(c):

1. Controllo dell'accesso fisico. Alle persone non autorizzate non sarà consentito ottenere l'accesso fisico a sedi, edifici o sale in cui sono ubicati i sistemi di elaborazione dati che trattano e/o utilizzano i dati personali.

   Misure: Tutti i centri dati aderiscono alle rigide procedure di sicurezza applicate dal personale di sicurezza, dall'apparecchiatura di sorveglianza, da rilevatori di movimento, da meccanismi di controllo dell'accesso e da altre misure per impedire la violazione di apparecchiature e strutture del centro dati. Solo i rappresentati autorizzati hanno accesso ai sistemi e all'infrastruttura all'interno delle strutture del centro dati. Per assicurarne l'adeguata funzionalità, le apparecchiature fisiche di sicurezza (ad es. sensori di movimento, telecamere e così via) sono sottoposte a regolare manutenzione. In dettaglio, le seguenti misure di sicurezza fisica sono implementate in tutti i centri dati:

   a. In generale, gli edifici sono protetti mediante sistemi di controllo d'accesso (sistema di accesso tramite smart card).
   b. Al personale autorizzato sono fornite credenziali di autorizzazione che includono un badge elettronico di accesso (esclusivo per il dipendente, il fornitore o l'appaltatore) e un PIN per consentire l'accesso fisico alle strutture del centro dati.
   c. L'accesso fisico ai centri dati all'interno dei confini del sistema è regolato da un sistema elettronico di controllo dell'accesso, costituito da lettori di schede e tastiere per PIN situati negli ingressi di edifici e sale e di soli lettori di schede sulle uscite di edifici e sale.
   d. A seconda della classificazione di sicurezza, gli edifici, le singole aree e gli stabilimenti circostanti sono ulteriormente protetti da misure aggiuntive. Queste includono profili di accesso specifici, videosorveglianza, sistemi di allarme anti-intrusione e sistemi biometrici di controllo dell'accesso.
   e. I diritti di accesso verranno concessi al personale autorizzato su base individuale conformemente alle misure di Controllo dell'accesso a sistema e dati stabilite di seguito. Ciò si applica anche all'accesso di visitatori. Gli ospiti e i visitatori degli edifici SISW devono registrare i loro nomi alla reception e devono essere accompagnati da personale SISW autorizzato. SISW e tutti i fornitori del centro dati di terza parte registrano i nomi e gli orari delle persone che accedono alle aree private di SISW all'interno dei centri dati.
   f. I dipendenti SISW e il personale esterno devono indossare i loro cartellini ID in tutti i locali SISW.

2. Controllo dell'accesso ai sistemi. I sistemi di elaborazione dati utilizzati per fornire il Servizio cloud devono essere protetti dall'utilizzo non autorizzato.

   Misure:
   a. SISW o i relativi subincaricati gestiscono l'ambiente per soddisfare i requisiti NIST SP 800-53 Rev 4 Access Control (AC) e Identification and Authentication (IA).
   b. Per concedere l'accesso ai sistemi sensibili, inclusi quelli di memorizzazione e trattamento dei dati personali, sono utilizzati diversi livelli di autorizzazione. Vengono attuati processi per assicurare che solo gli utenti autorizzati dispongano dell'autorizzazione appropriata per aggiungere, eliminare o modificare utenti.
   c. Tutti gli utenti accedono ai sistemi SISW con un nome utente una password univoci che devono soddisfare dei criteri di complessità minima.
   d. SISW e i relativi subincaricati attuano procedure per assicurare che le modifiche delle autorizzazioni richieste vengano implementate esclusivamente in modo conforme alle linee guida (ad esempio, nessun diritto viene concesso senza autorizzazione). Se un utente SISW cambia di ruolo o lascia la società, viene attuato un processo di revoca dei diritti di accesso all'ambiente.
   e. SISW e i relativi subincaricati hanno stabilito criteri per le password che proibiscono la condivisione di password, indicano come comportarsi in caso di divulgazione di una password, richiedono modifiche periodiche di tutte le password degli utenti e richiedono la modifica delle password predefinite. Per l'autenticazione vengono assegnati ID utente personalizzati. Tutte le password devono soddisfare i requisiti di complessità minima e sono memorizzate in forma crittografata. Per le password di dominio, il sistema impone un cambiamento delle password ogni 60 giorni, conformemente ai requisiti di complessità minima. Ogni computer SISW dispone di un salva schermo protetto tramite password.

f. SISW o i relativi subincaricati controllano automaticamente i seguenti eventi sugli account: creazione, modifica, abilitazione, disabilitazione e rimozione. Un amministratore di sistema rivede periodicamente i log.
g. Le reti di SISW e dei relativi subincaricati sono protette dalla rete Internet pubblica mediante firewall.
h. SISW e i relativi subincaricati utilizzano un software antivirus aggiornato sui punti di accesso della rete aziendale, per gli account email, in tutti i file server e in tutte le workstation.
i. SISW e i relativi subincaricati implementano sistemi di gestione patch di sicurezza per assicurare gli aggiornamenti di sicurezza relativi.
j. L'accesso remoto completo alla rete aziendale di SISW e all'infrastruttura critica è protetto da un'affidabile autenticazione multi-fattore.

3. Controllo dell'accesso ai dati. Il personale autorizzato a utilizzare i sistemi di elaborazione dati otterrà accesso esclusivamente ai dati personali per cui ha diritto di accesso, e i dati personali non potranno essere letti, copiati, modificati o rimossi senza autorizzazione in corso di trattamento, utilizzo o memorizzazione.

   Misure:
   a. L'accesso a informazioni personali, riservate o sensibili è concesso sulla base di ciò che è necessario sapere. In altre parole, i dipendenti o le terze parti esterne hanno accesso alle informazioni di cui hanno bisogno per completare il loro lavoro. SISW utilizza concetti di autorizzazione che documentano come le autorizzazioni vengono assegnate e quali autorizzazioni vengono assegnate. Tutte le informazioni personali, riservate o altrimenti sensibili sono protette conformemente agli standard e ai criteri di sicurezza di SISW.
   b. Tutti i server di produzione di qualsiasi Servizio cloud SISW sono gestiti nei centri dati relativi. Le misure di sicurezza che proteggono le applicazioni che elaborano informazioni personali, riservate o altre informazioni sensibili vengono controllate regolarmente. A questo fine, SISW include anche controlli esterni periodici per verificare che queste misure vengano applicate in modo appropriato.
   c. SISW non consente l'installazione di software personale o altro software non approvato da SISW nei sistemi utilizzati per qualsiasi Servizio cloud.
   d. In caso sia necessario trasferire dati a causa di un guasto del supporto di memorizzazione dati sottostante, al completamento di tale trasferimento, il supporto di memorizzazione guasto verrà smagnetizzato (in caso di supporto magnetico) o triturato (in caso di supporto solid-state o ottico).

4. Controllo della trasmissione dei dati. I dati personali non devono essere letti, copiati, modificati o rimossi senza autorizzazione durante il trasferimento.

   Misure:
   a. SISW o il relativo subincaricato gestirà l'infrastruttura e la configurazione in modo conforme ai requisiti NIST SP 800-53 Rev 4 Systems and Communication Protection (SC). Ciò include sistemi di prevenzione intrusioni in rete (NIPS) e firewall sui margini del sistema per la protezione da comunicazioni malintenzionate sul margine esterno dell'infrastruttura. NIPS e firewall sono configurati in base agli standard DISA STIG. I dati sono crittografati in transito utilizzando moduli crittografici conformi a FIPS 140-2.
   b. Quando i supporti dati vengono trasportati fisicamente, sono implementate misure adeguate presso SISW per garantire i livelli di servizio concordati (ad esempio, crittografia e contenitori piombati).
   c. La trasmissione dei dati personali sulle reti interne di SISW è protetta nello stesso modo di qualsiasi altro dato riservato conformemente ai criteri di sicurezza di SISW.
   d. Quando i dati vengono trasferiti tra SISW e il Cliente, le misure di protezione dei dati personali sono conformi a quanto stabilito nel Contratto o nella documentazione relativa per il Servizio cloud. Ciò si applica sia al trasferimento di dati fisico che in rete. I Cliente si assume la responsabilità del trasferimento di dati dal punto di demarcazione di SISW (ad esempio il firewall in uscita del centro dati che ospita il Servizio cloud).

5. Controllo dell'immissione dati. Il Servizio cloud permetterà di determinare in modo retrospettivo se e da chi sono stati inseriti, modificati o rimossi dati personali dall'infrastruttura utilizzata per fornire il Servizio cloud.

   Misure:
   a. SISW consente esclusivamente al personale autorizzato di accedere ai dati secondo quando richiesto per lo svolgimento del loro lavoro. SISW ha implementato un sistema di registrazione per l'inserimento, la modifica e l'eliminazione o il blocco di dati personali da parte di SISW o dei relativi subincaricati nella misura massima supportata dal Servizio cloud.
   b. Gli audit trail forniscono i dettagli sufficienti richiesti per la ricostruzione degli eventi in caso si verifichino o sospettino attività non autorizzate o malfunzionamenti. Ogni log eventi del sistema operativo include il tipo di

evento, un contrassegno orario, l'origine dell'evento, l'ubicazione dell'evento, il risultato dell'evento e l'utente associato all'evento.

6. Controllo dei processi. I Dati personali verranno trattati esclusivamente in modo conforme al Contratto e a eventuali istruzioni correlate fornite dal Cliente.

   Misure:
   a. SISW utilizza controlli e processi per assicurare la conformità ai contratti tra SISW e i relativi clienti, subincaricati o altri provider di servizi.
   b. I Dati del cliente saranno soggetti almeno allo stesso livello di protezione delle informazioni riservate, conformemente allo standard di classificazione delle informazioni di SISW.
   c. Tutti i dipendenti SISW e i partner contrattuali sono contrattualmente vincolati a rispettare la riservatezza di tutte le informazioni sensibili inclusi i segreti commerciali di clienti e partner SISW.

7. Controllo della disponibilità. I dati personali verranno protetti da distruzione o perdita accidentale o non autorizzata.

   Misure:
   a. SISW adotta processi di backup e altre misure che assicurano il ripristino rapido dei sistemi business-critical quando necessario.
   b. SISW fa affidamento su provider di servizi cloud globali per assicurare la disponibilità dei centri dati.
   c. SISW ha definito piani di emergenza nonché strategie di ripristino aziendale e di emergenza per i Servizi cloud.

8. Controllo della separazione dati. I dati personali sono raccolti per scopi diversi e possono essere trattati separatamente.

   Misure:
   a. Quando applicabile, SISW utilizza le funzionalità tecniche del software distribuito (ad esempio: ambienti multi-tenancy o sistemi separati) per ottenere la separazione dei dati tra i dati personali del Cliente e quelli di altri clienti.
   b. SISW mantiene istanze dedicate (con separazione logica o fisica) per ogni cliente.
   c. Il Cliente (incluse le relative affiliate) ha accesso solo alle proprie istanze.

9. Controllo dell'integrità dei dati. Assicura che i dati personali restino intatti, completi e aggiornati durante le attività di elaborazione:

   Misure: SISW ha implementato una strategia di difesa su molti livelli come protezione contro le modifiche non autorizzate. Ciò si riferisce ai controlli stabiliti nelle sezioni su controlli e misure sopra riportate. La Configurazione di firewall causerà la presenza di più segmenti di rete che separano l'accesso pubblico e privato. Ogni regola di firewall impostata avrà controlli di accesso specifici che definiranno le comunicazioni consentite tra questi segmenti.

   a. Centro di monitoraggio sicurezza: Verrà utilizzato software di rilevamento delle intrusioni automatico, insieme ad altri software e processi di prevenzione di sicurezza e forensi per avvisare, investigare e, se richiesto, notificare e assistere nella risoluzione di eventuali violazioni della sicurezza.
   b. Software antivirus: in tutti i sistemi saranno configurate le definizioni antivirus aggiornate per la protezione contro virus, worm, trojan e altre forme di malware.
   c. Backup e ripristino: tutti i sistemi avranno un livello di base di istantanee di backup di dati e configurazione. Se applicabile, SISW e i relativi subincaricati gestiranno anche un'istanza del cliente con configurazione di disponibilità elevata che assicurerà che i dati siano memorizzati in due centri dati separati a sufficiente distanza l'uno dall'altro.
   d. Controlli esterni periodici per comprovare le misure di sicurezza. SISW e i relativi subincaricati verranno sottoposti a controlli esterni periodici per testare le misure di sicurezza sopra elencate.