

Il presente Supplemento sul trattamento dei dati di Ivanti (“DPA”) è parte dell’Accordo per la licenza e i servizi dell’Utente finale di Ivanti (“l’Accordo”) ed è stipulato ed entra in vigore a partire dall’ultima data della firma apposta di seguito (la “Data di efficacia”) tra il cliente identificato di seguito o nell’Accordo (“Titolare”) e l’entità Ivanti pertinente (“Ivanti” o “Responsabile”) (singolarmente, una “Parte”; collettivamente, le “Parti”). Qualsiasi termine maiuscolo non definito nel presente Supplemento avrà il rispettivo significato stabilito nell’Accordo.

PREMESSE

CONSIDERANDO che le Parti hanno stipulato l’Accordo.

CONSIDERANDO che nel corso della fornitura dei Servizi al Titolare conformemente all’Accordo, il Responsabile potrebbe Trattare dei Dati personali per conto del Titolare;

CONSIDERANDO che, al fine di assicurare adeguate protezioni al Trattamento dei Dati personali forniti dal Titolare al Responsabile, le Parti concordano di conformarsi alle seguenti disposizioni rispetto a qualsiasi Dato personale, agendo ognuna in modo responsabile e in buona fede.

PERTANTO, considerate le premesse di cui sopra e le reciproche promesse e patti di seguito enunciati, il Titolare e il Responsabile del trattamento concordano quanto segue:

ACCORDO

1. DEFINIZIONI

Tutti i termini maiuscoli non definiti nel presente documento avranno il rispettivo significato stabilito nell’Accordo.

“**Consociata**” indica qualsiasi entità che, direttamente o indirettamente, controlla o è controllata da, o è sotto il controllo congiunto dell’entità soggetto. “**Controllo**”, ai sensi della presente definizione, indica la proprietà diretta o indiretta o il controllo di oltre il 50% dei diritti di voto dell’entità soggetto.

“**Leggi applicabili sulla Protezione dei dati**” indicano tutte le leggi applicabili, i regolamenti, gli orientamenti normativi o i requisiti che, in qualsiasi giurisdizione, fanno riferimento alla protezione dei dati, alla riservatezza o alla confidenzialità dei Dati personali, inclusi, a titolo indicativo ma non esclusivo (a) il GDPR, unitamente a qualsiasi normativa di recepimento, attuazione o integrazione e (b) il CCPA.

“**Consociata autorizzata**” indica qualsiasi Consociata del Titolare che (a) è soggetta alle leggi e ai regolamenti sulla protezione dei dati dello Spazio Economico Europeo e/o dei suoi Stati membri, del Regno Unito e della Svizzera, (b) è soggetta alle leggi e ai regolamenti sulla Protezione dei dati al di fuori dello Spazio Economico Europeo e/o dei suoi Stati membri, della Svizzera e del Regno Unito (a seconda del caso) e (c) ha acconsentito all’utilizzo del Responsabile per il Trattamento derivante dal presente Accordo.

“**CCPA**” indica la Legge della California sulla Riservatezza dei Consumatori, ai sensi del Codice civile Californiano art. 1798.100 e seguenti e i suoi regolamenti attuativi.

“**Titolare**” indica l’entità che determina le finalità e i mezzi del Trattamento dei Dati personali. A scanso di equivoci, la Parte sopra indicata come “Titolare” è un “Titolare” ai sensi del presente DPA.

“**Violazione dei dati**” indica una violazione della sicurezza che causa la distruzione, la perdita, la modifica, la divulgazione, l’accesso o altro Trattamento accidentale, non autorizzato o illegale dei Dati personali trasmessi, conservati o altrimenti trattati.

“**Autorità di protezione dei dati**” indica qualsiasi rappresentante o agente di un’entità governativa o di un’agenzia che ha l’autorità di fare rispettare le Leggi sulla protezione dei dati applicabili.

“**Interessato al trattamento dei dati**” indica una persona fisica alla quale si riferiscono i Dati personali.

“**GDPR**” indica il Regolamento (UE) 2016/679 del Parlamento e del Consiglio europeo del 27 aprile 2016 sulla protezione delle persone fisiche rispetto al trattamento dei dati personali e alla libertà di circolazione di tali dati e all’abrogata Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei dati).

“**Ivanti**” indica l’entità di seguito identificata che si trova nella medesima area geografica del Cliente:

- Ivanti, Inc., una società del Delaware, nel continente americano, ad eccezione del Brasile.
- Ivanti Comércio de Software Brasil Ltda, una società brasiliana, in Brasile.
- Ivanti Software K.K., una società giapponese, in Giappone.

- Ivanti Software Technology (Beijing) Co., Ltd., una società cinese, in Cina.
- Ivanti International Limited, una società irlandese per i prodotti e servizi con marchio Wavelink e Naurtech in Europa, Medio-Oriente, Africa e nella regione Asia-Pacifico.
- Ivanti UK Limited, una società a responsabilità limitata con sede in Inghilterra e nel Galles, per tutte le altre località.

“Dati personali” indicano qualsiasi informazione che identifica, si riferisce, descrive, può o potrebbe essere associata, direttamente o indirettamente, a una persona fisica identificata o identificabile o a un particolare nucleo familiare. Una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un nome, un numero identificativo, a dati sulla posizione a un identificativo online o a uno o più fattori specifici all’identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di quella persona fisica.

“Processo” indica qualsiasi operazione o insieme di operazioni che sono effettuate sui Dati personali da o in connessione con e per le finalità della fornitura dei Servizi, con o senza mezzi automatici, quali raccolta, registrazione, organizzazione, conservazione, adattamento o modifica, recupero, consultazione, utilizzo, divulgazione mediante trasmissione, diffusione o in altro modo messa a disposizione, allineamento o combinazione, blocco, cancellazione o distruzione; e come definito dalle Leggi applicabili in materia di Protezione dei dati.

“Responsabile” indica l’entità che effettua il Trattamento dei Dati personali per conto del Titolare. A scanso di equivoci, la Parte sopra indicata come “Responsabile” è un “Responsabile” ai sensi del presente DPA.

“Servizi” indica il Trattamento dei Dati personali da parte del Responsabile in relazione con e per le finalità della fornitura dei servizi che devono essere forniti dal Responsabile ai sensi del presente Accordo.

“Fornitore di servizi” indica un’impresa individuale, un partenariato, una società a responsabilità limitata, un’azienda, un’associazione o un’altra entità legale che sia organizzata o operata a fini di profitto o di benefici finanziari per i propri soci o altri proprietari, che tratta le informazioni per conto del Titolare dei dati e alla quale il Titolare dei dati divulga i Dati personali di un Interessato al trattamento dei dati per una Finalità commerciale a seguito di un contratto scritto, nella misura in cui il contratto proibisca al Fornitore di Servizi la conservazione, l’utilizzo o la divulgazione dei Dati personali per qualsiasi finalità diversa dallo scopo specifico di effettuare i servizi specificati nel contratto o secondo quanto altrimenti consentito dalla CCPA, inclusa la conservazione, l’utilizzo o la divulgazione di Dati personali per una Finalità commerciale diversa dalla fornitura dei servizi specificati nel contratto con il Titolare dei dati. I termini “Finalità aziendale” e “Finalità commerciale” hanno lo stesso significato dei termini usati nella CCPA. A scanso di equivoci, il Responsabile è un Fornitore di servizi.

“Sub-Responsabile” indica l’entità che effettua il Trattamento dei Dati personali per conto del Responsabile.

2. TRATTAMENTO DEI DATI PERSONALI

2.1 Ruoli delle Parti. Le Parti prendono atto e concordano che in merito al Trattamento dei Dati personali, il Titolare è il Titolare, il Responsabile è il Responsabile o Fornitore di Servizi. L’oggetto, la durata, la finalità del Trattamento e i tipi di Dati personali e le categorie di Dati personali trattati ai sensi del presente DPA sono ulteriormente specificati nell’Allegato 1.

2.2 Obblighi del Titolare Le istruzioni del Titolare in merito al Trattamento dei Dati personali devono essere conformi alle Leggi sulla Protezione dei dati e ai regolamenti. Il Titolare ha l’esclusiva responsabilità dell’accuratezza, della qualità e della legalità dei Dati personali e dei mezzi tramite i quali il Titolare acquisisce i Dati personali e li fornisce al Responsabile.

2.3 Obblighi del Responsabile Tutti i Dati personali trattati dal Responsabile in relazione all’Accordo sono Informazioni riservate e il Responsabile effettuerà il Trattamento dei Dati personali esclusivamente nel rispetto delle istruzioni documentate del Titolare definite nell’Allegato 1 o secondo quanto altrimenti fornito dal Titolare per iscritto. Il Responsabile non venderà i Dati personali trattati ai sensi del presente DPA e non conserverà, utilizzerà o divulgherà i Dati personali al di fuori della relazione d’affari diretta esistente tra il Responsabile e il Titolare. Con riferimento al Trattamento dei Dati personali, il Responsabile rispetterà tutte le Leggi applicabili sulla Protezione dei dati. Il Responsabile del trattamento non combinerà i Dati personali forniti dal Titolare del trattamento con i Dati personali che riceve da altre fonti. Qualora il Responsabile ritenga che l’ottemperanza a eventuali istruzioni del Titolare darebbe luogo a una violazione della Legge applicabile sulla Protezione dei dati, il Responsabile ne informerà immediatamente il Titolare per iscritto. Il Responsabile metterà a disposizione del Titolare tutte le informazioni necessarie per dimostrare la conformità del Responsabile ai suoi obblighi ai sensi del presente DPA.

2.3.1. Requisiti di assistenza. Il Responsabile assisterà il Titolare in merito a: conformità con le Leggi applicabili sulla Protezione dei dati; sospette e rilevanti Violazioni di dati; segnalazioni a o richieste da parte di un'Autorità sulla Protezione dei dati; notifiche a e domande dagli Interessati al trattamento dei dati; e agli obblighi del Titolare di effettuare valutazione d'impatto sulla protezione dei dati e prima di consultare un'Autorità di Protezione dei dati.

3. OBBLIGHI DI NOTIFICA

3.1 Obblighi di Notifica del Responsabile Il Responsabile deve notificare immediatamente il Titolare, per iscritto di quanto segue:

3.1.1 Una richiesta da parte dell'Interessato al trattamento dei dati di esercitare i suoi diritti sulla riservatezza quali l'accesso, la modifica, la cancellazione, il trasferimento, l'opposizione o la restrizione dei suoi Dati personali;

3.1.2 Qualsiasi richiesta o reclamo ricevuto dai clienti o dai dipendenti del Titolare;

3.1.3 Qualsiasi domanda, reclamo, indagine o altra richiesta da parte di un'Autorità sulla Protezione dei dati;

3.1.4 Qualsiasi richiesta di divulgazione di Dati personali che sia legata in qualsiasi modo al Trattamento dei Dati personali da parte del Responsabile ai sensi del presente DPA;

3.1.5 Una Violazione dei dati conformemente agli obblighi di notifica indicati all'Articolo 7.1; e

3.1.6 qualora i Dati Personali siano oggetto di perquisizione e sequestro, di sequestro conservativo, di confisca durante una procedura fallimentare o concorsuale, o di eventi o misure simili da parte di terzi durante il Trattamento.

Il Responsabile assisterà il Titolare nell'adempimento degli obblighi del Titolare di rispondere a richieste relative ai paragrafi (3.1.1) - (3.1.6) di cui sopra e non risponderà a tali richieste senza il preventivo consenso scritto del Titolare, a meno che il Responsabile non sia tenuto a rispondere per legge.

4. RISERVATEZZA

4.1 Informazioni riservate. Tutte le Informazioni fornite dal Responsabile ai sensi del presente Accordo sono Informazioni riservate.

4.2 Personale del Responsabile. Il Responsabile deve assicurare che tutto il personale coinvolto nel Trattamento di Dati personali sia informato della natura confidenziale dei Dati personali, abbia ricevuto una formazione adeguata in merito alle proprie responsabilità e abbia sottoscritto accordi scritti di riservatezza. Il Responsabile assicurerà che gli obblighi di riservatezza saranno validi anche dopo la risoluzione dei rispettivi rapporti di lavoro con tali persone.

4.3 Limiti all'accesso Il Responsabile si assicurerà che l'accesso ai Dati personali da parte del Responsabile sia limitato al personale che svolge i Servizi ai sensi del presente Accordo.

5. SUB-RESPONSABILI

5.1 Nomina di Sub-responsabili. Il Responsabile riconosce e accetta che il Responsabile e le Consociate del Responsabile possono incaricare sub-responsabili terzi in relazione alla fornitura dei Servizi. Il Responsabile o la Consociata del Responsabile sottoscriveranno un accordo scritto con ciascun Sub-Responsabile contenente obblighi di protezione di livello non inferiore a quello indicato nel presente DPA nella misura applicabile alla natura dei Servizi forniti da tale Sub-responsabile. Il Titolare con il presente autorizza il Responsabile a incaricare il suo attuale elenco di Sub-Responsabili come da elenco su <https://www.ivanti.com/company/legal/ivanti-subprocessors> per effettuare il Trattamento dei Dati personali ai sensi del presente DPA. Il Titolare non comunicherà direttamente con i Sub-Responsabili del Responsabile in merito ai Servizi, se non diversamente concordato con il Responsabile a esclusiva discrezione del Responsabile.

5.2. Notifica di cambiamenti ai Sub-responsabili. Il Responsabile informerà il Titolare di eventuali modifiche previste relative all'aggiunta o alla sostituzione di Sub-responsabili dotando il Titolare di un meccanismo per attivare le notifiche dei nuovi Sub-Responsabili all'indirizzo <https://www.ivanti.com/company/legal/ivanti-subprocessors>. Il Responsabile informerà il Titolare di eventuali modifiche previste relative all'aggiunta o alla sostituzione di Sub-Responsabili prima del suo utilizzo di Sub-responsabili.

5.3 Diritto di obiezione per nuovi Sub-responsabili Il Titolare può presentare obiezione ragionevole all'utilizzo di un nuovo Sub-responsabile da parte del Responsabile notificando senza indugio il Responsabile entro quindici (15) giorni lavorativi dopo la notifica del Responsabile. Qualora il Titolare obietti a un nuovo Sub-responsabile, il Responsabile farà gli sforzi ragionevoli per rendere disponibile al Titolare una modifica dei Servizi al fine di evitare il Trattamento dei Dati personali da parte del nuovo Sub-responsabile contestato. Qualora il Responsabile non sia in

grado di fare tale modifica, il Titolare può risolvere l'Accordo applicabile per quei servizi che non possono essere forniti dal Responsabile senza l'utilizzo del nuovo Sub-responsabile contestato.

5.4 Responsabile per gli atti dei Sub-responsabili. Il Responsabile sarà responsabile degli atti e delle omissioni dei suoi Sub-responsabili nella stessa misura in cui il Responsabile sarebbe stato responsabile dell'effettuazione dei servizi prestati da ciascun Sub-responsabile direttamente ai sensi del presente DPA.

6. SICUREZZA

6.1 Protezione dei Dati personali. Il Responsabile adoterà le appropriate misure tecniche ed organizzative per proteggere la sicurezza (compresa la protezione contro il Trattamento non autorizzato o illecito e contro la distruzione accidentale o illecita, la perdita o l'alterazione o il danneggiamento, la divulgazione o l'accesso non autorizzati ai Dati Personali), la riservatezza e l'integrità dei Dati Personali.

6.2 Diritti di controllo Il titolare accetta che il suo diritto di controllare il Responsabile può essere soddisfatto dal Responsabile presentando attestazioni aggiornate, rapporti o estratti di organismi indipendenti, inclusi, a mero titolo esemplificativo, revisori esterni o interni, incaricati della protezione dei dati del Responsabile, il dipartimento di sicurezza IT, revisori della protezione dei dati o della qualità o altri terzi reciprocamente concordati o certificazione mediante revisione della sicurezza informatica o della protezione dei dati. Nella misura in cui non sia possibile soddisfare un obbligo di revisione richiesto dai Regolamenti e dalla Legge di Protezione dei dati applicabili attraverso tali attestazioni, rapporti o estratti, il Titolare o l'incaricato del Titolare ha il diritto di revisionare e ispezionare, a spese del Titolare, i locali, le politiche, le procedure e i sistemi informatici del Responsabile al fine di accertare la conformità del Responsabile ai requisiti previsti dal presente DPA. Il Titolare, o l'incaricato del Titolare, invieranno una notifica almeno trenta (30) giorni prima della verifica, a meno che tale verifica sia richiesta a causa di una Violazione dei dati che coinvolge il Responsabile. Le revisioni effettuate dal Titolare o dall'incaricato del Titolare non violeranno gli obblighi di confidenzialità del Responsabile nei confronti degli altri clienti del Responsabile. Tutte le revisioni verranno effettuate durante le normali ore di lavoro, presso la sede principale del Responsabile o le altre sedi del Responsabile in cui avviene l'accesso, il trattamento o l'amministrazione dei Dati personali e non interferirà in modo irragionevole con le operazioni quotidiane del Responsabile. Prima dell'inizio di tale revisione, il Responsabile e il Titolare concorderanno l'ora, la finalità e la durata di tale revisione. Il Titolare può richiedere uno o più rapporti di revisione o effettuare una revisione del Responsabile non più di una volta all'anno.

7. VIOLAZIONI DEI DATI

7.1 Notifiche di Violazione dei dati Il Responsabile notificherà al Titolare per iscritto senza indebito ritardo di essere venuto a conoscenza di una sospetta Violazione dei dati. In ogni caso, tale notifica dovrà essere effettuata non oltre le 72 ore dalla scoperta della Violazione dei dati da parte del Responsabile.

7.2 Gestione della Violazione dei dati Il Responsabile farà gli sforzi ragionevoli per identificare la causa di tale Violazione dei dati e adoterà le misure che riterrà necessarie e ragionevoli per rimediare alla causa di tale Violazione di dati nella misura in cui il rimedio sia sotto il ragionevole controllo del Responsabile.

8. ESTINZIONE

8.1 Estinzione Il presente DPA si estingue automaticamente al più tardi (a) alla disdetta o alla scadenza dell'Accordo o (b) alla cancellazione o alla restituzione dei Dati personali da parte del Responsabile. Il Titolare è inoltre autorizzato a disdire il presente DPA per giusta causa qualora il Responsabile, a insindacabile giudizio del Titolare, abbia commesso una violazione sostanziale o persistente del presente DPA la quale, in caso di violazione passibile di rimedio, non sia stata rimediata dal Responsabile entro dieci (10) giorni dalla data di ricevuta di una notifica del Titolare che lo informava della violazione e gli richiedeva di porvi rimedio.

8.2 Restituzione o Eliminazione dei dati. Al termine del presente DPA, il Responsabile cancellerà o restituirà tutte le copie esistenti di Dati personali tranne nel caso in cui la legge applicabile richieda l'ulteriore conservazione dei Dati personali. Su richiesta del Titolare, il Responsabile confermerà per iscritto la conformità a tali obblighi ed eliminerà tutte le copie esistenti. Nei casi in cui la legge locale richieda al Responsabile la conservazione dei Dati personali, il Responsabile proteggerà la confidenzialità, l'integrità e l'accessibilità dei Dati personali; non tratterà attivamente i Dati personali; e continuerà ad attenersi ai termini del presente DPA.

9. MECCANISMI PER I TRASFERIMENTI INTERNAZIONALI

9.1 Trasferimenti al di fuori dell'UE. Nell'ambito della fornitura dei Servizi ai sensi del DPA, potrebbe essere necessario per il Titolare trasferire i Dati personali dall'Unione Europea, dallo Spazio Economico Europeo e/o dai

loro Stati membri, dalla Svizzera o dal Regno Unito, al Responsabile situato in un Paese che non dispone di una decisione di adeguatezza da parte dell'Unione Europea o che non si trova nello Spazio Economico Europeo.

9.1.1. Con riferimento ai Dati personali soggetti al GDPR, (i) il Responsabile è considerato l'“importatore di dati” e il Titolare l'“esportatore di dati”; (ii) i termini del Modulo Due si applicheranno laddove il Titolare è un Titolare dei dati e laddove il Responsabile è un Responsabile dei dati, (iii) nella Clausola 7, la clausola di “docking” facoltativa viene eliminata; (iv) nella Clausola 9 del Modulo Due, si applica l'opzione 2 e la lista dei Sub-Responsabili e del termine per la notifica delle modifiche deve essere concordata ai sensi dell'Articolo 5 del presente DPA; (v) nella Clausola 11, la lingua facoltativa viene eliminata; (vi) nella Clausola 17 si applica l'Opzione 1 e le Clausole Contrattuali Standard saranno regolate dallo Stato membro in cui è domiciliato il Titolare; (vii) nella Clausola 18(b) le controversie verranno risolte dinanzi ai tribunali dello Stato membro in cui è domiciliato il Titolare; (viii) l'Allegato I e l'Allegato II si intendono completi delle informazioni di cui rispettivamente all'Allegato 1 del presente DPA; e (ix) se e nella misura in cui le Clausole Contrattuali Standard fossero in contrasto con qualsiasi disposizione dell'Accordo (incluso il presente DPA) le Clausole Contrattuali Standard prevarranno per quanto necessario a eliminare tale conflitto. Per il presente articolo, le Clausole Contrattuali Standard dalla Decisione di Implementazione della Commissione (UE) 2021/914 sono incluse a titolo di riferimento e sono disponibili qui: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

9.1.2. Con riferimento ai Dati personali soggetti alle Leggi di Protezione dei dati del Regno Unito, si applica l'Accordo sul trasferimento internazionale dei dati (“IDTA”) con le seguenti modifiche: (i) i dati di contatto delle parti per l'Accordo sono i dati di contatto per l'IDTA; (ii) il Titolare è l'esportatore di dati e il Responsabile è l'importatore di dati; (iii) le leggi che disciplinano l'IDTA e i luoghi in cui possono essere avanzate le pretese legali sono l'Inghilterra e il Galles; (iv) il GDPR del Regno Unito non si applica al trattamento dei dati trasferiti da parte dell'importatore di dati; (v) le Parti non utilizzano ulteriori clausole di sicurezza o commerciali rispetto all'IDTA; e (vi) le informazioni nel presente DPA e nell'Allegato 1 possono essere utilizzate per le Tabelle 1-4. Per il presente articolo, le Clausole Contrattuali Standard dall'Information Commissioner Officer del Regno Unito (ICO) sono incluse a titolo di riferimento e sono disponibili qui: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/>.

9.1.3. In relazione ai Dati personali soggetti all'Autorità di protezione dei dati svizzera, le Clausole Contrattuali Standard a cui si fa riferimento all'articolo 9.1.1. si applicano con le seguenti modifiche (i) i riferimenti al “Regolamento (UE) 2016/679 devono essere interpretati come riferimenti alla LPD svizzera; (ii) i riferimenti a “UE”, “Unione” e “legge dello Stato membro” devono essere interpretati come riferimenti alla legge svizzera; e (iii) i riferimenti all'“Autorità di vigilanza competente” e ai “tribunali competenti” devono essere sostituiti con “l'Incaricato federale svizzero per la protezione dei dati e l'informazione”.

9.2. Meccanismo alternativo di trasferimento dei dati. Le Parti prendono atto che le leggi, le regole e i regolamenti relativi ai trasferimenti internazionali di dati stanno rapidamente evolvendo. Qualora il Titolare adotti un diverso meccanismo autorizzato da leggi, regole o regolamenti applicabili per il trasferimento dei Dati personali (ciascuno un “Meccanismo alternativo di trasferimento dei dati”), le Parti acconsentono a lavorare insieme in buona fede per implementare eventuali modifiche al presente Accordo necessarie per implementare il Meccanismo alternativo di trasferimento dei dati.

10. DISPOSIZIONI VARIE

10.1. Modifiche. Il presente DPA non può essere modificato o integrato, né alcuna delle sue disposizioni sarà considerata derogata o altrimenti modificata, ad eccezione che con un documento scritto debitamente sottoscritto dai rappresentanti autorizzati di entrambe le Parti.

10.2 Legge applicabile. Il presente DPA è disciplinato dalla legge applicabile indicata nell'Accordo.

ivanti SUPPLEMENTO SUL TRATTAMENTO DEI DATI DI IVANTI

A CONFERMA DI QUANTO SOPRA, le Parti hanno reso effettivo il presente Accordo dalla Data di efficacia.

TITOLARE: _____ IVANTI

Firma: _____

Firma: _____

Cognome: _____

Cognome: _____

Titolo: _____

Titolo: _____

Data: _____

Data: _____

Elenco degli Allegati:

Allegato 1: Descrizione del Trattamento

ALLEGATO 1:

Descrizione del Trattamento

Dati di contatto di Ivanti:

Ivanti

10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095

Contatto Responsabile della protezione dei dati: privacy@ivanti.com

Oggetto

Oggetto del Trattamento:

Fornitura di licenze informatiche software, servizi di supporto e di implementazione, sia in loco o come soluzioni SaaS ospitate, concernenti l'amministrazione e la facilitazione di processi aziendali essenziali nel settore/nei settori della gestione degli endpoint unificata, gestione dei servizi IT, sicurezza, rendicontazione e analisi e catena di fornitura.

I servizi informatici includono l'utilizzo di un software come installazione in loco o come soluzione SaaS compresa l'installazione di moduli (tra cui a titolo indicativo e non esaustivo, moduli di gestione degli incidenti, delle modifiche, degli asset, della configurazione e delle release); cataloghi self-service e di servizio; supporto e manutenzione incluso, a titolo indicativo e non esaustivo, l'accesso remoto; patch, controllo app, sicurezza endpoint/mobile e gestione dei privilegi.

Frequenza del trattamento:

Continua.

Durata

Durata del Trattamento:

Come indicato nell'Accordo.

Portata, tipo e finalità del Trattamento

La portata, il tipo e le finalità del Trattamento sono indicate di seguito:

Come indicato nell'Accordo.

Interessati al trattamento dei dati

Il trattamento dei dati personali può riferirsi alle seguenti categorie di Interessati al trattamento dei dati:

Clienti, clienti potenziali; dipendenti; fornitori, rappresentanti commerciali; contatti, appaltatori (inclusi i lavoratori a tempo determinato); volontari, lavoratori temporanei o casuali; liberi professionisti, agenti, consulenti e altri professionisti interpellati e loro rispettivi familiari, beneficiari e contatti di emergenza; dipendenti potenziali e personale temporaneo dei clienti; denunciati, corrispondenti e inquirenti; potenziali dipendenti e personale temporaneo dei clienti; ricorrenti, corrispondenti e inquirenti; consiglieri, consulenti e altri esperti professionisti; dipendenti o persone di contatto di potenziali esportatori di dati, clienti, partner commerciali e fornitori; partner commerciali e fornitori dell'esportatore di dati (che sono persone fisiche); e utenti dell'esportatore di dati autorizzati dall'esportatore di dati a utilizzare il software e i relativi servizi.

Categorie di dati

Il Trattamento dei dati personali può riferirsi alle seguenti categorie di dati:

i dati del Cliente caricati sui Servizi sotto i servizi e gli account del Cliente.

Misure tecniche e organizzative

Di seguito sono descritte le misure di sicurezza tecniche ed organizzative implementate dal Responsabile:

Formazione di sensibilizzazione alla sicurezza

Il Responsabile ha una formazione di sensibilizzazione alla sicurezza che include formazione obbligatoria sulla sicurezza sulla gestione e la protezione delle informazioni confidenziali e sensibili quali informazioni di identificazione personale, informazioni sui conti finanziari e informazioni sulla salute in conformità con la legge applicabile e comunicazioni periodiche di sensibilizzazione alla sicurezza e corsi di sicurezza che si concentrano sulla sensibilizzazione dell'utente finale.

Politiche e procedure di sicurezza

Il Responsabile ha politiche di sicurezza delle informazioni, di utilizzo e gestione che stabiliscono le azioni dei dipendenti e dei fornitori in merito all'utilizzo appropriato, all'accesso e alla conservazione delle informazioni confidenziali e sensibili; limitare l'accesso alle informazioni confidenziali e sensibili a membri della forza lavoro del Responsabile che hanno "necessità di conoscere" tali informazioni; prevenire l'accesso a ex-dipendenti alle informazioni del Responsabile dopo la fine del rapporto di lavoro; e imporre misure disciplinari in caso di mancato rispetto di tali politiche. Accesso al sistema alle risorse del Responsabile negato a meno che non sia stato specificamente valutato e concesso l'accesso. Il Responsabile effettua i controlli dei precedenti dei suoi dipendenti al momento dell'assunzione, come permesso dalla legge.

Controlli di accesso fisico e ambientali

Il Responsabile limita l'accesso fisico ai suoi sistemi e impianti informativi utilizzando controlli fisici (ad es. accessi con pass codificato) che forniscono una ragionevole garanzia che l'accesso ai suoi centri di dati sia limitato a persone fisiche autorizzate e utilizza telecamere o sistemi di videosorveglianza nei punti critici di ingresso interni ed esterni. Il Responsabile applica controlli di temperatura dell'aria e dell'umidità per i suoi centri di dati e protegge da perdite dovute a interruzioni di corrente.

Controlli di accesso logici

Il Responsabile utilizza tecnologia di login e di monitoraggio per aiutare a riconoscere e prevenire tentativi di accessi non autorizzati alle sue reti e ai suoi sistemi di produzione. Il monitoraggio del Responsabile include una revisione delle modifiche riguardanti autenticazione di gestione dei sistemi, autorizzazione e revisione; accesso privilegiato ai sistemi di produzione del Responsabile.

Controlli di crittografia

Il Responsabile applica controlli di crittografia appropriati all'attività sui nostri prodotti. Il Responsabile valuta e applica la crittografia in transito e a riposo utilizzando le migliori pratiche del settore per i codici. Le migliori pratiche sono utilizzate per la gestione del ciclo di vita delle chiavi di crittografia, inclusa la creazione, la conservazione, il controllo d'accesso e la rotazione.

Gestione della vulnerabilità

Il Responsabile effettua regolarmente scansioni di vulnerabilità e tratta le vulnerabilità scoperte in base al loro rischio. I prodotti del Responsabile sono altresì soggetti a valutazioni periodiche di vulnerabilità e a test di intrusione.

Ripristino di emergenza e controlli di back-up

Il Responsabile effettua back-up periodici dei file system e dei database di produzione secondo una pianificazione definita e mantiene un piano di ripristino di emergenza formale per il data center cloud di produzione, inclusi test regolari.

Piano di risposta agli incidenti informatici

Il Responsabile utilizza un piano di risposta agli incidenti informatici per gestire e minimizzare gli effetti di eventi informatici non pianificati che include procedure da seguire in caso di una violazione effettiva o potenziale della sicurezza incluso: un team interno di risposta agli incidenti con un dirigente del piano; un team di indagine che effettua un'analisi delle cause alla radice e che identifica le parti colpite; rapporti interni e processi di notifica; documentazione delle azioni di risposta e dei piani di correzione; e un rapporto post-incidente degli eventi.

Sicurezza della conservazione e di trasmissione

Il Responsabile adotta misure tecniche di sicurezza per proteggersi da accessi non autorizzati ai dati del Responsabile che vengono trasmessi tramite un rete di comunicazioni elettroniche pubblica o conservate elettronicamente.

Distruzione sicura

Il Responsabile adotta politiche e procedure in merito alla distruzione di beni materiali e immateriali che contengono dati del Responsabile così che i dati del Responsabile non possano essere letti o ricostruiti.

Identificazione e valutazione del rischio

Il Responsabile adotta un programma di valutazione del rischio che aiuta a identificare i prevedibili rischi interni ed esterni alle risorse informative del Responsabile e determinare se i controlli, le politiche e le procedure esistenti sono adeguate ad affrontare i rischi identificati.

Fornitori e fornitori di servizi

I fornitori o i fornitori di servizi terzi (collettivamente “Fornitori”) con accesso alle informazioni confidenziali del Responsabile sono soggetti a valutazioni del rischio per misurare la sensibilità delle informazioni del Responsabile che vengono condivise. I fornitori sono tenuti a rispettare i termini contrattuali pertinenti relativi alla sicurezza dei dati del Responsabile, nonché le politiche o le procedure del Responsabile applicabili. Periodicamente, il Responsabile può chiedere a un Fornitore di rivalutare il suo approccio alla sicurezza al fine di garantire la conformità.