ACCORDO SUL TRATTAMENTO DEI DATI

Il presente accordo sul trattamento dei dati (Data Processing Agreement**, "DPA"**) riflette l'accordo delle parti in relazione ai termini che disciplinano il trattamento dei Dati personali per conto del Cliente ai sensi di ogni accordo scritto applicabile tra il Cliente e Dynatrace che disciplini l'uso dei Servizi Offerti da Dynatrace nell' esecuzione del Contratto (Offerte Dynatrace),(a pagamento o d'altro tipo e di eventuali moduli d'ordine, allegati e dichiarazioni di lavoro correlati (collettivamente, il' **"Contratto"**). Il presente DPA entra in vigore alla data in cui è stato sottoscritto da entrambe le parti (la **"Data di decorrenza**").

Il presente DPA è soggetto ai termini del Contratto, e pienamente incorporato e facente parte dello stesso. Il presente DPA sostituirà qualsiasi accordo esistente sul trattamento dei dati, salvo diversamente specificato nel presente documento. In caso di conflitto tra il presente DPA e qualsiasi altra disposizione del Contratto in relazione ai dati personali, prevarrà e sarà applicabile il presente DPA. I termini in maiuscolo utilizzati ma non definiti nel presente DPA hanno lo stesso significato attribuito loro nel Contratto di abbonamento disponibile all'indirizzo https://assets.dynatrace.com/global/legal/Online-SA-April-2023-Italian.pdf

1. Definizioni.

(a) "**APPI**" indica la Legge giapponese sulla protezione delle informazioni personali (Legge n. 57 del 2003 e successive modifiche nel 2016).

(b) "**Legge sulla protezione dei dati**" indica tutte le leggi e le normative sulla protezione dei dati e sulla privacy applicabili al Trattamento dei Dati personali del Cliente da parte di Dynatrace ai sensi del Contratto.

(c) "**Titolare del trattamento**" ha lo stesso significato ad esso attribuito dalla Legge sulla protezione dei dati applicabile e include "Titolare del database", ai sensi della Legge sulla protezione della privacy di Israele, e "Business", ai sensi della Legge sulla privacy dello stato federato statunitense applicabile.

(d) "**Dati personali del Cliente**" indica tutti i Dati personali inviati, archiviati, pubblicati, visualizzati o altrimenti trasmessi da o per conto del Cliente nel corso dell'utilizzo delle Offerte Dynatrace; ed esclude i Dati personali (come le Informazioni soggette a restrizioni) inviati, archiviati, pubblicati, visualizzati o altrimenti trasmessi da o per conto del Cliente in violazione di qualsiasi disposizione del Contratto e/o del presente DPA.

(e) "**Gruppo Dynatrace**" indica una o più società tra Dynatrace LLC, una società a responsabilità limitata del Delaware, e le sue Collegate, che possono assistere Dynatrace nella fornitura delle Offerte Dynatrace, e/o del supporto o dei servizi correlati, ai sensi del Contratto e del presente DPA.

(f) "**Europa**" indica l'Unione europea, lo Spazio economico europeo ("SEE") e/o i loro Stati membri, la Svizzera e il Regno Unito.

(g) "**GDPR**" (acronimo di General Data Protection Regulation [) indica il Regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 Aprile 2016 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati.

(h) "**LGPD**" indica Lei Geral de Proteção de Dados Pessoais (Legge generale sulla protezione dei dati personali in Brasile).

(i) "**Violazione dei dati personali**" indica una violazione della sicurezza che comporta l'accidentale o illecita distruzione, perdita, alterazione o la divulgazione o l'accesso non autorizzati ai Dati personali del Cliente durante la trasmissione, l'archiviazione o altro tipo di Trattamento da parte di Dynatrace.

(j) "**PIPL**" indica la Legge cinese sulla protezione delle informazioni personali.

(k) Per "**Dati personali**" si intendono i "Dati personali" o le "Informazioni personali" come definite ai sensi delle Leggi applicabili in materia di protezione dei dati che Dynatrace raccoglie o riceve per conto del Cliente. I Dati personali non includono informazioni che Dynatrace ottiene o tratta a prescindere dall'adempimento dei propri rispettivi obblighi ai sensi del Contratto con il Cliente.

(l) "**Responsabile del trattamento**" ha lo stesso significato ad esso attribuito dalla Legge sulla protezione dei dati applicabile e include "Holder", ai sensi della Legge sulla protezione della privacy di Israele, e "Service Provider", ai sensi della Legge sulla privacy dello stato federato statunitense applicabile.

(m) "**Clausole contrattuali tipo**" indica le Clausole contrattuali tipo promulgate dalla Decisione della Commissione UE 2021/914/UE quivi incorporate per riferimento, ed eventuali aggiornamenti, emendamenti o sostituzioni periodici.

(n) "**Sub-responsabile del trattamento**" indica i Responsabili del trattamento incaricati da Dynatrace o da membri del Gruppo Dynatrace per consentire a Dynatrace di consegnare/fornire le Offerte Dynatrace ai sensi dei termini del Contratto o del presente DPA.

(o) "**Autorità di controllo**" indica l'agenzia, il dipartimento o altra organizzazione competente del governo con autorità sul trattamento dei Dati personali pertinenti al presente DPA.

(p) "**Addendum del Regno Unito**" indica l'Addendum al trasferimento transfrontaliero dei dati alle Clausole contrattuali tipo della Commissione UE emesse dall'ufficio del Commissario per le informazioni del Regno Unito ai sensi del S119A (1) della Legge sulla protezione dei dati del 2018, e successivi aggiornamenti, modifiche, o sostituzioni di volta in volta apportati.

(q) **"Attività", "Titolare del trattamento", "Consumatore", "Responsabile del trattamento", "Fornitore di servizi", "Interessato", "Vendere", "Autorità di controllo" e "Trattamento" (e "Trattare")** avranno il significato ad essi attribuito dalla Legge applicabile in materia di protezione dei dati.

2. Applicabilità del DPA e ruoli delle parti

(a) Il presente DPA si applica al Trattamento dei Dati personali del Cliente da parte di Dynatrace per conto del Cliente al fine di adempiere alle sue obbligazioni ed esercitare i suoi diritti ai sensi del Contratto e del presente DPA. Il presente DPA non si applica al Trattamento dei Dati personali del Cliente da parte di Dynatrace in qualità di Titolare del trattamento.

(b) Il Cliente è un Titolare del trattamento o un Responsabile del trattamento, mentre Dynatrace è un Responsabile del trattamento. Nella misura applicabile ai sensi della Legge sulla protezione dei dati, il Cliente nomina Dynatrace come Responsabile del trattamento ai sensi dell'art. 28 di GDPR, per trattare i Dati personali del Cliente per conto del Cliente.

3. Trattamento dei Dati personali del Cliente

(a) La natura e la finalità del Trattamento dei Dati personali del Cliente da parte di Dynatrace per fornire le Offerte Dynatrace sono determinate e controllate dal Cliente e specificate ulteriormente nell'Allegato A. La natura, la finalità e la durata del Trattamento, nonché i tipi di Dati personali raccolti e le categorie di Interessati i cui Dati personali possono essere trattati da Dynatrace, sono descritti nell'**Allegato A** al presente DPA. Il Cliente riconosce che Dynatrace non è a conoscenza dei dati o tipo di Dati personali contenuti nei Dati del Cliente. Le parti convengono che le istruzioni complete e definitive del Cliente sulla natura e le finalità del Trattamento in relazione alle Offerte Dynatrace sono stabilite nelContratto e nel presente DPA.

(b) Eventuali modifiche alle istruzioni dovranno essere comunicate per iscritto e approvate da entrambe le parti. Dynatrace informerà il Cliente se, a suo ragionevole giudizio, le istruzioni del Cliente in materia di trattamento potrebbero violare qualsiasi Legge applicabile in materia di protezione dei dati; in tal caso, Dynatrace ha il diritto di rifiutare il trattamento dei Dati personali del Cliente, il cui trattamento ritiene violino

qualsiasi Legge applicabile in materia di protezione dei dati fino a quando il Cliente non modifichi tali istruzioni in modo da ripristinare la conformità alla legge.

(c) Nella misura in cui per effetto della configurazione delle Offerte Dynatrace da parte del Cliente, si verifichi l'acquisizione dei Dati personali del Cliente da parte di Dynatrace, il Cliente dichiara e garantisce che, in ogni momento, rispetterà tutte le Leggi applicabili in materia di protezione dei dati. Per quanto riguarda il Cliente e Dynatrace, il Cliente è responsabile di: (i) proteggere i Dati personali del Cliente mentre utilizza Dynatrace configurandone le Impostazioni di privacy come descritto all'indirizzo https://docs.dynatrace.com/docs/manage/data-privacy-and-security (istruzioni di Dynatrace per la configurazione delle impostazioni sulla privacy), in modo tale che via sia un controllo capillare dei Dati e del tipo di Dati personali che devono essere trattati da Dynatrace per effetto della fornitura delle Offerte Dynatrace; (ii) l'accuratezza, la qualità e la legittimità dei Dati personali del Cliente, e i mezzi con cui il Cliente o qualsiasi parte terza ha acquisito i Dati personali.

(d) Se il Cliente è un Responsabile del Trattamento che agisce per conto di una terza parte Titolare del trattamento, il Cliente garantisce a Dynatrace che le istruzioni date e le azioni intraprese in relazione ai Dati personali del Cliente, compresa la nomina di Dynatrace come altro Responsabile del trattamento, sono state autorizzate dal Titolare del trattamento pertinente.

(e) Il Cliente dichiara e garantisce che: (i) informerà gli Interessati come richiesto dalla legge in merito al proprio utilizzo di Responsabili del trattamento per Trattare i Dati personali del Cliente, tra cui Dynatrace, anche, ove necessario, inviando agli Interessati una comunicazione in merito all'uso delle Offerte Dynatrace; (ii) ha ottenuto, e mantiene, durante il periodo di validità, tutti i diritti, le basi giuridiche, le autorizzazioni e/o il consenso valido dei soggetti Interessati necessari per il trattamento dei Dati personali del Cliente da parte di Dynatrace come previsto dal Contratto; (iii) l'uso da parte del Cliente delle Offerte Dynatrace non violerà, né causerà violazione da parte di Dynatrace de, le Leggi applicabili in materia di protezione dei dati o altre leggi o regolamenti applicabili né una violazione di qualsiasi accordo o obbligo tra il Cliente e un terzo.

(f) Il Cliente fornirà a Dynatrace solo i Dati personali del Cliente necessari affinché Dynatrace adempia ai propri obblighi ai sensi del Contratto in relazione alle Offerte Dynatrace e a qualsiasi servizio correlato. Il Cliente riconosce che l'uso delle Offerte Dynatrace non richiede e non è adatto al Trattamento di alcuna Informazione soggetta a restrizioni e non fornirà, attraverso il suo utilizzo delle Offerte Dynatrace, alcuna Informazione soggetta a restrizioni ai fini del trattamento da parte di Dynatrace.

4. Richieste da parte di terzi.

(a) Le Offerte Dynatrace forniscono al Cliente la funzionalità di accedere ai Dati personali del Cliente al fine di assistere i Clienti nelle richieste ricevute dal cliente da parte dei Soggetti Interessati nell'esercizio dei loro diritti ai sensi della Legge sulla protezione dei dati ("Richieste dei Soggetti Interessati") o nelle richieste da parte di organismi normativi o giudiziari relativi al Trattamento dei Dati personali del Cliente. Nella misura in cui il Cliente non sia in grado di accedere ai Dati personali del Cliente pertinenti all'interno delle Offerte Dynatrace o l'accesso ai Dati personali del Cliente non fornisca sufficiente assistenza per rispondere a tali richieste, e, ove richiesto dalla Legge sulla protezione dei dati applicabile, Dynatrace accetta, su richiesta del Cliente, di fornire al Cliente ragionevole assistenza per consentirgli di rispondere alle Richieste dei Soggetti Interessati o alle richieste provenienti da organismi normativi o giudiziari relativi al Trattamento dei Dati personali del Cliente ai sensi dell'Accordo. Se viene presentata una richiesta direttamente a Dynatrace relativa ai Dati personali del Cliente per i quali Dynatrace può identificare il Cliente come Titolare del trattamento, Dynatrace dovrà senza indebito ritardo indirizzare tale comunicazione al Cliente e non dovrà rispondere a tale richiesta senza l'espressa autorizzazione del Cliente. Quanto sopra non proibirà a Dynatrace di comunicare con un Soggetto Interessato o un organismo normativo o giudiziario se non è ragionevolmente desumibile dalla comunicazione che la richiesta si riferisce al Cliente o nel caso in cui Dynatrace ha l'obbligo legale di rispondere.

(b) Se Dynatrace è obbligata ai sensi di legge a divulgare i Dati personali per i quali il Cliente è il Titolare del

Trattamento in forza di una richiesta da parte di un'agenzia governativa o altro terzo, Dynatrace darà al Cliente notifica di tale richiesta prima di concedere l'accesso e/o fornire i Dati personali, per consentire al Cliente di richiedere un ordine restrittivo o altro rimedio appropriato. Se a Dynatrace è fatto divieto per legge di notificare il Cliente, Dynatrace adotterà misure volte a proteggere i Dati personali dalla divulgazione indebita, come se fossero state richieste le proprie Informazioni confidenziali.

5. **Assistenza e collaborazione.** Fatta salva la natura del trattamento e dei Dati personali a disposizione di Dynatrace e ove richiesto dalla Legge applicabile in materia di protezione dei dati, Dynatrace, su richiesta scritta del Cliente, fornirà ragionevole assistenza e informazioni al Cliente, laddove, a giudizio del Cliente, il tipo di Trattamento eseguito da Dynatrace richieda una valutazione d'impatto sulla protezione dei dati, e/o previa consultazione con le autorità competenti per la protezione dei dati e fornirà ragionevole assistenza al Cliente nel rispetto degli altri suoi obblighi previsti dalla Legge applicabile in materia di protezione dei dati in relazione alla sicurezza dei dati e alle notifiche di Violazione dei dati personali, nella misura applicabile al Trattamento dei Dati personali del Cliente. Il Cliente rimborserà a Dynatrace tutti i costi non trascurabili sostenuti da quest'ultima nell'adempiere ai propri obblighi ai sensi della presente sezione.

6. **Conformità** . Dynatrace accetta di fornire al cliente le informazioni necessarie per dimostrare la propria conformità al presente accordo, su ragionevole richiesta del Cliente.

7. **Revisioni e valutazioni.**

(a) Laddove le Leggi sulla protezione dei dati applicabili conferiscano al Cliente un diritto di revisione o di valutazione e fatto salvo la finalità di tale diritto, il Cliente può eseguire, su richiesta scritta del Cliente e al massimo una volta all'anno, una revisione o valutazione delle politiche, delle procedure e dei registri di Dynatrace pertinenti al Trattamento dei Dati personali del Cliente, in conformità alle Leggi sulla protezione dei dati applicabili.

(b) Per richiedere una revisione, il Cliente deve presentare a Dynatrace un piano di revisione dettagliato almeno quattro (4) settimane prima della data della revisione proposta, il quale piano descriverà l'ambito, la durata e la data di inizio proposti per la revisione. Dynatrace esaminerà il piano di revisione e comunicherà al Cliente eventuali dubbi o domande. Prima dell'inizio di qualsiasi revisione, le parti concorderanno un piano di revisione dettagliato, comprensivo di onorari, tempistiche, ambito dei controlli, prove da produrre e durata. Se l'ambito della revisione richiesto viene spiegato in una relazione di revisione simile risalente ai dodici mesi precedenti e Dynatrace conferma che non vi sono modifiche sostanziali nei controlli oggetto della revisione, il Cliente accetterà tali conclusioni invece di richiedere una revisione dei controlli trattati nella relazione.

(c) Qualsiasi revisione o valutazione deve essere: (i) condotta durante il normale orario lavorativo di Dynatrace; (ii) soggetta agli obblighi di riservatezza delle parti. Se è un terzo a dover condurre la revisione, esso non deve essere un concorrente di Dynatrace, sarà soggetto al previo consenso di Dynatrace e dovrà stipulare un accordo di riservatezza scritto con le parti prima di condurre la revisione.

(d) Tutte le revisioni sono a carico del Cliente. Qualsiasi richiesta a Dynatrace di fornire assistenza in una revisione è considerata un servizio separato se tale assistenza nella revisione richiede l'uso di risorse diverse da, o in aggiunta a, quelle richieste per la fornitura delle Offerte Dynatrace. Dynatrace richiederà la conferma scritta del Cliente indicante che questi si farà carico di eventuali tariffe applicabili prima di offrire tale assistenza nella revisione.

8. **Confidenzialità.** Dynatrace garantirà che qualsiasi persona autorizzata a trattare i Dati personali del Cliente (tra cui il relativo personale, agenti e subappaltatori) sia soggetta a un obbligo di riservatezza contrattuale, legale o comunque vincolante.

9. **Security**

(a) **Misure di sicurezza.** Tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché del rischio di mutevole probabilità e gravità per i diritti e

le libertà delle persone fisiche, Dynatrace ha adottato e manterrà adeguate misure tecniche e organizzative, concepite per fornire un livello di sicurezza adeguato al rischio associato al trattamento dei Dati personali del Cliente (**"Misure di sicurezza"**). Il Cliente conferma che l'attuazione da parte di Dynatrace delle Misure di sicurezza indicate nell'**Allegato B** è sufficiente ai fini del rispetto dei suoi obblighi ai sensi del presente Accordo. Fermo restando quanto sopra, il Cliente riconosce e accetta di essere responsabile dell'uso corretto e sicuro delle Offerte Dynatrace.

(b) **Violazione dei dati personali.** Dynatrace informerà il Cliente senza indebito ritardo e non oltre il termine imposto a Dynatrace dalla Legge applicabile in materia di protezione dei dati, dopo essere venuta a conoscenza di una Violazione dei dati personali. Dynatrace avvierà una tempestiva indagine sulle circostanze relative alla Violazione dei dati personali e renderà disponibili al Cliente le proprie conclusioni in merito alla violazione. . Dynatrace si impegnerà ad adottare tutte le misure richieste dalla Legge applicabile in materia di protezione dei dati per mitigare gli effetti di tale Violazione. Su richiesta del Cliente e tenendo conto della natura del Trattamento e delle informazioni a disposizione di Dynatrace, Dynatrace adotterà misure commercialmente ragionevoli per aiutare il Cliente a rispettare i propri obblighi, necessarie affinché quest'ultimo, se tenuto a farlo ai sensi della Legge applicabile in materia di protezione dei dati, notifichi le Violazioni dei Dati personali pertinenti alle autorità competenti e/o agli Interessati coinvolti. La notifica di una Violazione dei dati personali sarà recapitata a uno o più amministratori del Cliente tramite i mezzi scelti da Dynatrace, anche via e-mail. È esclusiva responsabilità del Cliente garantire che i propri amministratori rendano i propri recapiti disponibili e riportati correttamente sul portale online o come altrimenti richiesto da Dynatrace in una notifica scritta all'/agli amministratore/i del Cliente. L'obbligo di Dynatrace di segnalare o rispondere a una Violazione dei dati personali ai sensi della presente Sezione non è un riconoscimento da parte di Dynatrace di un qualche tipo di colpa o responsabilità in relazione alla Violazione dei dati personali.

10. Sub-trattamento

(a) Il Cliente concede la propria autorizzazione generale a nominare membri del Gruppo Dynatrace come sub-responsabili del trattamento ai sensi del presente DPA e autorizza Dynatrace e i membri del Gruppo Dynatrace a incaricare ulteriori Sub-responsabili del trattamento. Un elenco aggiornato degli attuali Sub-responsabili del trattamento per le Offerte Dynatrace è disponibile all'indirizzo https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/. Per informarsi su nuovi Sub-responsabili del trattamento o eventuali modifiche agli stessi, il Cliente deve registrarsi per ricevere notifiche all'indirizzo https://www.dynatrace.com/company/trust-center/customers/subprocessors-dynatrace-services/ ("**Notifiche sulla protezione dei dati**"). Dynatrace aggiornerà l'Elenco dei Sub-responsabili del trattamento per riflettere qualsiasi aggiunta o modifica a Sub-responsabili del trattamento terzi non meno di trenta (30) giorni prima della data di entrata in vigore della modifica. I Clienti che si sono iscritti per ricevere aggiornamenti all'Elenco dei sub-responsabili del trattamento riceveranno una notifica della modifica.

(b) Nella misura richiesta dalla Legge applicabile in materia di protezione dei dati, il Cliente può opporsi al trattamento dei Dati personali del Cliente da parte di qualsiasi Sub-responsabile del trattamento appena nominato per ragionevoli motivi relativi alla protezione dei Dati personali del Cliente e informerà Dynatrace per iscritto entro quindici (15) giorni dalla notifica delle modifiche pubblicate nell'Elenco dei Sub-responsabili del trattamento, indicando i motivi specifici della sua obiezione. Il Cliente deve fornire la propria obiezione per iscritto e indicare per la stessa una giustificazione commercialmente ragionevole, sulla base di ragionevoli dubbi riguardanti le pratiche di protezione dei dati del Sub-responsabile del trattamento proposto. A seguito di un'obiezione, le parti collaboreranno in buona fede per rispondere alle ragionevoli obiezioni del Cliente e procedere con la modifica del Sub-responsabile del trattamento. Se non si raggiunge un accordo entro quindici (15) giorni dall'obiezione, a discrezione di Dynatrace: (a) Dynatrace istruirà il Sub-responsabile del trattamento a non trattare i Dati personali del Cliente, il che potrebbe comportare la sospensione e la non disponibilità di una funzionalità delle Offerte Dynatrace al Cliente, o (b) il Cliente potrà risolvere immediatamente il presente Accordo e il contratto e Dynatrace rimborserà tempestivamente la parte proporzionale di eventuali pagamenti già effettuati per il periodo successivo a tale data di sospensione

o risoluzione. Se Dynatrace non riceve alcuna obiezione entro il periodo di tempo sopra specificato, si riterrà che il Cliente abbia approvato l'incarico di un nuovo sub-responsabile del trattamento.

(c) Dynatrace dovrà: (i) stipulare un accordo scritto con ciascun Sub-responsabile del trattamento contenente obblighi di protezione dei dati che stabiliscano obblighi contrattuali adeguati sostanzialmente simili, ma non meno restrittivi di quelli stabiliti nel presente DPA, nella misura adeguata alla natura del servizio fornito da tale Sub-responsabile del trattamento; e (ii) rimanere responsabile della conformità di tale Sub-responsabile del trattamento agli obblighi del presente DPA e di qualsiasi atto od omissione di tale Sub-responsabile del trattamento che induca Dynatrace a violare uno qualsiasi dei propri obblighi ai sensi del presente DPA.

11. Eliminazione dei Dati del Cliente alla Risoluzione. Dopo la risoluzione o la scadenza del Contratto i Dati personali del Cliente saranno eliminati entro trenta (30) giorni, o, a scelta del Cliente, restituiti, salvo ove richiesto dalla legge applicabile o nella misura in cui siano archiviati su sistemi di backup, nel qual caso i termini del presente Accordo rimarranno in validità.

12. Trasferimenti transfrontalieri di dati

(a) Il Cliente autorizza Dynatrace e i suoi Sub-responsabili del trattamento a trasferire i Dati personali del Cliente oltre i confini internazionali, anche, a titolo esemplificativo ma non esaustivo, dal SEE, dal Regno Unito e/o dalla Svizzera, da Israele e dalla Cina agli Stati Uniti. Se i Dati personali del Cliente provenienti dall'SEE o dalla Svizzera vengono trasferiti in un Paese che ai sensi della Legge applicabile in materia di protezione dei dati non è stato ritenuto in grado di fornire un livello adeguato di protezione ("**Trasferimento soggetto a restrizioni**"), le parti convengono che il trasferimento sarà disciplinato dalle Clausole contrattuali tipo, che sono incorporate al presente Accordo per riferimento come segue. Le firme sul presente DPA o sull'Accordo costituiscono la firma delle Clausole contrattuali tipo e degli eventuali allegati ad esso acclusi. Quando il trasferimento dei Dati personali del Cliente dal Cliente ("**Esportatore dei dati**") a Dynatrace ("**Importatore dei dati**") è un trasferimento soggetto a restrizioni e una Legge sulla protezione dei dati richiede l'attuazione di un valido meccanismo di trasferimento, i trasferimenti saranno soggetti alle Clausole contrattuali tipo.

(b) Le Clausole contrattuali tipo saranno compilate come segue:

i. Si applicherà il Modulo Due (se applicabile);

ii. Nella Clausola 7 (Clausola di adesione postuma), si applicherà la clausola di adesione postuma opzionale;

iii. Nella Clausola 8.5 e nella Clausola 16 (d), su richiesta scritta dell'esportatore dei dati sarà fornita la certificazione di avvenuta cancellazione;

iv. Nella Clausola 8.9, il diritto di revisione sarà esercitato in conformità alla Sezione 7 del DPA;

v. Nella Clausola 9 (Incarico di Sub-responsabili del trattamento), si applicherà l'opzione 2 "Autorizzazione scritta generale" per i sub-responsabili del trattamento e il termine per il preavviso sarà quello stabilito nella Sezione 11 del presente DPA;

vi. Nella Clausola 11 (Rimedio), il testo facoltativo non si applica;

vii. Nella Clausola 13 (Supervisione), l'autorità di controllo competente è la Commission nationale de l'informatique et des libertes (CNIL).

viii. Nella Clausola 14 (f) e nella Clausola 16 (c), il diritto di risoluzione si limiterà alla risoluzione delle Clausole;

ix. Nella Clausola 17 (Legge applicabile), le Clausole contrattuali tipo saranno disciplinate dalla legge francese;

x. Nella Clausola 18(b) (Foro competente e Giurisdizione), le parti convengono che le controversie saranno risolte dinanzi ai tribunali francesi;

xi. L'Allegato 1 alle Clausole contrattuali tipo deve essere compilato con le informazioni indicate nell'Allegato A del presente DPA;

xii. L'Allegato 2 alle Clausole contrattuali tipo deve essere compilato con le informazioni indicate nell'Allegato B del presente DPA; e

xiii. Alle Clausole contrattuali tipo viene aggiunta una nuova Clausola 1 (e) che recita come segue: "Nella misura applicabile ai sensi del presente documento, le presenti Clausole si applicano anche fatte le debite modifiche al Trattamento dei Dati personali del Cliente ad opera delle parti, nel rispetto della Legge federale svizzera sulla protezione dei dati. Ove applicabile, il riferimento al diritto degli Stati membri dell'UE o alle autorità di controllo dell'UE deve essere modificato per includere l'opportuno riferimento ai sensi del diritto svizzero per quanto concerne il trasferimento dei Dati personali del Cliente che sono soggetti alla Legge federale svizzera sulla protezione dei dati e all'Incaricato federale svizzero della protezione dei dati e della trasparenza in qualità di autorità di controllo ai sensi delle presenti Clausole".

(c) Nella misura in cui la fornitura da parte di Dynatrace delle Offerte Dynatrace comporti il trasferimento di Dati personali del Cliente provenienti dal Regno Unito verso un Paese terzo che ai sensi delle Leggi applicabili nel Regno Unito non fornisce un livello adeguato di protezione ai Dati personali del Cliente, le Clausole contrattuali tipo: (i) saranno utilizzate e compilate come stabilito nella Sezione 13; (ii) ad esse viene aggiunta una nuova Clausola 1(f) che recita come segue: "Nella misura applicabile ai sensi del presente documento, le presenti Clausole, integrate dalla Sezione 13, si applicano anche fatte le debite modifiche al Trattamento ad opera delle parti dei Dati personali del Cliente, che sono soggetti alle Leggi sulla protezione dei dati del Regno Unito; e (iii) l'Addendum del Regno Unito sarà compilato come segue:

i. La Tabella 1 dell'Addendum del Regno Unito deve essere compilata con le informazioni contenute nell'Allegato A.

ii. La Tabella 2 dell'Addendum del Regno Unito deve essere compilata con le informazioni riportate nella Sezione 13 (c) del presente DPA.

iii. La Tabella 3 dell'Addendum per il Regno Unito deve essere compilata come segue:

1) L'elenco delle parti è riportato nell'Allegato A;

2) Una descrizione del trasferimento è riportata nell'Allegato A;

3) Una descrizione delle misure tecniche e organizzative è riportata nell'Allegato B;

4) L'elenco dei sub-responsabili del trattamento si trova nella Sezione 11 del presente DPA;

5) Ai fini della compilazione della Tabella 4 dell'Addendum del Regno Unito, sia l'importatore che l'esportatore possono terminare l'Addendum del Regno Unito come stabilito nella relativa Sezione 19.

(d) Nella misura in cui la fornitura da parte di Dynatrace delle Offerte Dynatrace comporti il trasferimento dei Dati personali del Cliente provenienti dalla Cina verso un Paese terzo che ai sensi delle Leggi applicabili in Cina non fornisce un livello adeguato di protezione dei Dati personali del Cliente, il Cliente sarà responsabile dell'adempimento di tutti i seguenti obblighi di esportazione dei Dati personali del Cliente (laddove il Cliente sia il Titolare del trattamento) o di garantire che tutti i seguenti obblighi siano stati adempiuti dal titolare del trattamento terzo pertinente (laddove il Cliente sia il Responsabile del trattamento):

i. informare gli individui del nome e dei recapiti della parte ricevente estera dei Dati personali del Cliente, della finalità e dei mezzi del Trattamento, delle categorie di Dati personali del Cliente e dei metodi e delle procedure attraverso i quali gli individui possono avanzare richieste di esercizio dei diritti sui Dati personali del Cliente alla parte ricevente estera dei Dati personali del Cliente;

ii. garantire una base giuridica per l'esportazione dei Dati personali del Cliente, e laddove il consenso degli individui sia la base giuridica, ottenere il consenso separato degli individui;

iii. condurre una valutazione d'impatto sulla protezione delle informazioni personali sull'esportazione dei Dati personali del Cliente; e

iv. adottare le opportune misure di salvaguardia richieste dal PIPL e dalle relative normative amministrative (ovvero, superare la valutazione della sicurezza governativa, presentare le Clausole

contrattuali tipo sottoscritte o ottenere la certificazione), a meno che non si applichi una deroga.

(e) In aggiunta a quanto sopra, se un'Autorità di controllo adotta, aggiorna o sostituisce delle clausole contrattuali tipo o meccanismi di trasferimento dei dati analoghi, Dynatrace si riserva il diritto di adottare uno standard di conformità alternativo per sostituire o integrare le Clausole contrattuali tipo o l'Addendum del Regno Unito per il legittimo trasferimento dei Dati personali, o aggiungere nuovi meccanismi di trasferimento dei dati per altri Paesi, a condizione che siano riconosciuti ai sensi della Legge sulla protezione dei dati. Dynatrace fornirà un preavviso di trenta (30) giorni sull'attuazione dello standard di conformità alternativo ai clienti che si iscrivono per ricevere Notifiche sulla protezione dei dati. La variazione si applicherà automaticamente come stabilito nella notifica di Dynatrace alla fine del periodo di preavviso.

(f) In caso di conflitto o incongruenza tra i seguenti documenti, l'ordine di precedenza sarà: (1) le Clausole contrattuali tipo (a condizione, tuttavia, che il Responsabile del trattamento possa nominare Sub-responsabili del trattamento come stabilito dalla Sezione 11 del presente Accordo, e fatti i salvi i requisiti della sezione stessa) o un meccanismo simile richiesto dalle Leggi applicabili in materia di protezione dei dati specificamente per i trasferimenti transfrontalieri di dati; (2) il presente Accordo; e (3) il Contratto.

(g) Nella misura in cui Dynatrace trasferisce i Dati del Cliente provenienti e protetti dalla Legge sulla protezione dei dati applicabile in Brasile, Dynatrace dovrà rispettare i principi e i diritti degli Interessati e gli obblighi di protezione dei dati previsti nella LGPD.

(h) Nella misura in cui Dynatrace trasferisce i Dati del Cliente provenienti e protetti dalla Legge sulla protezione dei dati applicabile in Giappone, Dynatrace rispetterà i principi e i diritti degli Interessati e gli obblighi di protezione dei dati previsti nell'APPI.

(i) Nella misura in cui la fornitura da parte di Dynatrace delle Offerte Dynatrace comporti il trasferimento dei Dati personali del Cliente provenienti da Israele a un Paese terzo che ai sensi delle Leggi applicabili in Israele non fornisce un livello adeguato di protezione dei Dati personali del Cliente, il Cliente sarà responsabile di garantire una base giuridica per l'esportazione dei Dati personali del Cliente. Per chiarezza, il presente DPA costituisce l'obbligo scritto di Dynatrace di adottare le adeguate misure di salvaguardia richieste dalle Normative sulla protezione della privacy (Trasferimento transfrontaliero dei dati), 2001. Per chiarezza, gli obblighi del presente DPA sono ritenuti sufficienti dal Cliente per facilitare il trasferimento di informazioni al di fuori di Israele in conformità al Regolamento 3 della Normativa sulla protezione della privacy (Trasferimento di dati a banche dati al di fuori dei confini del Paese), 2001.

14. Termini aggiuntivi specifici delle leggi sulla privacy degli Stati Uniti.

(a) La definizione di "Legge applicabile in materia di protezione dei dati include le Leggi statali sulla Privacy degli Stati Uniti. "Leggi statali sulla Privacy degli Stati Uniti" indica tutte le leggi statali relative alla tutela e al trattamento dei dati personali in vigore negli Stati Uniti d'America, che possono includere, a titolo esemplificativo man on limitativo, la Legge sulla Privacy del Consumatore della California (California Consumer Privacy Act), così come modificata dalla Legge sui Diritti alla Privacy della California ("CCPA" o California Privacy Rights Act), e simili normative sulla privacy del consumatore in altri stati, in ciascun caso, così come modificate, integrate, o sostituite di volta in volta).

(b) Laddove Dynatrace tratti i Dati Personali del Cliente soggetti alle Leggi statali sulla Privacy degli Stati Uniti, Dynatrace risulta essere "fornitore di servizi", o "responsabile del trattamento" (come applicabile) in caso di trattamento dei Dati Personali del Cliente. Il Cliente comunica, o diversamente rende disponibili, i Dati Personali del Cliente a Dynatrace per la finalità limitata e specifica della fornitura di Offerte Dynatrace in conformità all'Accordo (la "Finalità"). Dynatrace dovrà (e imporrà ai propri Sub-responsabili del trattamento di):

i. rispettare gli obblighi ad essa applicabili nel suo ruolo di fornitore di servizi ai sensi delle Leggi statali sulla Privacy degli Stati Uniti;

ii. notificare se non può più adempiere ai propri obblighi ai sensi delle Leggi statali sulla Privacy degli Stati Uniti;

iii. astenersi dal "vendere" o "condividere" (alla stregua della definizione di tali termini ai sensi del CCPA) i Contenuti del Cliente o conservare, utilizzare o divulgare i Dati Personali del Cliente: (1) per qualunque scopo diverso dalla Finalità, inclusa la conservazione, l'utilizzo, o la divulgazione dei Dati Personali del Cliente a scopo commerciale diverso dalla Finalità, o come diversamente consentito dalle Leggi statali sulla Privacy degli Stati Uniti; oppure (2) al di fuori del rapporto commerciale diretto tra il Cliente e Dynatrace; oppure, salvo diversamente consentito dalle Leggi statali sulla Privacy degli Stati Uniti, astenersi dal combinare i Dati Personali del Cliente con i Dati Personali che Dynatrace riceve da, o per conto di un'altra attività o soggetto, o che essa raccoglie dalle proprie interazioni con persone fisiche, a meno che tale combinazione non sia richiesta per perseguire qualsiasi finalità commerciale consentita dalle Leggi statali sulla Privacy degli Stati Uniti.

iv. Il Cliente dovrà: (1) previa comunicazione, avere il diritto di intraprendere azioni ragionevoli ed appropriate concordate tra le parti per contribuire ad assicurarsi che Dynatrace Tratti i Dati Personali del Cliente in maniera conforme agli obblighi del Cliente ai sensi delle Leggi statali sulla Privacy degli Stati Uniti e interrompere e porre rimedio al Trattamento non autorizzato dei Dati Personali del Cliente da parte di Dynatrace; (2) comunicare al Cliente qualora esso determini che non è più in grado di soddisfare i propri obblighi ai sensi delle Leggi statali sulla Privacy degli Stati Uniti in relazione ai Dati Personali del Cliente.

v. Dynatrace riconosce e conferma che essa non riceve i Dati Personali del Cliente quale corrispettivo per eventuali Offerte fornite al Cliente. Dynatrace certifica che comprende e che rispetterà i propri obblighi ai sensi delle Leggi statali sulla Privacy degli Stati Uniti.

5 Disposizioni varie

(a) Fatto salvo quanto emendato dal presente Accordo, l'Accordo rimarrà pienamente valido ed efficace. Qualsiasi modifica al presente Accordo dovrà essere messa per iscritto ed essere debitamente firmata dai rappresentanti autorizzati delle parti.

(b) Fatta salva qualsiasi disposizione contraria contenuta nel Contratto o nel presente Accordo, la responsabilità di ciascuna parte e di tutte le sue Affiliate, presa nel suo complesso, ascrivibile o correlata al presente Accordo, qualsiasi ordine o il Contratto, sia per contratto, illecito civile o qualsiasi altra teoria di responsabilità, rimarrà soggetto alla sezione "Limitazione di responsabilità" dell'Accordo, e qualsiasi riferimento di cui in tale sezione alla responsabilità di una parte indica la responsabilità complessiva di tale parte e di tutte le sue Affiliate ai sensi del Contratto e del presente Accordo, inclusi tutti gli Allegati. Dynatrace non sarà responsabile nei confronti del Cliente per perdite o danni, perdite di profitto, perdite di vendite, perdite di attività, perdite di risparmi previsti, perdite o danni all'avviamento di natura indiretta o consequenziale, o altrimenti, in ogni caso, di natura diretta o indiretta, che siano imputabili o correlati al presente DPA. Senza limitare gli obblighi delle parti ai sensi dell'Accordo o del presente DPA, il Cliente accetta che qualsiasi responsabilità posta a carico di Dynatrace in relazione ai Dati personali del Cliente che sorga a seguito di, o in relazione all'inadempimento da parte del Cliente dei propri obblighi ai sensi del presente DPA o della Legge applicabile in materia di protezione dei dati conterà ai fini di e ridurrà il limite di responsabilità di Dynatrace ai sensi del Contratto (o, se applicabile, ai sensi del presente Accordo, come se si trattasse di responsabilità nei confronti del Cliente. Fatta salva qualsiasi disposizione contraria contenuta nel presente Accordo(inclusi, a titolo esemplificativo ma non esaustivo, gli obblighi di indennizzo delle parti), nessuna delle parti sarà responsabile per eventuali multe emesse o applicate ai sensi dell'art. 83 del GDPR contro l'altra parte da un'autorità regolatoria o da un ente governativo in relazione alla violazione del GDPR da parte di tale altra parte.

(c) Il presente DPA sarà disciplinato e interpretato in conformità alle disposizioni di legge e giurisdizione vigenti nelContratto, a condizione che le Clausole contrattuali tipo siano disciplinate come stabilito nella Sezione 13 del presente Accordo.

Concordato e accettato da:	Concordato e accettato da:
Nome_entità_Cliente	**Nome_entità_Dynatrace**
Firma autorizzata	Firma autorizzata
Nome	Nome
Qualifica	Qualifica
Data	Data
Indirizzo	Indirizzo
Numero della Società (se applicabile)	Numero della Società (se applicabile)

ALLEGATO A
DETTAGLI DEL TRATTAMENTO

Descrizione dell'esportatore dei dati

L'esportatore è l'entità giuridica identificata come il "Cliente" o "Dynatrace", in caso di Sub-trattamento, nell'Accordo sul trattamento dei dati in vigore tra l'esportatore e l'importatore e al quale Accordo è accluso il presente Allegato.

Descrizione dell'importatore dei dati

L'importatore è l'entità giuridica identificata come "Dynatrace" o un Sub-responsabile del trattamento debitamente autorizzato nell'Accordo sul trattamento dei dati in vigore tra l'esportatore e l'importatore e al quale Accordo è accluso il presente Allegato.

Oggetto e durata del trattamento

L'oggetto e la durata del trattamento sono i seguenti:

Per quanto riguarda le Parti, il Cliente sarà il Titolare del trattamento di alcuni Dati personali del Cliente forniti a Dynatrace dal Cliente in relazione al suo utilizzo delle Offerte Dynatrace. La durata del trattamento corrisponderà al periodo di validità dell'Accordo.

Finalità del trattamento

Il trattamento è necessario per le seguenti finalità:

Consentire a Dynatrace di fornire le Offerte Dynatrace al Cliente ed esercitare i suoi diritti e obblighi ai sensi dell'Accordo.

Soggetti Interessati

I Soggetti interessati possono includere: (i) utenti autorizzati dal Cliente a utilizzare le Offerte Dynatrace e (ii) utenti o visitatori delle applicazioni e/o dei siti web monitorati del Cliente (inclusi, a titolo esemplificativo ma non esaustivo, i dipendenti, i clienti, gli agenti, gli appaltatori e i consulenti del Cliente), come determinato a esclusiva discrezione del Cliente.

Tipo di Dati personali

Il Cliente è tenuto a fornire determinati Dati personali al fine di utilizzare le Offerte Dynatrace, tra cui l'indirizzo IP e il nome e cognome se inclusi nell'indirizzo e-mail e nelle credenziali dell'utente. Il Cliente può inviare Dati personali aggiuntivi alle Offerte Dynatrace, la cui finalità è determinata e controllata dal Cliente a sua esclusiva discrezione.

Categorie speciali di dati o dati personali sensibili (se appropriato)

I Dati personali trasferiti riguardano le seguenti categorie speciali di dati o dati personali sensibili:

Non applicabile. Il Cliente non può utilizzare le Offerte Dynatrace per trattare qualsiasi dato classificato cui si applichino restrizioni speciali o "dati personali sensibili", salvo espliciti accordi scritti fra le Parti.

Operazioni di trattamento

I dati personali trasferiti saranno soggetti alle seguenti attività di trattamento di base:

Dynatrace tratterà i Dati personali del Cliente solo se necessario per fornire le Offerte Dynatrace ed esercitare i propri diritti e obblighi come contenuti nei termini dell'Accordo e del presente Accordo sul trattamento dei dati, inclusi, a titolo esemplificativo ma non esaustivo, l'abilitazione del cliente, il supporto tecnico, i servizi professionali, il miglioramento delle prestazioni e delle funzioni delle Offerte Dynatrace, l'autenticazione e le comunicazioni degli utenti e l'amministrazione degli account.

ALLEGATO B

MISURE DI SICUREZZA

Dynatrace (indicata anche nel presente documento come il "Responsabile del trattamento") attuerà quantomeno le misure di sicurezza tecniche e organizzative descritte di seguito in relazione ai Dati personali del Cliente, i quali tratta per conto del Cliente (indicato nel presente documento anche come il "Titolare del trattamento"). Queste misure di sicurezza saranno applicate a tutti i Dati personali del Cliente oggetto dell'accordo di fondo tra il Responsabile del trattamento e il Titolare del trattamento (l'"Accordo"). In relazione ai sub-responsabili del trattamento terzi che potrebbero trattare i Dati personali per conto di Dynatrace, tali terzi saranno soggetti ai propri requisiti di sicurezza per la protezione dei Dati personali.

Misure tecniche

1.1 Autorizzazione

(a) Quando si utilizzano diversi profili di autorizzazione per scopi diversi, va utilizzato un sistema di autorizzazione.

1.2 Identificazione

(a) A ogni Utente autorizzato deve essere rilasciato un codice identificativo personale e univoco a tale scopo ("ID utente"). Un ID utente non può essere assegnato a un'altra persona, neanche in un momento successivo.

(b) Occorre tenere un registro aggiornato degli Utenti autorizzati, e l'accesso autorizzato disponibile per ciascuno di essi, e bisogna stabilire delle procedure di identificazione e autenticazione per tutti gli accessi ai sistemi informatici o per svolgere qualsiasi attività di Trattamento dei dati. Ai fini del presente atto, "Trattamento" si riferisce a qualsiasi operazione o insieme di operazioni eseguite sui Dati, con o senza mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o l'alterazione, il recupero, la consultazione, l'uso, la divulgazione mediante trasmissione, la diffusione o altra messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

(c) Le password devono essere modificate periodicamente come stabilito nelle Politiche sulla sicurezza delle informazioni.

1.3 Autenticazione

(a) Agli Utenti autorizzati sarà consentito trattare i Dati se vengono loro fornite credenziali di autenticazione tali da completare correttamente una procedura di autenticazione relativa a una specifica operazione di Trattamento o a una serie di operazioni di Trattamento.

(b) L'autenticazione deve essere basata su una password segreta associata all'ID utente e tale password deve essere nota solo all'utente autorizzato.

(c) Una o più credenziali di autenticazione saranno assegnate o associate a un Utente autorizzato.

(d) Deve essere prevista una procedura per la riservatezza e l'integrità delle password. Le password devono essere memorizzate in maniera tale da essere indecifrabili per tutto il periodo della loro validità. Deve essere in atto una procedura per l'assegnazione, la distribuzione e l'archiviazione delle password.

(e) Le password devono essere composte da almeno dodici caratteri o, se ciò non è tecnicamente consentito dai sistemi informatici pertinenti, devono essere costituite dal numero massimo di

caratteri consentito. Le password non devono contenere alcun elemento che possa essere facilmente correlato all'Utente autorizzato responsabile del Trattamento e devono essere modificate a intervalli regolari, intervalli che devono essere indicati nel documento di sicurezza. Le password devono essere modificate dall'Utente autorizzato in base a un valore segreto noto solo all'Utente autorizzato al loro primo utilizzo e successivamente con cadenza periodica.

(f) Oltre a una combinazione valida di ID utente e password, tutti gli accessi ai dati o ai sistemi Dynatrace devono essere protetti da una soluzione di autenticazione a più fattori (Multi-Factor Authentication, "MFA"). La soluzione MFA può essere di natura software o hardware.

(g) Le credenziali di autenticazione saranno disattivate anche se l'Utente autorizzato viene licenziato, trasferito o privato della sua autorizzazione all'accesso ai sistemi informatici o ai Dati di trattamento.

1.4 Controlli dell'accesso

(a) Solo gli Utenti autorizzati avranno accesso ai Dati, anche quando essi sono archiviati su supporti elettronici o portatili o vengono trasmessi. Gli Utenti autorizzati avranno accesso autorizzato solo ai dati e alle risorse necessari per svolgere le proprie mansioni.

(b) Deve essere utilizzato un sistema per concedere agli Utenti autorizzati l'accesso ai dati e alle risorse designati.

(c) Occorre verificare con cadenza semestrale che i prerequisiti per il mantenimento dei relativi profili di autorizzazione siano ancora validi. Tale verifica riguarda anche l'elenco degli Utenti autorizzati redatto per categorie omogenee di attività e il corrispondente profilo di autorizzazione.

(d) Vanno messe in atto delle misure per impedire che un utente ottenga l'accesso o l'uso non autorizzato dei sistemi informatici. In particolare, devono essere installati sistemi di rilevamento delle intrusioni che riflettano le migliori pratiche del settore per proteggere i sistemi informatici da accesso non autorizzato.

(e) I controlli dell'accesso al sistema operativo o al database devono essere configurati correttamente per garantire solo l'accesso autorizzato.

(f) Solo il personale autorizzato sarà in grado di concedere, modificare o annullare l'accesso da parte degli utenti ai sistemi informatici.

1.5 Gestione dei sistemi informatici e dei supporti rimovibili

(a) I sistemi informatici di rete e i supporti fisici su cui sono archiviati i Dati devono essere conservati in un ambiente sicuro, con accesso fisico limitato al solo personale autorizzato. Vanno mantenuti rigorosi controlli di autorizzazione e accesso.

(b) Il software, il firmware e l'hardware utilizzati nei sistemi informatici devono essere esaminati annualmente al fine di rilevare, e quindi risolvere, eventuali vulnerabilità e difetti riscontrati nei sistemi informatici.

(c) Dovranno essere istituite politiche e attività di formazione per quanto riguarda la conservazione e l'utilizzo dei supporti su cui i Dati sono conservati al fine di prevenire l'accesso e il Trattamento non autorizzati.

(d) Quando i supporti devono essere smaltiti o riutilizzati, devono essere adottate le misure necessarie a impedire un eventuale recupero successivo dei Dati e di altre informazioni precedentemente memorizzate su tali supporti, oppure a renderle altrimenti indecifrabili o impedire che vengano ricostruite con qualsiasi mezzo tecnico prima di essere ritirate dall'inventario. Tutti i supporti riutilizzabili impiegati per la conservazione dei dati saranno sovrascritti almeno tre volte con dati randomizzati prima dello smaltimento o del riutilizzo.

(e) La rimozione di supporti contenenti Dati dai locali designati deve essere specificamente

autorizzata dal Titolare del trattamento ed essere eseguita in conformità alle politiche di Dynatrace.

(f) I supporti contenenti Dati devono essere cancellati o resi illeggibili in caso di inutilizzo e prima del corretto smaltimento.

1.6 Distribuzione o trasmissione

(a) I dati devono essere disponibili solo per gli Utenti autorizzati.

(b) Per proteggere i Dati trasmessi elettronicamente su una rete pubblica o archiviati su un dispositivo portatile, o laddove vi sia la necessità di archiviare o trattare i Dati in un ambiente fisicamente non sicuro, è necessario utilizzare la crittografia (a 128 bit o più) o altra forma di protezione equivalente.

(c) Quando i Dati devono lasciare i locali designati a seguito di operazioni di manutenzione, devono essere adottate le misure necessarie a impedire qualsiasi recupero non autorizzato dei Dati e di altre informazioni ivi memorizzate.

(d) Laddove i Dati siano trasmessi o trasferiti su una rete di comunicazioni elettronica, saranno adottate misure per controllare il flusso di dati e registrare la tempistica della trasmissione o del trasferimento, i Dati trasmessi o trasferiti, la destinazione di tali Dati trasmessi o trasferiti e i dettagli dell'Utente autorizzato che esegue la trasmissione o il trasferimento.

1.7 Conservazione, copie di backup e recupero

(a) Devono essere definite e stabilite procedure per la produzione di copie di backup e per il recupero dei dati. Queste procedure devono prevedere che i Dati siano ripristinati allo stato in cui si trovavano al momento della loro perdita o distruzione.

(b) Le copie di backup devono essere prodotte almeno una volta alla settimana, a meno che in tale periodo non siano stati aggiornati i Dati.

(c) Devono essere applicate delle procedure di recupero dati e deve essere conservata una copia di backup in un luogo diverso dal sito in cui si trovano i sistemi informatici che trattano i dati; questi requisiti minimi di sicurezza si applicano a tali copie di backup.

1.8 Antivirus e rilevamento delle intrusioni

(a) Sui sistemi informatici devono essere installati software antivirus e dei sistemi di rilevamento delle intrusioni per proteggere tali sistemi informatici da attacchi o altre azioni non autorizzate. I software antivirus e i sistemi di rilevamento delle intrusioni devono essere aggiornati regolarmente in conformità alle migliori pratiche del settore per i sistemi informatici interessati (e comunque con cadenza non inferiore a una volta all'anno).

1.9 Test

(a) I test condotti prima dell'implementazione o modifica dei sistemi informatici che trattano i dati non devono utilizzare dati reali o "live", a meno che tale uso non sia necessario e non vi sia alcuna alternativa ragionevole. Laddove vengano utilizzati dati reali o "live", questi saranno limitati nella misura necessaria ai fini del test e deve essere garantito il livello di sicurezza corrispondente al tipo di Dati trattati.

1.10 Revisione

(a) Devono essere eseguite delle revisioni regolari, e comunque non meno di una volta all'anno, in conformità a questi requisiti di sicurezza.

(b) I risultati devono fornire un parere sul grado di conformità delle misure di sicurezza e dei controlli adottati a tali requisiti di sicurezza, individuare eventuali lacune e (se del caso) proporre eventuali misure correttive o supplementari necessarie. Devono inoltre includere i dati, i fatti e le osservazioni a sostegno dei pareri formulati e delle raccomandazioni proposte.

2. Misure organizzative

2.1 Piano e documento di sicurezza

- Le misure adottate per rispettare questi requisiti di sicurezza saranno oggetto delle Politiche sulla sicurezza delle informazioni della Società e definite in un portale di sicurezza, che sarà mantenuto aggiornato e rivisto ogni volta che vengono apportate delle modifiche rilevanti al/i sistema/i informatico/i o alle misure tecniche o organizzative.
- Le Politiche sulla sicurezza delle informazioni devono riguardare:

  (i) Misure di sicurezza relative alla modifica e alla manutenzione del/i sistema/i utilizzato/i per trattare i dati, tra cui lo sviluppo e la manutenzione delle applicazioni, l'adeguato supporto del fornitore e un inventario di hardware e software;

  (ii) Sicurezza fisica, compresa la sicurezza degli edifici o dei locali in cui si svolge il Trattamento dei dati, la sicurezza delle apparecchiature di dati e dell'infrastruttura di telecomunicazione e i controlli ambientali; e

  (iii) Sicurezza dei computer e dei sistemi di telecomunicazione, comprese le procedure per la gestione delle copie di backup, le procedure relative ai virus informatici, le procedure per la gestione di segnali/codici, la sicurezza per l'implementazione del software, la sicurezza relativa ai database, la sicurezza per la connessione dei sistemi a Internet, l'ispezione dell'elusione di sistemi di dati, i meccanismi per registrare i tentativi di violazione della sicurezza del sistema o di ottenere un accesso non autorizzato.

- Il piano di sicurezza includerà tutte le politiche di Dynatrace, aggiornate di volta in volta, tra cui, a titolo esemplificativo ma non esaustivo:

  (i) Codice di condotta ed etica aziendale

  (ii) Politica globale sulla protezione dei dati

  (iii) Politica sull'uso accettabile dei servizi IT di Dynatrace

  (iv) Politiche sulla sicurezza del sistema: Politica di gestione del controllo degli accessi; Standard di conservazione dei backup; Politica di gestione delle modifiche; Politica di gestione delle modifiche - Sistemi aziendali; Politica di conformità; Piano di risposta agli incidenti di sicurezza informatica e dei dati; Politica sulla classificazione dei dati; Politica sulla prevenzione della perdita di dati; Politica sul monitoraggio elettronico; Politica sulla crittografia; Politica sulla sicurezza delle Risorse umane; Politica sulla gestione delle risorse informatiche; Politica sulla gestione del rischio per le informazioni; Politica sulle operazioni IT; Politica sui dispositivi mobili; Politica di accesso alla rete; Politica sulla password dell'account di rete; Politica sul firewall di rete; Politica sulla sicurezza fisica e ambientale; Politica sulla restituzione dei beni per i dipendenti licenziati; Politica di phishing per la sicurezza; Politica sul ciclo di vita dell'account di servizio; Politica di gestione dei fornitori; Politica di gestione delle vulnerabilità; Politica sulla sicurezza della workstation di Dynatrace.

  (v) Il piano di sicurezza sarà disponibile per il personale che ha accesso ai Dati e ai sistemi informatici e dovrà coprire almeno i seguenti aspetti:

  (vi) L'ambito, con una specifica dettagliata delle risorse protette;

  (vii) Le misure, gli standard, le procedure, le regole e norme del codice di condotta per garantire

la sicurezza, compresi il controllo, l'ispezione e la supervisione dei sistemi informatici;

(viii) Le procedure per la segnalazione, la gestione e la risposta relativamente agli incidenti; e

(ix) Le procedure per produrre copie di back-up e recuperare i Dati, compreso il membro del personale che ha intrapreso l'attività di Trattamento, i Dati ripristinati e, a seconda dei casi, quali dati dovevano essere inseriti manualmente nel processo di recupero.

2.2 Funzioni e obblighi del personale

- Solo i membri del personale che hanno una legittima necessità operativa di accedere ai sistemi informatici o di eseguire qualsiasi Trattamento dei dati saranno autorizzati a farlo ("**Utenti autorizzati**").

- Saranno adottate le misure necessarie per formare e far conoscere al personale questi requisiti minimi di sicurezza, tutte le politiche pertinenti e le leggi applicabili riguardanti l'esecuzione delle loro funzioni e dei loro doveri in relazione al trattamento dei dati e le conseguenze di qualsiasi violazione di tali requisiti.
- Le funzioni e gli obblighi del personale che ha accesso ai Dati e ai sistemi informatici devono essere chiaramente definiti attraverso ruoli di sicurezza delle applicazioni.
- Gli Utenti autorizzati devono essere istruiti in merito al fatto che le apparecchiature elettroniche non vanno lasciate incustodite o rese accessibili durante le sessioni di Trattamento. L'accesso fisico alle aree in cui sono archiviati i Dati sarà limitato agli Utenti autorizzati. Le misure disciplinari per una violazione del piano di sicurezza devono essere chiaramente definite, documentate e comunicate al personale.

2.3 Responsabile della sicurezza

- Una o più persone responsabili della conformità complessiva a questi requisiti minimi di sicurezza saranno designate come Responsabile/i della sicurezza delle informazioni (Chief Information Security Officer, "**CISO**"). Il CISO deve essere adeguatamente formato e competente nella gestione della sicurezza delle informazioni e deve disporre di risorse adeguate a garantire efficacemente la conformità.
- Su richiesta, i recapiti del CISO saranno forniti al Titolare del trattamento.

2.4 Conservazione di registri

- Deve essere registrata, con una traccia di revisione sicura, una cronologia dell'accesso o della divulgazione dei Dati da parte dell'Utente autorizzato.
- Solo il personale debitamente autorizzato può avere accesso fisico ai locali in cui sono archiviati i sistemi informatici e i supporti su cui sono memorizzati i Dati.
- Sarà adottata una procedura per segnalare, rispondere e gestire gli incidenti di sicurezza, come le violazioni della sicurezza dei dati. Tale procedure deve includere almeno:

  (i) Una procedura per segnalare tali incidenti/violazioni ai dirigenti competenti;

  (ii) Un team chiaramente designato, e guidato dal CISO, per la gestione e il coordinamento della risposta a un incidente;

  (iii) Un processo documentato per la gestione della risposta a un incidente, compreso il requisito di mantenere un opportuno registro delle problematiche e delle azioni e così includere l'ora in cui si è verificato l'incidente, la persona che ha segnalato l'incidente, a chi è stato segnalato e gli effetti dello stesso;

(iv) L’obbligo per il Responsabile del trattamento di informare il Titolare del trattamento senza indebito ritardo in caso di una violazione della sicurezza che comporti l’accidentale o illecita distruzione, perdita, alterazione, o la divulgazione o l’accesso non autorizzati ai Dati trasmessi, archiviati o altrimenti trattati dal Responsabile del trattamento; e

(v) Il team di gestione della sicurezza/degli incidenti del Responsabile del trattamento deve collaborare, se del caso, con i rappresentanti della sicurezza del Titolare del trattamento fino a quando l’incidente o la violazione non venga risolto/a in modo soddisfacente.

(vi) La procedura per la segnalazione, la gestione e la risposta agli incidenti deve essere testata almeno una volta all’anno.