Accordo per il Trattamento dei Dati ai sensi del RGPD e Clausole Contrattuali Tipo

Il presente Accordo per il trattamento dei dati ai sensi del RGPD ("**DPA**") viene stipulato tra l'entità identificata più avanti come titolare del trattamento (il "**Titolare del trattamento**") e Proofpoint, Inc., 925 W. Maude Avenue, Sunnyvale, CA 94085 ("**Responsabile del trattamento**" o "**Proofpoint**") e viene allegato: (1) al Contratto Quadro d'Abbonamento o alle Condizioni generali di Proofpoint e ai Product Exhibit applicabili, (2) a un contratto di licenza con l'utente finale (Accordo online con il Cliente, un accordo di licenza con l'utente finale (EULA), accordo clickwrap, se applicabile, o clickthrough) accettato dal Titolare del trattamento al momento della sua registrazione e accesso iniziale al prodotto o servizio di Proofpoint, o (3) a qualsiasi altro contratto di licenza scritto e firmato tra le parti, in base al quale il Responsabile del trattamento fornisce prodotti o servizi al Titolare del trattamento ("**Contratto per i Servizi**"). Il presente DPA entra in vigore alla data in cui è firmato dal Titolare del trattamento, ma solo se Proofpoint riceve il DPA firmato in conformità alle istruzioni riportate più avanti.

Il presente DPA stabilisce i termini e le condizioni in base ai quali il Responsabile del trattamento può ricevere Dati Personali dal Titolare del trattamento e trattarli. Il presente DPA tiene conto della natura del trattamento ai sensi del Contratto per i Servizi e descrive le misure tecniche e organizzative adeguate intraprese nel trattamento dei Dati Personali dal Responsabile del trattamento.

Inoltre il presente DPA incorpora le Clausole Contrattuali Tipo allegate alla decisione della Commissione Europea (UE) 2021/914 (le "**Clausole SCC**"). Oltre agli obblighi di Proofpoint indicati nel presente DPA, Proofpoint rispetterà gli obblighi di un importatore stabiliti nelle Clausole SCC. Qualsiasi riferimento all'**Importatore** sarà da considerarsi come un riferimento a **Proofpoint, Inc., ovvero al Responsabile del trattamento**, mentre qualsiasi riferimento all'**Esportatore** o al Titolare del trattamento sarà da considerarsi come un riferimento al **Responsabile del trattamento** e alle sue società affiliate all'interno dell'Unione Europea. Con il presente documento il Titolare del trattamento dichiara e garantisce di avere il diritto e l'autorità di stipulare il presente DPA per conto proprio e delle proprie società affiliate.

Le parti del presente DPA accettano di essere vincolate ai termini e alle condizioni degli Allegati 1 (Termini del trattamento dei dati) e 2 (Clausole contrattuali tipo) e delle relative Appendici. Il presente DPA è stato preventivamente firmato dal Responsabile del trattamento, Proofpoint, Inc. Affinché il DPA divenga efficace, il Titolare del trattamento deve prima:

1. inserire le proprie informazioni e la firma nelle apposite righe più avanti, indicando la ragione sociale completa del Titolare del trattamento, l'indirizzo e le informazioni del firmatario; e
2. inviare il DPA completato e firmato a Proofpoint via e-mail all'indirizzo privacy@proofpoint.com.

Se il Titolare del trattamento effettua cancellazioni o altre revisioni al presente DPA, tali cancellazioni o revisioni vengono fin d'ora respinte e non saranno valide, salvo diversamente accordato da Proofpoint. Il firmatario del Titolare del trattamento dichiara e garantisce di avere l'autorità legale di vincolare il Titolare del trattamento al presente DPA. Il presente DPA terminerà automaticamente alla risoluzione del Contratto per i Servizi o a una data precedente, secondo quanto stabilito nei termini del presente DPA.

Accettato e approvato dal Titolare del trattamento:		Accettato e approvato da **Proofpoint, Inc.:** (**Responsabile del trattamento**)	
Firma:	_____	Firma:	DocuSigned by: Paul Auvil 2955B8CEBD2B45C...
Nome:	_____	Nome:	Paul Auvil, CFO
Data:	_____		
Società:	_____		
Indirizzo:	_____		
	_____		

ALLEGATO 1

TERMINI DEL TRATTAMENTO DEI DATI

1. Definizioni.

a. Tutti i termini utilizzati senza una definizione nel presente DPA hanno il significato loro attribuito, in primo luogo, nel Regolamento generale sulla protezione dei dati (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (**RGDP**), e in secondo luogo nel Contratto per i Servizi.

b. **Dati del Titolare del trattamento** si riferisce ai Dati Personali del Titolare del trattamento, Dati Personali così come definiti nel RGPD.

c. **Leggi sulla Protezione dei Dati** si riferisce a tutte le leggi e i regolamenti applicabili riguardo al trattamento dei Dati Personali nella misura relativa alla fornitura dei prodotti e servizi di Proofpoint in base al Contratto per i Servizi.

d. **Interessato** si riferisce a la persona identificata o identificabile a cui si riferiscono i Dati Personali.

e. **Trattamento** (e le parole relative) ha il significato definito nell'articolo 4.2 RGPD.

f. **Sub-responsabile del trattamento** si riferisce a ogni responsabile del trattamento incaricato dal Responsabile del trattamento per trattare Dati Personali.

g. **Autorità di Controllo** si riferisce a un'autorità pubblica istituita da uno Stato membro dell'UE ai sensi del RGPD.

2. Trattamento dei Dati Personali.

a. Le parti convengono, in relazione alle attività descritte nell'Appendice 1, che il Titolare del trattamento e le sue società affiliate all'interno dell'Unione Europea (o le loro affiliate o clienti) saranno i titolari del trattamento/esportatori e che il Responsabile del trattamento sarà il responsabile del trattamento/importatore nella misura in cui si occupa del trattamento dei Dati Personali. Il Titolare del trattamento dichiara e garantisce che le sue istruzioni al Responsabile del trattamento per quanto riguarda il trattamento dei Dati Personali sono e saranno conformi alle disposizioni pertinenti delle leggi applicabili sulla protezione dei dati.

b. L'oggetto e la durata del trattamento dei Dati Personali sono esposti nel Contratto per i Servizi, che descrive la fornitura dei servizi al Titolare del trattamento. La natura e la finalità del trattamento, i tipi di Dati Personali e le categorie di interessati sono definiti nell'Appendice 1 al presente DPA.

c. Il Titolare del trattamento è responsabile dell'accuratezza, qualità e legittimità dei Dati Personali e dei mezzi con cui li ha acquisiti.

d. Il Contratto per i Servizi e il presente DPA costituiscono le istruzioni del Titolare del trattamento al Responsabile del trattamento per quanto riguarda: (1) il trattamento dei Dati Personali e (2) il trasferimento di tali Dati Personali in qualsiasi paese o territorio, quando è ragionevolmente necessario per la fornitura dei servizi.

3. Valutazione d'impatto sulla protezione dei dati ("DPIA")

Tenendo conto della natura del Trattamento, il Responsabile del trattamento potrà fornire al Titolare del trattamento la cooperazione ragionevole e l'assistenza necessaria per l'adempimento degli obblighi del Titolare del trattamento in base al RGPD di effettuare una valutazione d'impatto sulla protezione dei dati relativa all'uso dei Servizi da parte del Titolare del trattamento, nella misura in cui il Titolare del trattamento non può avere altrimenti accesso a informazioni utili e in cui il Responsabile del trattamento dispone di tali informazioni. Il Responsabile del trattamento fornirà al Titolare del trattamento l'assistenza ragionevole nella cooperazione o consultazione preventiva con l'Autorità di Controllo per eseguire i suoi compiti relativi all'obbligo di DPIA del Titolare del trattamento nella misura richiesta dal RGPD.

4. **Diritti degli interessati.** Il Responsabile del trattamento, nella misura consentita dalla legge, comunicherà tempestivamente al Titolare del trattamento l'eventuale ricezione di una richiesta di un interessato di esercitare i suoi diritti d'accesso, di rettifica, di limitazione del trattamento, all'oblio, alla portabilità dei dati, di opposizione al trattamento e di non essere sottoposto a un processo decisionale individuale automatizzato. Tenendo conto della natura del Trattamento, il Responsabile del trattamento assisterà il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alla richiesta dell'interessato.

5. **Utilizzo limitato di Dati Personali e personale.** A eccezione di quanto stabilito diversamente nel Contratto per i Servizi, (i) il Responsabile del trattamento non acquisirà alcun diritto con riferimento ai Dati Personali e (ii) il Responsabile del trattamento e le sue società affiliate dovranno adottare misure ragionevoli per garantire l'affidabilità di ogni dipendente, agente o fornitore di qualsiasi Sub-responsabile del trattamento ingaggiato che possa avere accesso ai Dati Personali, garantendo in ogni caso che l'accesso sia strettamente limitato alle persone che hanno necessità di conoscere/accedere ai Dati Personali pertinenti, in quanto strettamente necessario ai fini del Contratto per i Servizi, e dovranno rispettare le leggi applicabili sulla protezione dei dati e sulla privacy, assicurando che tali persone siano tutte soggette a impegni di riservatezza o a obblighi professionali o di riservatezza previsti per legge.

6. **Sub-responsabili del trattamento**.

a. **Nomina di Sub-responsabili del trattamento**. Il Titolare del trattamento fornisce un'autorizzazione generale al ricorso a Sub-responsabili del trattamento da parte del Responsabile del trattamento. Il Titolare del trattamento riconosce e accetta che (a) le società affiliate del Responsabile del trattamento possano essere impegnate come Sub-responsabili del trattamento e (b) il Responsabile del trattamento e le sue società affiliate possano rispettivamente ingaggiare Sub-responsabili del trattamento terzi in relazione alla fornitura dei Servizi. Il Responsabile del trattamento o le sue società affiliate hanno stipulato un accordo scritto con ciascun Sub-responsabile del trattamento contenente obblighi di protezione dei dati non meno protettivi di quelli contenuti nel presente DPA per quanto riguarda la protezione dei dati del Titolare del trattamento nella misura applicabile alla natura dei servizi forniti da tale Sub-responsabile del trattamento. Il Responsabile del trattamento rimane pienamente responsabile nei confronti del Titolare del trattamento dell'adempimento degli obblighi dei Sub-responsabili del trattamento in conformità al contratto stipulato con il Responsabile del trattamento.

b. **Elenco**. L'elenco attuale dei Sub-responsabili del trattamento per i servizi è disponibile sul sito Proofpoint Trust: https://www.proofpoint.com/us/legal/trust. Nel caso che il Responsabile del trattamento faccia un qualsiasi cambiamento o aggiunta a tale elenco, nella misura in cui il Titolare del trattamento abbia aderito a ricevere notifiche sul sito Trust, il Responsabile del trattamento comunicherà tali cambiamenti via e-mail. Le parti convengono che questa notifica soddisfi i requisiti di notifica secondo l'articolo 28, paragrafo 2, del RGPD e la Clausola 9 delle Clausole Contrattuali Tipo.

c. **Opposizione.** Il Titolare del trattamento può opporsi alla nomina di un nuovo Sub-responsabile del trattamento da parte del Responsabile del trattamento comunicando prontamente per iscritto l'opposizione al Responsabile del trattamento a privacy@proofpoint.com. Nel caso in cui il Titolare del trattamento si opponga a un nuovo Sub-responsabile del trattamento, il Responsabile del trattamento (dopo avere ricevuto l'obiezione scritta del Titolare del trattamento come indicato nella frase precedente) determinerà ragionevolmente se sia possibile mettere a disposizione del Titolare del trattamento una soluzione per evitare il trattamento di Dati Personali da parte del nuovo Sub-responsabile del trattamento oggetto dell'opposizione senza gravare eccessivamente sul Titolare del trattamento. Se il Responsabile del trattamento non è in grado di rendere disponibile tale modifica entro un periodo di tempo ragionevole, che non deve superare i trenta (30) giorni, il Titolare del trattamento potrà porre fine al documento d'ordine applicabile solo per quanto riguarda i Servizi che non possono essere forniti dal Responsabile del trattamento senza ricorrere al nuovo Sub-responsabile del trattamento oggetto dell'opposizione, inviando una comunicazione scritta al Responsabile del trattamento entro trenta (30) giorni dalla decisione del Responsabile del trattamento.

7. **Categorie particolari di Dati Personali.** Il Titolare del trattamento (e le sue società affiliate nell'Unione Europea) sono gli unici responsabili del rispetto delle Leggi sulla Protezione dei Dati e sulla privacy, così come applicabili al Titolare del trattamento (e alle sue società affiliate nell'Unione Europea), compresi tutti i Dati Personali che richiedono una gestione speciale o categorie particolari di Dati Personali come quelli che riguardano, a titolo esemplificativo e non esaustivo, razza o etnia di un individuo, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, salute, vita sessuale o finanze personali.

8. **Sicurezza dei Dati Personali.**

a. Il Responsabile del trattamento dovrà come minimo implementare le misure tecniche e organizzative specificate nell'Appendice 2 per garantire la sicurezza dei Dati Personali. Questo comprende la protezione dei Dati Personali da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali. Nel valutare l'adeguato livello di sicurezza, le parti terranno debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

b. Il Responsabile del trattamento concederà al suo personale l'accesso ai Dati Personali soggetti a trattamento soltanto nella misura necessaria per l'attuazione, la gestione e il controllo del Contratto per i Servizi. Il Responsabile del trattamento garantisce che le persone autorizzate al trattamento dei Dati Personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

9. **Cooperazione con le Autorità di Controllo.** Il Responsabile del trattamento fornirà al Titolare del trattamento l'assistenza ragionevole nella cooperazione o consultazione preventiva con l'Autorità di Controllo in esecuzione dei suoi compiti relativi alla Sezione 8 del presente DPA nella misura richiesta dal RGPD. Inoltre, in connessione con la richiesta dell'Autorità di Controllo, il Responsabile del trattamento dovrà compiere, a spese del Titolare del trattamento, ogni sforzo ragionevole per ottenere la cooperazione e assistenza dei Sub-responsabili del trattamento in misura ragionevole al fine di fornire l'accesso alle informazioni pertinenti necessarie per adempiere agli obblighi del Titolare del trattamento in base al RGPD.

10. **Violazione dei Dati Personali.**

a. In caso in cui venga a conoscenza di un uso, divulgazione o acquisizione non autorizzati da parte di terzi di Dati Personali che compromettono la sicurezza, la riservatezza o l'integrità dei Dati Personali trattati dal Responsabile del trattamento ("Violazione della Sicurezza"), il Responsabile del trattamento notificherà la violazione al Titolare del trattamento per iscritto entro 48 ore e in seguito fornirà aggiornamenti periodici.

b. Tale notifica dovrà contenere almeno
   (i) una descrizione della natura della Violazione della Sicurezza (compresi, ove possibile, le categorie e il numero approssimativo di Interessati e di registrazioni dei dati in questione);
   (ii) i dettagli di un punto di contatto dove si possono ottenere maggiori informazioni sulla violazione dei Dati Personali; e
   (iii) le probabili conseguenze della Violazione della Sicurezza e le misure adottate o di cui si propone l'adozione per porre rimedio alla Violazione della Sicurezza, comprese le misure per attenuarne i possibili effetti negativi.

c. Qualora e nella misura in cui non sia possibile fornire tutte queste informazioni contemporaneamente, la notifica iniziale conterrà le informazioni disponibili in quel momento e ulteriori informazioni saranno fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

11. **Trasferimento internazionale di dati**

a. **Disposizioni generali**. Il Responsabile del trattamento rispetterà i requisiti delle leggi applicabili sulla protezione dei dati riguardo al trasferimento internazionale di Dati Personali dallo Spazio Economico Europeo.

Esclusivamente ai fini della fornitura di Servizi al Titolare del trattamento in base al Contratto per i Servizi, i Dati Personali possono essere trasferiti e conservati e/o trattati in tutti i paesi in cui operano il Responsabile del trattamento o i suoi Sub-responsabili del trattamento, che possono comprendere paesi terzi. Tutti i trasferimenti di Dati Personali all'esterno dello Spazio Economico Europeo sono disciplinati dalle Clausole Contrattuali Tipo, che le parti stipulano e incorporano nel presente DPA come Allegato 2.

b. **Valutazione del trasferimento di dati.** Molti servizi di sicurezza del Responsabile del trattamento richiedono che una certa quantità di Dati Personali venga trasferita negli Stati Uniti; pertanto, in applicazione della Clausola 14 lettera b) delle Clausole Contrattuali Tipo, il Responsabile del trattamento ha compilato una valutazione del trasferimento di dati ("Data Transfer Assessment" nota anche come "Transfer Impact Assessment"), che si può trovare qui: https://www.proofpoint.com/sites/default/files/misc/pfpt-us-data-transfer-assessment-20201028.pdf.

12. Richieste governative.

a. In applicazione della Clausola 15 delle Clausole Contrattuali Tipo, il Responsabile del trattamento non rivelerà a nessun terzo, ente governativo o ente pubblico nessun Dato del Titolare del trattamento, a eccezione di ciascuno dei casi in cui la rivelazione sia necessaria per rispettare la legge o un ordine valido e vincolante di un ente governativo (come un mandato di comparizione o una decisione giudiziaria). Se un ente governativo invia al Responsabile del trattamento una richiesta di Dati sensibili dei Clienti, il Responsabile del trattamento cercherà di invitare l'ente governativo a chiedere tali dati direttamente al Titolare del trattamento. Come parte di questo impegno, il Responsabile del trattamento potrà fornire all'ente governativo le informazioni di base per contattare il Titolare del trattamento. Se obbligato a rivelare i Dati del Titolare del trattamento a un ente governativo, il Responsabile del trattamento comunicherà questa richiesta al Titolare del trattamento entro un tempo ragionevole, al fine di permettergli di cercare di ottenere un ordine di protezione o un altro rimedio adeguato, a meno che non sia legalmente vietato al Responsabile del trattamento procedere con tale comunicazione. Ai sensi del Foreign Intelligence Surveillance Act (FISA, legge USA sulla sorveglianza e l'intelligence straniera), il Responsabile del trattamento è un "servizio di remote computing" e non un fornitore di servizi di telecomunicazioni; pertanto è improbabile (secondo il parere del Responsabile del trattamento) che sia oggetto di una richiesta governativa in base a tale legge.

b. Al fine di garantire che il Titolare del trattamento sia messo e tenuto al corrente dei rischi connessi al trasferimento di dati verso un paese terzo, il Responsabile del trattamento può di volta in volta, su ragionevole richiesta del Titolare del trattamento e non più di una volta per anno solare, rispondere ad un questionario strutturato del Titolare del trattamento circa le leggi e i regolamenti del paese di destinazione applicabili al Responsabile del trattamento o ai suoi Sub-responsabili del trattamento che consentirebbero l'accesso da parte delle autorità pubbliche ai Dati del Titolare del trattamento oggetto del trasferimento, in particolare per quanto concerne intelligence, applicazione della legge e controllo amministrativo e normativo applicabili ai dati trasferiti. Il Responsabile del trattamento deve essere in grado di fornire al Titolare del trattamento questo tipo di informazioni per quanto di sua conoscenza e dopo aver fatto tutto il possibile per ottenere tali informazioni.

13. Verifica e attività di revisione

a) In conformità dell'articolo 28, paragrafo 3, lettera h), del RGPD, il Responsabile del trattamento, su richiesta scritta ragionevole e soggetta all'esecuzione di un apposito accordo di non divulgazione, metterà a disposizione del Titolare del trattamento le informazioni relative al Trattamento dei Dati Personali del Titolare del trattamento, così come necessario per dimostrare l'osservanza degli obblighi ai sensi del presente DPA da parte del Responsabile del trattamento. Il Responsabile del trattamento permetterà ispezioni in loco richieste dal Titolare del trattamento o da un revisore indipendente in relazione al Trattamento di Dati Personali, al fine di verificare che il Responsabile del trattamento agisca in osservanza del presente DPA, se (a) il Responsabile del trattamento non ha fornito prove scritte sufficienti della sua osservanza delle misure tecniche e organizzative; (b) si è verificata una Violazione della Sicurezza; (c) un'ispezione viene richiesta ufficialmente dall'Autorità di Controllo del Titolare del trattamento; oppure (d) la Legge sulla Protezione dei Dati fornisce al Titolare del trattamento un diritto imperativo d'ispezione sul posto; questo purché il Titolare del trattamento non eserciti questo diritto più di una volta all'anno, a meno che una Legge sulla Protezione dei Dati richieda

obbligatoriamente ispezioni più frequenti. Qualsiasi informazione fornita dal Responsabile del trattamento e/o le revisioni eseguite in conformità di questo articolo sono soggette all'esecuzione di un apposito accordo di non divulgazione. Tali ispezioni sul in loco saranno condotte in modo da non avere un impatto continuativo sulla sicurezza, riservatezza, integrità, disponibilità, continuità e resilienza dei locali ispezionati e da non esporre o compromettere in alcun modo nessuno dei dati riservati ivi trattati.

b) Le spese di ciascuna parte collegate a qualsiasi revisione o ispezione restano a suo carico. Ciò si applica anche ad ogni trasmissione di informazioni o attività di revisione in conformità della Sezione 8.9 lettere da c) a e) delle Clausole Contrattuali Tipo.

14. Cessazione dell'accordo

Il Titolare del trattamento riconosce e accetta che, in caso di sospensione o cessazione di qualsiasi Trattamento dei dati in base al presente DPA o alla Clausola 18 delle Clausole Contrattuali Tipo, la tempistica per la cessazione di tutti i trattamenti di dati e la cancellazione dei dati personali da parte del Responsabile del trattamento sarà disciplinata dal Contratto per i Servizi.

APPENDICE 1 AL DPA – DETTAGLI DEL TRATTAMENTO

La presente Appendice 1 comprende alcuni dettagli del trattamento dei Dati Personali del Cliente come richiesto dall'articolo 28, paragrafo 3, RGPD (o, se applicabili, da disposizioni equivalenti di qualsiasi altra Legge sulla Protezione dei Dati).

Prodotto	Interessati	Categorie dei Dati Personali trattati	Trattamenti	Periodo di conservazione
Archive	Dipendenti, fornitori e clienti	Eventuali Dati Personali inclusi nei contenuti acquisiti (comprendenti e-mail, messaggi istantanei, contenuti dei social media, telemetria e allegati associati ai messaggi)	• Archive è una soluzione di archiviazione basata su cloud progettata per l'esibizione, la conformità normativa e l'accesso ai dati per gli utenti finali del Cliente e fornisce un archivio centrale ricercabile che supporta un'ampia gamma di tipi di contenuto.	Secondo quanto stabilito dal Titolare del trattamento
CAD/CASB	Dipendenti e fornitori	Metadati del proprietario dell'account cloud (indirizzi e-mail, nomi, posizione), metadati dei file e log d'accesso all'account cloud	Cloud Account Defense aiuta il Cliente a rilevare le attività sospette intorno agli account cloud del Cliente e a identificare gli account cloud compromessi. Cloud App Security Broker utilizza criteri per prevenire la perdita dei dati sensibili o riservati del Cliente contenuti negli account cloud del Cliente. CASB IaaS Protection aiuta il Cliente a identificare le proprie risorse IaaS, proteggere i dati sensibili all'interno dello storage IaaS e monitorare e bloccare gli accessi non autorizzati agli account cloud del Cliente	Fino a 180 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Cloudmark Active Filter, Authority, Content Categories, Insight Server e Sender Intelligence; Cloudmark Spam Reporting Service	Dipendenti, fornitori e clienti	Dati telemetrici associati a e-mail e messaggi SMS, MMS e RCS, comprendenti gli indirizzi e-mail e IP e i numeri di telefono	I prodotti Cloudmark sfruttano l'analisi intelligente delle minacce per garantire la sicurezza di posta elettronica e messaggistica mobile contro spam e malware.	30 giorni per i messaggi segnalati dal destinatario come potenzialmente dannosi. 30 giorni per i messaggi segnalati dal destinatario come non dannosi.

Cloudmark Safe Messaging Cloud, Cloudmark Safe Messaging Cloud Hybrid	Dipendenti, fornitori e clienti	Dati telemetrici collegati a e-mail e messaggi SMS, MMS e RCS, comprendenti gli indirizzi e-mail e IP e i numeri di telefono	I prodotti Cloudmark sfruttano l'analisi intelligente delle minacce per garantire la sicurezza di posta elettronica e messaggistica mobile contro spam e malware.	30 giorni per i messaggi segnalati dal destinatario come potenzialmente dannosi. 30 giorni per i messaggi segnalati dal destinatario come non dannosi. Altrimenti, come pattuito dal Titolare del trattamento.
Compliance Gateway	Dipendenti, fornitori e clienti	Eventuali Dati Personali inclusi nei contenuti acquisiti (comprendenti e-mail, messaggi istantanei, contenuti dei social media, telemetria e allegati associati ai messaggi)	Compliance Gateway funge da hub centrale per filtrare e indirizzare il contenuto dei messaggi ai sistemi di archiviazione, controllo e analisi del Cliente.	Fino a 14 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Content Capture	Dipendenti, fornitori e clienti	Eventuali Dati Personali inclusi nei contenuti acquisiti (comprendenti e-mail, messaggi istantanei, contenuti dei social media, telemetria e allegati associati ai messaggi)	Content Capture acquisisce il contenuto dalle piattaforme di messaggistica e archiviazione cloud supportate e fornisce servizi di conformità come e-discovery, archiviazione e controllo.	Fino a 90 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Content Patrol	Dipendenti, fornitori e clienti	Eventuali Dati Personali inclusi nei contenuti acquisiti (comprendenti e-mail, messaggi istantanei, contenuti dei social media, telemetria e allegati associati ai messaggi)	Content Patrol consente ai Clienti di acquisire, monitorare, correggere e generare report di conformità sulle attività dei propri utenti finali sugli account dei social media controllati dal Cliente.	Fino a 90 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Continuity	Dipendenti, fornitori e qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Titolare del trattamento	Eventuali Dati Personali inclusi in una e-mail	Continuity offre l'archiviazione temporanea delle e-mail in entrata e in uscita del Cliente all'interno dell'e-mail on-demand basata sul Web. Continuity serve solo come opzione secondaria di failover di emergenza in caso di guasto del servizio e-mail del Cliente e non come soluzione primaria di archiviazione e-mail o soluzione primaria di failover	I messaggi scadono dopo 30 giorni.
Digital Discover, Digital	Dipendenti, fornitori, clienti o qualsiasi	ID degli account aziendali dell'utente nei	Scansione delle piattaforme dei social media per trovare account attribuiti a un cliente e	Fino a 90 giorni dalla scadenza dell'abbonamento del

Protection e Digital Compliance	altro soggetto che pubblica sugli account dei social media del Cliente	social media, contenuti nei social media e informazioni biografiche optional se contenute nel profilo dell'account aziendale dell'utente	account falsi, fraudolenti e diffamatori collegati al cliente. Analisi dei contenuti statici e interattivi. Interfacce al servizio d'archivio dei social media così come richiesto per la compliance	Titolare del trattamento massimo
Email Data Loss Prevention (DLP)	Dipendenti, fornitori e qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Cliente	Eventuali Dati Personali inclusi in una e-mail	Email DLP utilizza criteri per prevenire la perdita di dati sensibili o riservati del Cliente tramite e-mail.	Fino a 366 giorni dopo la raccolta; ad eccezione di Threat Analytics, i cui dati vengono conservati per un massimo di 18 mesi dopo la raccolta.
Email Fraud Defense	Dipendenti, fornitori, clienti e qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Cliente	Informazioni negli header delle e-mail, comprendenti indirizzi e-mail e IP, nomi del mittente e del destinatario.	EFD elabora l'autenticazione, il reporting e la conformità dei messaggi basati sul dominio I report aggregati (DMARC) e i messaggi forensi DMARC campionano il traffico dei domini dei clienti e valutano l'autenticità dei mittenti in base alle informazioni di autenticazione del mittente e per evidenziare il traffico inviato da fonti non autenticate e non autorizzate.	I dati forensi di Cloudmark vengono conservati per 30 giorni dopo la raccolta. I dati forensi DMARC vengono conservati per 90 giorni dopo la raccolta.
Email Encryption	Dipendenti, fornitori, clienti e qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Cliente	Eventuali Dati Personali inclusi in una e-mail	Email Encryption fornisce una soluzione di crittografia e decrittografia dei messaggi completamente integrata.	Il contenuto dei messaggi crittografati viene conservato secondo quanto stabilito dal Titolare del trattamento (fino a 366 giorni).
Email Protection	Dipendenti, fornitori e qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Titolare del trattamento	Eventuali Dati Personali inclusi in una e-mail	Email Protection include funzioni come il rilevamento dello spam per identificare e classificare i messaggi di spam; funzioni di protezione antivirus per rilevare e filtrare messaggi contenenti virus noti; funzioni antivirus zero-hour per rilevare e filtrare i messaggi contenenti contenuti sospetti; una cartella di quarantena per l'analisi e l'eliminazione di contenuti sospetti	Fino a 18 mesi dopo la raccolta
Endpoint Data Loss Protection	Dipendenti e fornitori	Metadati registrati per gli utenti del Titolare del trattamento	Endpoint Data Loss Prevention distribuisce il software (un agente) su desktop e server di proprietà o controllati dal Cliente su piattaforme supportate. Questi agenti	Fino a 90 giorni dalla scadenza dell'abbonamento del

			acquisiscono i metadati registrati dalle attività degli Utenti con licenza e archiviano questi dati nell'archivio Endpoint Data Loss Prevention di Proofpoint.	Titolare del trattamento massimo
Essentials	Dipendenti, fornitori e clienti	Eventuali Dati Personali inclusi in una e-mail	• Scansione, filtraggio e routing in transito delle e-mail inviate e ricevute da parti esterne al cliente tramite il sistema e-mail aziendale del cliente. • Se viene utilizzata la funzionalità di archiviazione, vedere "Archive" sopra • Se viene utilizzata la sandbox TAP, vedere TAP di seguito	Fino a 18 mesi dopo la raccolta.
Insider Threat Management SaaS	Dipendenti e fornitori: a) Amministratori di ITM SaaS o analisti che usano il portale web. b) Utenti agli endpoint che usano gli endpoint dell'esportatore in cui è stato installato l'agente ITM SaaS.	Indirizzo e-mail, identificatore dell'apparecchio come l'indirizzo IP, informazioni sull'utente come il nome e l'ID dell'utente, informazioni sul sito come URL e nome della pagina, informazioni sull'app come nome dell'app, nome dell'eseguibile e titolo della finestra. Inoltre, con ITM si può catturare il contenuto dello schermo, funzione configurata e controllata dal cliente. La cattura dello schermo potrebbe comprendere qualsiasi dato personale supplementare mostrato sullo schermo dell'utente.	ITM colloca un endpoint agent sui laptop, desktop e server in possesso del titolare del trattamento o sotto il suo controllo. Gli endpoint agent raccolgono i dati telemetrici sulle attività degli utenti degli apparecchi, gli interessati. Se abilitati dal titolare del trattamento, gli endpoint agent possono anche catturare le schermate delle attività degli apparecchi degli utenti. Solo il cliente stabilisce se la cattura dello schermo è abilitata e il periodo di conservazione di tali contenuti. I dati telemetrici e quelli della cattura dello schermo sono conservati nello storage ITM SaaS multi-tenant di Proofpoint.	In conformità con il periodo di conservazione selezionato dal Titolare del trattamento fino a un periodo massimo di 366 giorni.
Intelligent Classification and Protection	Dipendenti, fornitori, clienti e qualunque soggetto che visualizza il documento.	Eventuali Dati Personali inclusi in un documento.	Individua e identifica automaticamente i dati sensibili e business-critical per migliorare le soluzioni di protezione dei dati esistenti come etichettatura, crittografia, controllo degli accessi, prevenzione della perdita di dati, CASB e suggerisce regole e/o criteri di protezione al Cliente	Fino a 90 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Internal Mail Defense (IMD)	Dipendenti e fornitori	Eventuali Dati Personali inclusi in una e-mail	IMD sfrutta le funzionalità di Email Protection e TAP per proteggere le comunicazioni e-mail interne del Cliente da spam e contenuti dannosi.	Fino a 18 mesi dopo la raccolta.
Browser and E-mail Isolation	Dipendenti e fornitori	Indirizzi e-mail, cookie del sito dell'utente, storia	I prodotti Browser and E-mail Isolation stabiliscono un browser Web remoto isolato o un ambiente di posta elettronica Web per	Fino a 90 giorni dalla scadenza dell'abbonamento del

		del browser e sede del centro elaborazione dati del container d'isolamento.	proteggere il Cliente da potenziali minacce quando gli Utenti si connettono a Internet o ad account di posta elettronica basati sul Web su dispositivi di proprietà o controllati dal Cliente. Il Cliente non consentirà agli Utenti di trasmettere (o pubblicare su) Isolation materiale illecito, diffamatorio, minatorio o offensivo.	Titolare del trattamento massimo
NexusAI for Compliance	Dipendenti, fornitori e clienti	Eventuali Dati Personali inclusi nei contenuti acquisiti (comprendenti e-mail, messaggi istantanei, contenuti dei social media, telemetria e allegati associati ai messaggi)	NexusAI for Compliance utilizza l'apprendimento automatico per valutare i messaggi archiviati supportati (come e-mail, social media, piattaforme di collaborazione e messaggi mobili) contrassegnati per la revisione da parte del Cliente dal prodotto Intelligent Supervision di Proofpoint.	Fino a 24 ore dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Nexus People Risk Explorer	Dipendenti e fornitori	Nomi, indirizzi e-mail, eventuali Dati Personali contenuti in Threat Analytics	Proofpoint Nexus People Risk Explorer sfrutta i dati di sicurezza incentrati sulle persone di Targeted Attack Protection, Security Awareness Training, Cloud Account Defense e Cloud Account Security Broker di Proofpoint per fornire informazioni dettagliate sui tipi, sulla gravità e sulla frequenza delle minacce rivolte al Cliente e ai suoi dipendenti.	Fino a 90 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo
Anti-Phishing Suite: include PhishAlarm e PhishAlarmAnalyzer:	Dipendenti e fornitori	Nome Indirizzo e-mail Eventuali Dati Personali inclusi in una e-mail	Routing e scansione di e-mail sospette segnalate dagli utenti finali con il pulsante PhishAlarm. PhishAlarm Analyzer fornisce un'identificazione altamente reattiva degli attacchi di phishing in tempo reale. Le e-mail segnalate tramite PhishAlarm e PhishAlarm Analyzer sono accessibili e classificate e immediatamente disponibili per i team di risposta del Cliente.	Fino a 30 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo; ad eccezione di Threat Analytics, i cui dati vengono conservati fino a 18 mesi dopo la raccolta
Proofpoint Security Awareness Training (PSAT)	Dipendenti e fornitori	Nome, indirizzo e-mail e campi dati supplementari selezionati dal cliente per l'upload a PSAT dalla directory attiva del cliente	I dati personali sono usati per il lancio di corsi di sensibilizzazione dei dipendenti sulla sicurezza informatica, valutazioni della sicurezza dei dipendenti e report	Fino a 90 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo; tuttavia, durante l'abbonamento del Titolare del trattamento, gli amministratori del Titolare del trattamento possono apportare modifiche ed eliminare utenti.
Secure E-Mail Relay (SER)	Dipendenti Fornitori Eventuali destinatari di e-mail inviate in massa tramite il sistema di posta elettronica aziendale del Cliente	Nome Indirizzo e-mail Eventuali Dati Personali inclusi in una e-mail	Secure Email Relay (SER) è una soluzione multi-tenant in hosting che consente al Cliente di controllare le applicazioni che inviano e-mail utilizzando i domini di proprietà o controllati dal Cliente. Aggiunge un livello di sicurezza a ciascuna applicazione e distribuisce l'e-mail a Internet in modo conforme a DMARC dopo l'esecuzione dei controlli di Proofpoint AS/AV. SER può essere utilizzato solo per il recapito di e-mail conformi alle leggi	Fino a 30 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo

			applicabili in materia di messaggi di massa o non richiesti.	
SecureShare	Dipendenti, fornitori, qualsiasi altro soggetto invitato a visualizzare un file condiviso	Nome, indirizzi e-mail	SecureShare è un metodo sicuro per condividere i file e archiviarli temporaneamente.	Fino a 180 giorni dopo la raccolta.
Targeted Attack Protection (TAP)	Dipendenti, fornitori e clienti Qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Cliente	Nome Indirizzo e-mail Eventuali Dati Personali inclusi in una e-mail	TAP identifica e protegge da URL dannosi e allegati dannosi nelle e-mail utilizzando un motore di analisi malware dinamico.	Fino a 18 mesi dopo la raccolta.
Threat Response Auto-pull (TRAP)	Dipendenti, fornitori e clienti Qualsiasi altro soggetto che invia o riceve e-mail tramite il sistema di posta elettronica aziendale del Cliente	Nome Indirizzo e-mail Eventuali Dati Personali inclusi in una e-mail	TRAP è una piattaforma di gestione degli incidenti che include l'automazione per analizzare e rimuovere le e-mail indesiderate.	La conservazione degli incidenti chiusi è stabilita dal Titolare del trattamento. I dati MIME del messaggio completo vengono eliminati ogni 30 giorni per gli incidenti chiusi.
ThreatSimulator	Dipendenti e fornitori	Nome Indirizzo e-mail	I dati personali vengono utilizzati per simulare campagne di phishing. Il Cliente può inviare e-mail di phishing simulate solo a domini di proprietà o controllati dal Cliente.	Su richiesta del cliente ed entro 90 giorni dopo tale richiesta.
Zero Trust Network Access (chiamato in precedenza "Meta")	Dipendenti e fornitori	Nome e indirizzo e-mail dell'utente (e numero di telefono come optional) ed eventi di traffico su Intranet, come eventi di accettazione/rifiuto e richieste DNS (il cliente ha l'opzione di abilitare o disabilitare i log degli eventi di traffico su Internet)	Meta sovrappone un network a fiducia zero al network aziendale del cliente. Gli utenti accedono al network aziendale collegandosi a livello del network Meta mediante una VPN con le loro credenziali di login. Una volta fatto il login nel network Meta, viene assegnata a ciascun utente un'identità unica che si collega al network aziendale sottostante dell'esportatore, mentre l'accesso agli asset all'interno del network aziendale dell'esportatore è basato sull'identità unica dell'utente	Fino a 90 giorni dalla scadenza dell'abbonamento del Titolare del trattamento massimo

1. <u>Sub-responsabili del trattamento</u>

Si può trovare un elenco attuale dei Sub-responsabili del trattamento sul sito https://www.proofpoint.com/us/legal/trust.

APPENDICE 2 AL DPA – SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento mette in atto le misure descritte più avanti per garantire un livello di sicurezza adeguato per la fornitura dei servizi:

A. *Autenticazione dell'utente*

Il management ha stabilito e approvato un programma di sicurezza delle informazioni.
È stata sviluppata una struttura di criteri e standard di sicurezza a sostegno degli obiettivi del programma di sicurezza.
Esistono delle procedure per l'autenticazione e l'autorizzazione degli utenti ai sistemi e per garantirne il rispetto.
Esistono delle procedure per garantire il rispetto delle politiche per chiedere, costituire, aprire, sospendere, cancellare e chiudere gli account degli utenti e i relativi privilegi d'accesso; ad. es. l'accesso al sistema sarà concesso in base al ruolo utilizzando il principio dei privilegi minimi.
È predisposta una procedura per monitorare i tentativi falliti di login. Le violazioni della sicurezza identificate verranno risolte.
L'accesso all'ambiente di produzione del Responsabile del trattamento da parte dei dipendenti del Responsabile del trattamento è concesso in base alle esigenze aziendali. Verrà utilizzata una VPN con autenticazione a due fattori.
Sono predisposti dei controlli per limitare ai soli individui autorizzati l'implementazione di modifiche alla produzione.

Tipo d'accesso

I vari tipi di accesso degli utenti finali del cliente sono documentati nelle Guide dell'Amministratore specifiche del servizio e sono controllati dagli amministratori del cliente mediante il pannello di controllo del servizio, l'interfaccia utente o l'integrazione SAML.

B. *Esecuzione di copie di backup*

La configurazione del cliente e i dati delle relazioni saranno salvati in backup su base regolare e conservati su disco fisso "spinning disk".

Le procedure per il backup e la conservazione di dati e programmi sono state documentate e implementate.

C. *Computer e terminali d'accesso*

I computer usati dai dipendenti del Responsabile del trattamento per accedere alla sua infrastruttura dovranno usare un tunnel VPN sicuro per accedere all'infrastruttura del Responsabile del trattamento. Tutti gli endpoint dei dipendenti dovranno avere software antivirus aggiornati ed esisteranno criteri e procedure per limitare i software che possono essere installati su queste macchine. Tutti i dipendenti del Responsabile del trattamento saranno tenuti ad autenticarsi in un sistema d'autenticazione centralizzata per accedere alle reti produttive e aziendali del Responsabile del trattamento.

Controlli da parte del Responsabile del trattamento dei dati

I nuovi dipendenti saranno tenuti a firmare un accordo di non divulgazione relativo al software proprietario e alla riservatezza sulle informazioni riguardanti i clienti.

Inoltre i nuovi dipendenti riceveranno una copia del Codice di Comportamento per la sicurezza del Responsabile del trattamento, una sintesi del programma di sicurezza delle informazioni del Responsabile del trattamento, e saranno tenuti a dare atto di averla ricevuta.
L'accesso all'ambiente di produzione del Responsabile del trattamento da parte dei dipendenti del Responsabile del trattamento è concesso in base alle esigenze aziendali. Verrà utilizzata una VPN con autenticazione a due fattori.
Gli strumenti di gestione centralizzata della configurazione vengono utilizzati per garantire che gli endpoint dei dipendenti siano configurati in modo appropriato.

D. ***Log d'accesso***

In relazione ai Servizi, ci sono almeno due forme differenti di log d'accesso:

Si farà un log centralizzato di tutti i tentativi d'accesso ai sistemi di computer del Responsabile del trattamento dei dati e l'attività insolita sarà segnalata automaticamente al gruppo Global Information Security del Responsabile del trattamento. Inoltre, il Responsabile del trattamento impone i criteri di blocco degli account e i requisiti delle password. I log degli accessi dei clienti ai Servizi vengono generati e conservati secondo quanto applicabile per ciascun Servizio.

Esistono delle procedure per l'autenticazione e l'autorizzazione degli utenti ai sistemi e per garantirne il rispetto.
Esiste una procedura di controllo, che verrà seguita per esaminare periodicamente i privilegi d'accesso e confermare che restino autorizzati e adeguati.
È predisposta una procedura per monitorare i tentativi falliti di login. Le violazioni della sicurezza identificate verranno investigate e risolte.
I dati degli eventi nelle applicazioni saranno conservati per fornire informazioni cronologiche e log al fine di permettere l'esame, la ricostruzione dei sistemi e degli eventi nelle applicazioni e nel trattamento dei dati.

E. ***Sistemi di telecomunicazione***

Tutti i centri di produzione del Responsabile del trattamento hanno flussi Internet ridondanti da fornitori con diverse ampiezze di banda.

F. ***Istruzione del personale***

Tutto il personale del Responsabile del trattamento è tenuto a completare un programma annuale di formazione online sulla sicurezza e sulla sensibilizzazione. Inoltre, il personale può ricevere una formazione continua specifica per il proprio ruolo. Questo addestramento potrà essere dato da Proofpoint o altre organizzazioni terze.

Il Responsabile del trattamento ha uno schema organizzativo che separa le mansioni incompatibili e gli obblighi del personale pertinente.
Sono state create mansioni e responsabilità del management diverse per separare le mansioni relative alle operazioni informatiche, allo sviluppo del sistema, alla manutenzione e alle funzioni generali dell'azienda del Responsabile del trattamento.
Le mansioni e le responsabilità personali sono chiaramente definite.

G. ***Uso dei computer***

L'accesso remoto alle reti di produzione del Responsabile del trattamento è limitato ai sistemi con software di sicurezza gestito e approvato dal Responsabile del trattamento. Tutti i sistemi del Responsabile del trattamento forniti al personale sono gestiti da un sistema di configurazione centralizzato. Tutti i dipendenti del Responsabile del trattamento saranno resi consapevoli delle politiche del Responsabile del trattamento sull'uso accettabile dei suoi computer, sull'accesso a Internet e sulle comunicazioni e-mail. I dipendenti del Responsabile del trattamento devono riconoscere queste politiche e accettare di rispettarle.

I nuovi dipendenti saranno tenuti a firmare un accordo di non divulgazione relativo al software proprietario e alla riservatezza sulle informazioni riguardanti i clienti.
I nuovi dipendenti esamineranno e accetteranno il Codice di Comportamento per la sicurezza del Responsabile del trattamento.

H. ***Stampa dei dati***

I Dati dei Clienti saranno trattati in memoria e non saranno disponibili per la stampa. Inoltre non è disponibile nessuna stampante nell'ambiente di produzione del Responsabile del trattamento e tutti i servizi stampa sono disabilitati di default in tutti i server produttivi.

K. ***Controllo dell'accesso fisico***

Controlli da parte del Responsabile del trattamento dei dati

Per i prodotti ospitati dai co-location provider del Responsabile del trattamento, il Responsabile del trattamento mantiene il controllo dell'accesso fisico all'Infrastruttura del Responsabile del trattamento. Per i prodotti ospitati dai fornitori dell'hosting AWS, Azure o Google Cloud, l'accesso fisico è controllato dall'hosting provider.

L. **Misure di sicurezza fisica per i centri elaborazione dati**

I controlli di sicurezza fisica delle strutture di co-location sono allineati agli standard dei centri di elaborazione dati di Livello III, tra cui sicurezza in loco 24x7, punti di accesso con personale, meccanismi anti-piggybacking, autenticazione a due fattori e telecamere a circuito chiuso monitorate. Le strutture utilizzate da AWS, Azure o Google Cloud sono allineate agli standard dei centri di elaborazione dati di Livello III.

M. ***Controllo dell'accesso ai sistemi IT***

Controlli da parte del Responsabile del trattamento dei dati

Il Responsabile del trattamento dei dati controlla l'accesso ai sistemi che forniscono i Servizi nei modi seguenti:

1. Tutti i dipendenti e fornitori del Responsabile del trattamento dei dati saranno muniti di user ID unici. La condivisione dell'account non è consentita.
2. I requisiti della password saranno definiti e applicati da un tool di sincronizzazione password. I requisiti comprendono:
    a. Minimo 12 caratteri
    b. Non deve apparire negli elenchi pubblici di password violate
    c. Diversa dalle precedenti 23
    d. Richiesta di cambio ogni 180 giorni
    e. Account bloccato dopo cinque (5) tentativi di login falliti
3. L'accesso logico sarà concesso in base alla mansione.

4. Il logging dell'audit sarà in essere sulla VPN verso l'ambiente di produzione del Responsabile del trattamento dei dati.
5. I log dell'audit saranno monitorati in tempo quasi reale da un log tool di aggregazione e allarme. Gli avvisi sono configurati per essere inviati al gruppo Global Information Security del Responsabile del trattamento dei dati.

N. ***Controllo dell'accesso ai dati***

Non è consentito che i Dati del Cliente stiano nell'ambiente aziendale del Responsabile del trattamento. L'accesso ai sistemi che ospitano i servizi è controllato nei modi seguenti:

1. L'accesso sarà basato sulla mansione presso il Responsabile del trattamento.
2. L'accesso privilegiato all'Ambiente di Produzione del Responsabile del trattamento sarà consentito solo al personale autorizzato del Responsabile del trattamento.

O. Il ***logging dell'audit*** sarà in essere sulla VPN e sui sistemi nell'Ambiente di Produzione del Responsabile del trattamento.

P. ***Implementazione del controllo degli accessi con privilegio minimo***

L'accesso all'Ambiente di Produzione del Responsabile del trattamento sarà concesso in base alla mansione.

Q. ***Sicurezza durante il trasferimento e trattamento***

Il Responsabile del trattamento non permetterà che i Dati dei Clienti restino nell'ambiente aziendale del Responsabile trattamento, dove si trovano i suoi dipendenti e fornitori. L'Ambiente di Produzione del Responsabile del trattamento sarà separato dal suo ambiente aziendale sul piano logico e fisico:

1. L'accesso all'Ambiente di Produzione del Responsabile del trattamento avverrà tramite una VPN con autenticazione a due fattori utilizzando dispositivi approvati dal Responsabile del trattamento e sarà fornito solo ai dipendenti e ai fornitori del Responsabile del trattamento che ne hanno bisogno per la loro mansione.
2. Firewall in linea con gli standard di settore sono installati e configurati per consentire il traffico solo dalle porte necessarie per il funzionamento dei Servizi, mentre ogni altro traffico è negato di default.
3. Tutti gli accessi degli amministratori alle interfacce web ospitate dei Servizi saranno criptati con HTTPS/TLS.

Controlli dell'accesso al sistema

1. LDAP viene utilizzato per autenticare il personale del Responsabile del trattamento negli ambienti di produzione.
2. L'accesso privilegiato sarà concesso solo al personale autorizzato del Responsabile del trattamento.

Sicurezza dell'endpoint

1. Gli endpoint utilizzati per accedere all'ambiente di produzione del Responsabile del trattamento dei dati sono gestiti a livello centralizzato, dispongono delle opportune patch di sicurezza installate, eseguono software di sicurezza standardizzato e vengono regolarmente analizzati per rilevare eventuali vulnerabilità.

Sicurezza del server

1. Le opportune patch di sicurezza vengono applicate in base alla criticità.
2. I servizi non necessari sono disabilitati.
3. Le password di default vengono cambiate.

R. ***Sicurezza durante la trasmissione di dati su reti pubbliche***

1. Tutti gli accessi degli amministratori del Responsabile del trattamento ai Servizi saranno criptati con HTTPS/TLS.

S. ***Controlli in fase operativa e d'implementazione***

La funzionalità fornita dai servizi è compiuta automaticamente e non richiede un intervento umano, a eccezione degli scopi d'analisi e per localizzare e risolvere problemi nei servizi. I servizi sono progettati per funzionare nel modo descritto nel Contratto per i servizi.

T. ***Tracciabilità di qualsiasi accesso, modifica e cancellazione***

L'accesso ai sistemi usati dai servizi è controllato nei modi seguenti:

1. L'accesso sarà concesso in base alla mansione presso il Responsabile del trattamento.
2. L'accesso privilegiato all'Ambiente di Produzione del Responsabile del trattamento sarà consentito solo al personale autorizzato.
3. Il logging dell'audit sarà in essere sulla VPN e sui sistemi nell'Ambiente di Produzione del Responsabile del trattamento.
4. I log di audit generati dal servizio acquisiscono l'accesso ai Servizi da parte del personale del Titolare del trattamento.

U. ***Garanzia di un trattamento conforme dei dati***

A eccezione degli scopi d'analisi e per localizzare e risolvere problemi nei Servizi, il personale del Responsabile del trattamento non tratterà manualmente i Dati dei Clienti. Tutti i dati del cliente saranno trattati automaticamente dai servizi, come descritto nella documentazione dei Servizi.

V. ***Garanzia della disponibilità***

Ciò si ottiene nel modo seguente:

1. L'infrastruttura è configurata in ogni struttura di produzione in modalità alta disponibilità, comprendente due linee d'alimentazione e un minimo di due connessioni diverse alla rete.
2. Le strutture di co-location sono allineate agli standard dei centri di elaborazione dati di Livello III, inclusi alimentazione ridondante e controlli ambientali ridondanti.
3. Le strutture di co-location hanno generatori in loco con on riserve di energia per un minimo di due (2) giorni.
4. Un Business Continuity Action Plan per la protezione del Responsabile del trattamento dei dati e il ripristino dei processi aziendali del Responsabile del trattamento dei dati sarà documentato e collaudato una volta all'anno.
5. Un'infrastruttura di monitoraggio ripartita controlla la disponibilità e le prestazioni.
6. .

W. ***Separazione dei dati***

I servizi mantengono la separazione dei Dati del Cliente. Ciò si ottiene nel modo seguente:

1. La separazione logica viene mantenuta dal servizio utilizzando alcune o tutte le seguenti misure:
   a. ID del cliente uniche per ciascun cliente, che sono usate per etichettare i Dati del Cliente all'interno del servizio;
   b. IP univoci; o
   c. chiavi di crittografia univoche.

ALLEGATO 2

Clausole Contrattuali Tipo per il trasferimento di dati personali verso paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

CLAUSOLE CONTRATTUALI TIPO

da titolare del trattamento a responsabile del trattamento

SEZIONE I

Clausola 1

Scopo e ambito di applicazione

(a) Scopo delle presenti Clausole contrattuali tipo è garantire il rispetto dei requisiti del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati) in caso di trasferimento di dati personali verso un paese terzo.

(b) Le Parti:

(i) la o le persone fisiche o giuridiche, la o le autorità pubbliche, lo o gli organismi o altri organi (di seguito la o le "entità") che trasferiscono i dati personali, elencate nell'Allegato I.A. (di seguito "esportatore"), e

(ii) la o le entità di un paese terzo che ricevono i dati personali dall'esportatore, direttamente o indirettamente tramite un'altra entità anch'essa Parte delle presenti Clausole, elencate nell'Allegato I.A. (di seguito "importatore") hanno accettato le presenti clausole contrattuali tipo (di seguito "Clausole").

(c) Le presenti clausole si applicano al trasferimento di dati personali specificato all'Allegato I.B.

(d) L'Appendice delle presenti Clausole contenente gli Allegati ivi menzionati costituisce parte integrante delle presenti Clausole.

Clausola 2

Effetto e invariabilità delle Clausole

(a) Le presenti Clausole stabiliscono garanzie adeguate, compresi diritti azionabili degli interessati e mezzi di ricorso effettivi, in conformità dell'articolo 46, paragrafo 1, e dell'articolo 46, paragrafo 2, lettera c), del Regolamento (UE) 2016/679 e, per quanto riguarda i trasferimenti di dati da titolari del trattamento a responsabili del trattamento e/o da responsabili del trattamento a responsabili del trattamento, Clausole contrattuali tipo in conformità dell'articolo 28, paragrafo 7, del Regolamento (UE) 2016/679, purché non siano modificate, tranne per selezionare il modulo o i moduli appropriati o per aggiungere o aggiornare informazioni nell'Appendice. Ciò non impedisce alle Parti di includere le Clausole contrattuali tipo stabilite nelle presenti Clausole in un contratto più ampio e di aggiungere altre Clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti Clausole o ledano i diritti o le libertà fondamentali degli interessati.

(b) Le presenti Clausole non pregiudicano gli obblighi cui è soggetto l'esportatore a norma del Regolamento (UE) 2016/679.

Clausola 3

Terzi beneficiari

(a) Gli interessati possono invocare e far valere le presenti Clausole, in qualità di terzi beneficiari, nei confronti dell'esportatore e/o dell'importatore, con le seguenti eccezioni:

(i) Clausola 1, Clausola 2, Clausola 3, Clausola 6, Clausola 7;

(ii) Clausola 8 – Clausola 8.1, lettera b), Clausola 8.9, lettere a), c), d) ed e);

(iii) Clausola 9 – Clausola 9, lettere a), c), d) ed e);

(iv) Clausola 12 – Clausola 12, lettere a), d) e f);

(v) Clausola 13;
(vi) Clausola 15.1, lettere c), d) ed e);
(vii) Clausola 16, lettera e);
(viii) Clausola 18 – Clausola 18, lettere a) e b)
(b) La lettera a) lascia impregiudicati i diritti degli interessati a norma del Regolamento (UE) 2016/679.

Clausola 4

Interpretazione

(a) Quando le presenti Clausole utilizzano termini che sono definiti nel Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui a detto Regolamento.

(b) Le presenti Clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679.

(c) Le presenti Clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679.

Clausola 5

Gerarchia

In caso di contraddizione tra le presenti Clausole e le disposizioni di accordi correlati, vigenti tra le Parti al momento dell'accettazione delle presenti Clausole, o conclusi successivamente, prevalgono le presenti Clausole.

Clausola 6

Descrizione dei trasferimenti

I dettagli dei trasferimenti, in particolare le categorie di dati personali trasferiti e le finalità per le quali i dati sono trasferiti, sono specificati nell'Allegato I.B.

Clausola 7 – Facoltativa

Clausola di adesione successiva – non applicabile

SEZIONE II – OBBLIGHI DELLE PARTI

Clausola 8

Garanzie in materia di protezione dei dati

L'esportatore garantisce di aver fatto quanto ragionevolmente possibile per stabilire che l'importatore, grazie all'attuazione di misure tecniche e organizzative adeguate, è in grado di adempiere agli obblighi che gli incombono a norma delle presenti Clausole.

Trasferimento da titolare del trattamento a responsabile del trattamento

8.1 **Istruzioni**

(a) L'importatore tratta i dati personali soltanto su istruzione documentata dell'esportatore. L'esportatore può impartire tali istruzioni per tutta la durata del contratto.

(b) L'importatore informa immediatamente l'esportatore qualora non sia in grado di seguire tali istruzioni.

8.2 **Limitazione delle finalità**

L'importatore tratta i dati personali soltanto per le finalità specifiche del trasferimento di cui all'Allegato I. B, salvo ulteriori istruzioni dell'esportatore.

8.3 **Trasparenza**

Su richiesta, l'esportatore mette gratuitamente a disposizione dell'interessato una copia delle presenti Clausole, compresa l'Appendice compilata dalle Parti. Nella misura necessaria a proteggere segreti aziendali o altre

informazioni riservate, comprese le misure descritte nell'Allegato II e i dati personali, l'esportatore può espungere informazioni dall'Appendice delle presenti Clausole prima di trasmetterne una copia, fornendo tuttavia una sintesi significativa qualora l'interessato non sia altrimenti in grado di comprenderne il contenuto o di esercitare i propri diritti. Su richiesta, le Parti comunicano all'interessato le ragioni delle espunzioni, per quanto possibile senza rivelare le informazioni espunte. Questa Clausola lascia impregiudicati gli obblighi incombenti all'esportatore a norma degli articoli 13 e 14 del Regolamento (UE) 2016/679.

8.4 **Esattezza**

Se l'importatore viene a conoscenza del fatto che i dati personali che ha ricevuto sono inesatti o obsoleti, ne informa senza ingiustificato ritardo l'esportatore. In tal caso, l'importatore coopera con l'esportatore per cancellarli o rettificarli.

8.5 **Durata del trattamento e cancellazione o restituzione dei dati**

L'importatore tratta i dati personali soltanto per la durata specificata nell'Allegato I.B. Al termine della prestazione dei servizi di trattamento l'importatore, a scelta dell'esportatore, cancella tutti i dati personali trattati per conto dell'esportatore e certifica a quest'ultimo di averlo fatto, oppure restituisce all'esportatore tutti i dati personali trattati per suo conto e cancella le copie esistenti. Finché i dati non sono cancellati o restituiti, l'importatore continua ad assicurare il rispetto delle presenti Clausole. Qualora la legislazione locale applicabile all'importatore vieti la restituzione o la cancellazione dei dati personali, l'importatore garantisce che continuerà ad assicurare il rispetto delle presenti Clausole e che tratterà i dati solo nella misura e per il tempo richiesto dalla legislazione locale. Ciò lascia impregiudicata la Clausola 14, in particolare il requisito per l'importatore, a norma della Clausola 14, lettera e), di informare l'esportatore per tutta la durata del contratto se ha motivo di ritenere di essere, o essere diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla Clausola 14, lettera a).

8.6 **Sicurezza del trattamento**

(a) L'importatore e, durante la trasmissione, anche l'esportatore mettono in atto misure tecniche e organizzative adeguate per garantire la sicurezza dei dati, compresa la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a tali dati (di seguito "violazione dei dati personali"). Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi derivanti dal trattamento per gli interessati. Le Parti prendono in considerazione in particolare la possibilità di ricorrere alla cifratura o alla pseudonimizzazione, anche durante la trasmissione, qualora la finalità del trattamento possa essere conseguita in tal modo. In caso di pseudonimizzazione, le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico restano, ove possibile, sotto il controllo esclusivo dell'esportatore. Nell'adempiere all'obbligo ai sensi del presente paragrafo, l'importatore mette in atto almeno le misure tecniche e organizzative specificate nell'Allegato II. L'importatore effettua controlli regolari per garantire che tali misure continuino a offrire un adeguato livello di sicurezza.

(b) L'importatore concede l'accesso ai dati personali ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

(c) In caso di violazione dei dati personali trattati dall'importatore a norma delle presenti Clausole, l'importatore adotta misure adeguate per porre rimedio alla violazione, anche per attenuarne gli effetti negativi. L'importatore informa l'esportatore senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Tale notifica contiene i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni, una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali in questione), le sue probabili conseguenze e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, se del caso anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni

contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

(d) L'importatore coopera con l'esportatore e lo assiste per consentirgli di adempiere agli obblighi che gli incombono a norma del Regolamento (UE) 2016/679, in particolare di dare notifica all'autorità di controllo competente e agli interessati in questione, tenuto conto della natura del trattamento e delle informazioni di cui dispone l'importatore.

8.7 **Dati sensibili**

Qualora il trasferimento riguardi dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati (in prosieguo "dati sensibili"), l'importatore applica le limitazioni specifiche e/o le garanzie supplementari di cui all'Allegato I.B.

8.8 **Trasferimenti successivi**

L'importatore comunica i dati personali a terzi soltanto su istruzione documentata dell'esportatore. L'importatore non comunica i dati personali a terzi situati al di fuori dell'Unione europea (4) (nel suo stesso paese o in un altro paese terzo - di seguito: "trasferimento successivo"), a meno che il terzo sia o accetti di essere vincolato dalle presenti Clausole, secondo il modulo appropriato, o se:

(i) il trasferimento successivo è diretto verso un paese che beneficia di una decisione di adeguatezza in conformità dell'articolo 45 del Regolamento (UE) 2016/679 che copre il trasferimento successivo;

(ii) il terzo fornisce in altro modo garanzie adeguate in conformità dell'articolo 46 o 47 del Regolamento (UE) 2016/679 in relazione al trattamento in questione;

(iii) il trasferimento successivo è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari; o

(iv) il trasferimento successivo è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

Qualunque trasferimento successivo è soggetto al rispetto da parte dell'importatore di tutte le altre garanzie previste dalle presenti Clausole, in particolare la limitazione delle finalità.

8.9 **Documentazione e rispetto**

(a) L'importatore risponde prontamente e adeguatamente alle richieste di informazioni dell'esportatore relative al trattamento a norma delle presenti Clausole.

(b) Le Parti devono essere in grado di dimostrare il rispetto delle presenti Clausole. In particolare, l'importatore conserva documentazione adeguata delle attività di trattamento effettuate per conto dell'esportatore.

(c) L'importatore mette a disposizione dell'esportatore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alle presenti Clausole e, su richiesta dell'esportatore, consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti Clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, l'esportatore può tenere conto delle pertinenti certificazioni in possesso dell'importatore.

(d) L'esportatore può scegliere di condurre l'attività di revisione autonomamente o di incaricare un revisore indipendente. Le attività di revisione possono comprendere ispezioni nei locali o nelle strutture fisiche dell'importatore e, se del caso, sono effettuate con un preavviso ragionevole.

(e) Le Parti mettono a disposizione dell'autorità di controllo competente, su richiesta, le informazioni di cui alle lettere b) e c), compresi i risultati di eventuali attività di revisione.

(4) L'accordo sullo Spazio economico europeo (accordo SEE) prevede l'estensione del mercato interno dell'Unione europea ai tre Stati del SEE: Islanda, Liechtenstein e Norvegia. La legislazione dell'Unione sulla protezione dei dati, Regolamento (UE) 2016/679 compreso, è materia contemplata dall'accordo SEE, nel cui Allegato XI è stata integrata. Pertanto, qualunque comunicazione da parte dell'importatore a terzi situati nel SEE non può essere considerata un trasferimento successivo ai fini delle presenti Clausole.

Clausola 9

Ricorso a sub-responsabili del trattamento

(a) AUTORIZZAZIONE SCRITTA GENERALE L'importatore ha l'autorizzazione generale dell'esportatore per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. L'importatore informa specificamente per iscritto l'esportatore di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 30 giorni, dando così all'esportatore tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento. L'importatore fornisce all'esportatore le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

(b) Qualora l'importatore ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto dell'esportatore), stipula un contratto scritto che prevede, nella sostanza, gli stessi obblighi in materia di protezione dei dati che vincolano l'importatore a norma delle presenti Clausole, anche in termini di diritti del terzo beneficiario per gli interessati. (8) Le Parti convengono che, conformandosi alla presente Clausola, l'importatore adempie agli obblighi di cui alla Clausola 8.8. L'importatore garantisce che il sub-responsabile del trattamento rispetta gli obblighi cui l'importatore è soggetto in conformità delle presenti Clausole.

(c) Su richiesta dell'esportatore, l'importatore gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, l'importatore può espungere informazioni dal contratto prima di trasmetterne una copia.

(d) L'importatore rimane pienamente responsabile nei confronti dell'esportatore dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con l'importatore. L'importatore notifica all'esportatore qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi derivanti da tale contratto.

(e) L'importatore concorda con il sub-responsabile del trattamento una Clausola del terzo beneficiario secondo la quale, qualora l'importatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'esportatore ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

(8) Questo requisito può essere soddisfatto dal sub-responsabile del trattamento che aderisce alle presenti Clausole secondo il modulo appropriato, conformemente alla Clausola 7.

Clausola 10

Diritti dell'interessato

(a) L'importatore notifica prontamente all'esportatore qualunque richiesta ricevuta da un interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dall'esportatore.

(b) L'importatore assiste l'esportatore nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti in virtù del Regolamento (UE) 2016/679. A tale riguardo, le Parti stabiliscono nell'Allegato II le misure tecniche e organizzative adeguate, tenuto conto della natura del trattamento, mediante le quali è fornita l'assistenza, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

(c) Nell'adempiere agli obblighi di cui alle lettere a) e b), l'importatore si attiene alle istruzioni dell'esportatore.

Clausola 11

Ricorso

(a) L'importatore informa gli interessati, in forma trasparente e facilmente accessibile, mediante avviso individuale o sul suo sito web, di un punto di contatto autorizzato a trattare i reclami. Tratta prontamente qualunque reclamo ricevuto da un interessato.

(b) In caso di controversia tra un interessato e una delle Parti sul rispetto delle presenti Clausole, la Parte in questione fa tutto il possibile per risolvere la questione in via amichevole in modo tempestivo. Le Parti si tengono reciprocamente informate di tali controversie e, se del caso, cooperano per risolverle.

(c) Qualora l'interessato invochi un diritto del terzo beneficiario in conformità della Clausola 3, l'importatore accetta la decisione dell'interessato di:

(i) proporre reclamo all'autorità di controllo dello Stato membro di residenza abituale o del luogo di lavoro o all'autorità di controllo competente in conformità della Clausola 13;
(ii) deferire la controversia agli organi giurisdizionali competenti ai sensi della Clausola 18.
(d) Le Parti accettano che l'interessato possa essere rappresentato da un organismo, un'organizzazione o un'associazione senza scopo di lucro alle condizioni di cui all'articolo 80, paragrafo 1, del Regolamento (UE) 2016/679.

(e) L'importatore si attiene a qualunque decisione vincolante a norma della legislazione applicabile dell'UE o degli Stati membri.

(f) L'importatore dichiara che la scelta compiuta dall'interessato non pregiudica i diritti sostanziali o procedurali spettanti allo stesso relativamente ai rimedi giuridici previsti dalla legislazione applicabile.

Clausola 12

Responsabilità

(a) Ciascuna Parte è responsabile nei confronti delle altre Parti per i danni che essa ha causato loro violando le presenti Clausole.

(b) L'importatore è responsabile nei confronti dell'interessato per i danni materiali o immateriali che egli stesso o il suo sub-responsabile del trattamento ha causato all'interessato violando i diritti del terzo beneficiario riconosciuti dalle presenti Clausole, e l'interessato ha il diritto di ottenere il risarcimento.

(c) Nonostante la lettera b), l'esportatore è responsabile nei confronti dell'interessato per i danni materiali o immateriali che egli stesso o l'importatore (o il suo sub-responsabile del trattamento) ha causato all'interessato violando i diritti del terzo beneficiario riconosciuti dalle presenti Clausole, e l'interessato ha il diritto di ottenere il risarcimento. Ciò lascia impregiudicata la responsabilità dell'esportatore e, qualora l'esportatore sia un responsabile del trattamento che agisce per conto di un titolare del trattamento, la responsabilità del titolare del trattamento a norma del Regolamento (UE) 2016/679 o del Regolamento (UE) 2018/1725, a seconda del caso.

(d) Le Parti convengono che, se l'esportatore è ritenuto responsabile a norma della lettera c) per i danni causati dall'importatore (o dal suo sub-responsabile del trattamento), egli ha il diritto di reclamare dall'importatore la parte del risarcimento corrispondente alla sua parte di responsabilità per il danno.

(e) Qualora più di una Parte sia responsabile per un danno causato all'interessato a seguito di una violazione delle presenti Clausole, tutte le Parti responsabili sono responsabili in solido e l'interessato ha il diritto di agire in giudizio contro una qualunque di loro.

(f) Le Parti convengono che, se una delle Parti è ritenuta responsabile a norma della lettera e), essa ha il diritto di reclamare dalle altre Parti la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

(g) L'importatore non può invocare il comportamento di un sub-responsabile del trattamento per sottrarsi alla propria responsabilità.

Clausola 13

Controllo

(a) [Se l'esportatore ha sede in uno Stato membro dell'UE:] L'autorità di controllo responsabile di garantire il rispetto da parte dell'esportatore del Regolamento (UE) 2016/679 per quanto riguarda il trasferimento dei dati come indicato nell'Allegato I.C, agisce in qualità di autorità di controllo competente.
[Se l'esportatore non ha sede in uno Stato membro dell'UE, ma rientra nell'ambito di applicazione territoriale del Regolamento (UE) 2016/679 ai sensi del suo articolo 3(2) e ha nominato un rappresentante ai sensi dell'articolo 27(1) del Regolamento (UE) 2016/679:] L'autorità di controllo dello Stato membro in cui ha sede il rappresentante ai sensi dell'articolo 27(1) del Regolamento (UE) 2016/679 come indicato nell'allegato I.C, agisce come autorità di controllo competente. [Laddove l'esportatore non abbia sede in uno Stato membro dell'UE, ma rientri nell'ambito di applicazione territoriale del Regolamento (UE) 2016/679 ai sensi del suo articolo 3(2) senza tuttavia dover nominare un rappresentante ai sensi dell'articolo 27(2) del Regolamento (UE) 2016/679]: L'autorità di controllo di uno degli Stati membri in cui si trovano gli interessati i cui dati personali sono trasferiti a norma delle presenti Clausole in relazione all'offerta di beni o alla prestazione di servizi, o il cui comportamento è oggetto di monitoraggio, quale indicata all'Allegato I.C, agisce in qualità di autorità di controllo competente.

(b) L'importatore accetta di sottoporsi alla giurisdizione dell'autorità di controllo competente e di cooperare con la stessa nell'ambito di qualunque procedura volta a garantire il rispetto delle presenti Clausole. In particolare, l'importatore accetta di rispondere alle richieste di informazioni, sottoporsi ad attività di revisione e rispettare le misure adottate dall'autorità di controllo, comprese le misure di riparazione e risarcimento. Fornisce all'autorità di controllo conferma scritta che sono state adottate le misure necessarie.

SEZIONE III – LEGISLAZIONE E OBBLIGHI LOCALI IN CASO DI ACCESSO DA PARTE DI AUTORITÀ PUBBLICHE

Clausola 14

Legislazione e prassi locali che incidono sul rispetto delle Clausole

(a) Le Parti garantiscono di non avere motivo di ritenere che la legislazione e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore, compresi eventuali requisiti di comunicazione dei dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impediscono all'importatore di rispettare gli obblighi che gli incombono a norma delle presenti Clausole. Ciò si basa sul presupposto che la legislazione e le prassi che rispettano l'essenza dei diritti e delle libertà fondamentali e non vanno oltre quanto necessario e proporzionato in una società democratica per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1, del Regolamento (UE) 2016/679 non sono in contraddizione con le presenti Clausole.

(b) Le Parti dichiarano che, nel fornire la garanzia di cui alla lettera a), hanno tenuto debitamente conto dei seguenti elementi:
   (i) le circostanze specifiche del trasferimento, tra cui la lunghezza della catena di trattamento, il numero di attori coinvolti e i canali di trasmissione utilizzati; i trasferimenti successivi previsti; il tipo di destinatario; la finalità del trattamento; le categorie e il formato dei dati personali trasferiti; il settore economico in cui ha luogo il trasferimento; il luogo di conservazione dei dati trasferiti;
   (ii) la legislazione e le prassi del paese terzo di destinazione – comprese quelle che impongono la comunicazione di dati alle autorità pubbliche o che le autorizzano ad accedere ai dati – pertinenti alla luce delle circostanze specifiche del trasferimento, nonché le limitazioni e le garanzie applicabili (12);
   (iii) qualunque garanzia contrattuale, tecnica o organizzativa pertinente predisposta per integrare le garanzie di cui alle presenti Clausole, comprese le misure applicate durante la trasmissione e il trattamento dei dati personali nel paese di destinazione.

(c) L'importatore garantisce che, nell'effettuare la valutazione di cui alla lettera b), ha fatto tutto il possibile per fornire all'esportatore le informazioni pertinenti e dichiara che continuerà a cooperare con l'esportatore per garantire il rispetto delle presenti Clausole.

(d) Le Parti accettano di documentare la valutazione di cui alla lettera b) e di metterla a disposizione dell'autorità di controllo competente su richiesta.

(e) L'importatore accetta di informare prontamente l'esportatore se, dopo aver accettato le presenti Clausole e per la durata del contratto, ha motivo di ritenere di essere, o essere diventato, soggetto a una legislazione o prassi non conformi ai requisiti di cui alla lettera a), anche a seguito di una modifica della legislazione del paese terzo o di una misura (ad esempio una richiesta di comunicazione) che indichi un'applicazione pratica di tale legislazione che non è conforme ai requisiti di cui alla lettera a).

(f) A seguito di una notifica in conformità della lettera e), o se ha altrimenti motivo di ritenere che l'importatore non sia più in grado di adempiere agli obblighi che gli incombono a norma delle presenti Clausole, l'esportatore individua prontamente le misure adeguate (ad esempio, misure tecniche o organizzative per garantire la sicurezza e la riservatezza) che egli stesso e/o l'importatore devono adottare per far fronte alla situazione. L'esportatore sospende il trasferimento dei dati se ritiene che non possano essere assicurate garanzie adeguate per tale trasferimento, o su istruzione dell'autorità di controllo competente. In tal caso l'esportatore ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti Clausole. Se le Parti del contratto sono più di due, l'esportatore può esercitare il diritto di risoluzione soltanto nei confronti della Parte interessata, salvo diversamente concordato dalle Parti. In caso di risoluzione del contratto in conformità della presente Clausola, si applica la clausola 16, lettere d) ed e).

---

(12) Per quanto riguarda l'impatto della legislazione e delle prassi sul rispetto delle presenti Clausole, possono essere presi in considerazione diversi elementi nell'ambito di una valutazione globale. Tali elementi possono includere un'esperienza pratica pertinente e documentata in casi precedenti di richieste di comunicazione da parte di autorità pubbliche, o l'assenza di tali richieste, per un periodo di tempo sufficientemente rappresentativo. Si tratta in particolare di registri interni o altra documentazione, elaborati su base continuativa conformemente alla dovuta diligenza e certificati a livello di alta dirigenza, sempre che tali informazioni possano essere lecitamente condivise con terzi. Qualora per concludere che all'importatore non sarà impedito di rispettare le presenti Clausole si faccia affidamento su questa esperienza pratica, essa deve essere sostenuta da altri elementi pertinenti e oggettivi, e spetta alle Parti valutare attentamente se tali elementi, congiuntamente, abbiano un peso sufficiente in termini di affidabilità e rappresentatività per sostenere tale conclusione. In particolare, le Parti devono considerare se la loro esperienza pratica è corroborata e non contraddetta da informazioni disponibili al pubblico, o altrimenti accessibili, e affidabili sull'esistenza o sull'assenza di richieste nello stesso settore e/o sull'applicazione pratica della legislazione, come la giurisprudenza e le relazioni di organi di vigilanza indipendenti.

Clausola 15

Obblighi dell'importatore in caso di accesso da parte di autorità pubbliche

15.1 **Notifica**

(a) L'importatore accetta di informare prontamente l'esportatore e, ove possibile, l'interessato (se necessario con l'aiuto dell'esportatore) se:

(i) riceve una richiesta giuridicamente vincolante di un'autorità pubblica, comprese le autorità giudiziarie, a norma della legislazione del paese di destinazione, di comunicare dati personali trasferiti in conformità delle presenti Clausole; tale notifica comprende informazioni sui dati personali richiesti, sull'autorità richiedente, sulla base giuridica della richiesta e sulla risposta fornita; o

(ii) viene a conoscenza di qualunque accesso diretto effettuato, conformemente alla legislazione del paese terzo di destinazione, da autorità pubbliche ai dati personali trasferiti in conformità delle presenti Clausole; tale notifica comprende tutte le informazioni disponibili all'importatore.

(b) Se la legislazione del paese di destinazione vieta all'importatore di informare l'esportatore e/o l'interessato, l'importatore accetta di fare tutto il possibile per ottenere un'esenzione dal divieto, al fine di comunicare al più

presto quante più informazioni possibili. Per poterlo dimostrare su richiesta dell'esportatore, l'importatore accetta di documentare di aver fatto tutto il possibile.

(c) Laddove consentito dalla legislazione del paese di destinazione, l'importatore accetta di fornire periodicamente all'esportatore, per la durata del contratto, quante più informazioni pertinenti possibili sulle richieste ricevute (in particolare, il numero di richieste, il tipo di dati richiesti, la o le autorità richiedenti, se le richieste sono state contestate e l'esito di tali contestazioni ecc.).

(d) L'importatore accetta di conservare le informazioni di cui alle lettere da a) a c) per la durata del contratto e di metterle a disposizione dell'autorità di controllo competente su richiesta.

(e) Le lettere da a) a c) lasciano impregiudicato l'obbligo dell'importatore in conformità della Clausola 14, lettera e), e della Clausola 16 di informare prontamente l'esportatore qualora non sia in grado di rispettare le presenti Clausole.

15.2 **Riesame della legittimità e minimizzazione dei dati**

(a) L'importatore accetta di riesaminare la legittimità della richiesta di comunicazione, in particolare il fatto che essa rientri o meno nei poteri conferiti all'autorità pubblica richiedente, e di contestarla qualora, dopo un'attenta valutazione, concluda che sussistono fondati motivi per ritenere che essa sia illegittima a norma della legislazione del paese di destinazione, compresi gli obblighi applicabili a norma del diritto internazionale e dei principi di cortesia internazionale. L'importatore, alle stesse condizioni, si avvale delle possibilità di ricorso. Quando contesta una richiesta, l'importatore chiede l'adozione di provvedimenti provvisori affinché gli effetti della richiesta siano sospesi fintantoché l'autorità giudiziaria competente non abbia deciso nel merito. Non comunica i dati personali richiesti fino a quando non sia tenuto a farlo ai sensi delle norme procedurali applicabili. Tali requisiti lasciano impregiudicati gli obblighi dell'importatore a norma della Clausola 14, lettera e).

(b) L'importatore accetta di documentare la propria valutazione giuridica e qualunque contestazione della richiesta di comunicazione e, nella misura consentita dalla legislazione del paese di destinazione, mette tale documentazione a disposizione dell'esportatore. Su richiesta, la mette a disposizione anche dell'autorità di controllo competente.

(c) Quando risponde a una richiesta di comunicazione l'importatore accetta di fornire la quantità minima di informazioni consentite, sulla base di un'interpretazione ragionevole della richiesta.

SEZIONE IV – DISPOSIZIONI FINALI

Clausola 16

Inosservanza delle Clausole e risoluzione

(a) L'importatore informa prontamente l'esportatore qualora, per qualunque motivo, non sia in grado di rispettare le presenti Clausole.

(b) Qualora l'importatore violi le presenti Clausole o non sia in grado di rispettarle, l'esportatore sospende il trasferimento dei dati personali all'importatore fino a che il rispetto non sia nuovamente garantito o il contratto non sia risolto. Ciò lascia impregiudicata la Clausola 14, lettera f).

(c) L'esportatore ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti Clausole qualora:

(i) l'esportatore abbia sospeso il trasferimento dei dati personali all'importatore in conformità della lettera b) e il rispetto delle presenti Clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

(ii) l'importatore violi in modo sostanziale o persistente le presenti Clausole; o

(iii) l'importatore non si conformi a una decisione vincolante di un organo giurisdizionale competente o di un'autorità di controllo competente in merito agli obblighi che gli incombono a norma delle presenti Clausole.

In tali casi, informa l'autorità di controllo competente di tale inosservanza. Qualora le Parti del contratto siano più di due, l'esportatore può esercitare il diritto di risoluzione soltanto nei confronti della Parte interessata, salvo diversamente concordato dalle parti.

(d) I dati personali che sono stati trasferiti prima della risoluzione del contratto in conformità della lettera c) sono, a scelta dell'esportatore, restituiti immediatamente all'esportatore o cancellati integralmente. Lo stesso vale per qualunque copia dei dati. L'importatore certifica all'esportatore la cancellazione dei dati. Finché i dati non sono cancellati o restituiti, l'importatore continua ad assicurare il rispetto delle presenti Clausole. Qualora la legislazione locale applicabile all'importatore vieti la restituzione o la cancellazione dei dati personali trasferiti, l'importatore garantisce che continuerà ad assicurare il rispetto delle presenti Clausole e che tratterà i dati solo nella misura e per il tempo richiesto dalla legislazione locale.

(e) Ciascuna Parte può revocare il proprio accordo a essere vincolata dalle presenti Clausole qualora i) la Commissione europea adotti una decisione in conformità dell'articolo 45, paragrafo 3, del Regolamento (UE) 2016/679 riguardante il trasferimento di dati personali cui si applicano le presenti Clausole; o ii) il Regolamento (UE) 2016/679 diventi parte del quadro giuridico del paese verso il quale i dati personali sono trasferiti. Ciò lascia impregiudicati gli altri obblighi che si applicano al trattamento in questione a norma del Regolamento (UE) 2016/679.

Clausola 17

Legge applicabile

Le presenti Clausole sono disciplinate dalla legge di uno degli Stati membri dell'UE, purché essa riconosca i diritti del terzo beneficiario. Le Parti convengono che si tratta: (a) delle leggi del paese specificato nel Contratto per i Servizi, se tale contratto è disciplinato dalle leggi di uno Stato membro dell'UE, oppure (b) delle leggi dei Paesi Bassi, se il Contratto per i Servizi è disciplinato dalle leggi di un paese terzo.

Clausola 18
Scelta del foro e giurisdizione

Qualunque controversia derivante dalle presenti Clausole è risolta dagli organi giurisdizionali di uno Stato membro dell'UE.

(a) Le Parti convengono che tali organi giurisdizionali sono (i) quelli specificati nell'Accordo per i Servizi, se lo stesso ha stabilito un organo giurisdizionale di uno Stato membro dell'UE, oppure (ii) i tribunali di Amsterdam, se il Contratto per i Servizi ha stabilito un organo giurisdizionale di un paese terzo.

(b) L'interessato può agire in giudizio contro l'esportatore e/o l'importatore anche dinanzi agli organi giurisdizionali dello Stato membro in cui ha la propria residenza abituale.

(c) Le Parti accettano di sottoporsi alla giurisdizione di tali organi giurisdizionali.

NOTA ESPLICATIVA:

APPENDICE

Deve essere possibile distinguere chiaramente le informazioni applicabili a ciascun trasferimento o a ciascuna categoria di trasferimenti e, a tale riguardo, determinare i ruoli rispettivi delle Parti quali esportatori e/o importatori. Non occorre per forza compilare e firmare appendici distinte per ciascun trasferimento/categoria di trasferimenti e/o rapporto contrattuale laddove tale trasparenza possa essere garantita con un'unica appendice. Tuttavia, ove necessario per assicurare una sufficiente chiarezza, dovrebbero essere utilizzate appendici distinte.

ALLEGATO I

A. **ELENCO DELLE PARTI**

Esportatore/i: L'esportatore è identificato come Titolare del trattamento a pagina 1 del presente DPA**.**

Importatore/i: L'importatore è Proofpoint, Inc., un fornitore di servizi di sicurezza per e-mail e social media, analisi delle minacce e corsi sulla sicurezza.

B. **DESCRIZIONE DEL TRASFERIMENTO**

Gli **interessati** sono i dipendenti e i fornitori del Titolare del trattamento, nonché i dipendenti e i fornitori dei clienti e rivenditori del Titolare del trattamento

Categorie di dati: Le categorie di dati sono identificate nell'Appendice 1 al presente DPA. Il Titolare del trattamento non trasferirà dati sensibili a Proofpoint.

Trattamenti: La frequenza di trasferimento, la natura e la finalità del trattamento e il periodo di conservazione sono identificati nell'Appendice 1 al presente DPA.

C. **AUTORITÀ DI CONTROLLO COMPETENTE** ***Identificare la o le autorità di controllo competenti conformemente alla clausola 13***

[Se l'esportatore ha sede in uno Stato membro dell'UE:] L'autorità di controllo dello Stato membro della sede legale dell'esportatore.

[Se l'esportatore di dati non ha sede in uno Stato membro dell'UE, ma rientra nell'ambito di applicazione territoriale del Regolamento (UE) 2016/679 ai sensi del suo articolo 3(2) e ha nominato un rappresentante ai sensi dell'articolo 27(1) del Regolamento (UE) 2016/679:] L'autorità di controllo dello Stato membro della sede legale dell'esportatore.

[Se l'esportatore di dati non ha sede in uno Stato membro dell'UE, ma rientra nell'ambito di applicazione territoriale del Regolamento (UE) 2016/679 ai sensi del suo articolo 3(2) senza tuttavia dover nominare un rappresentante ai sensi dell'articolo 27(2) del Regolamento (UE) 2016/679:] L'autorità di controllo dei Paesi Bassi

ALLEGATO II

MISURE TECNICHE E ORGANIZZATIVE, COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

Le misure tecniche, organizzative e per la sicurezza sono descritte nell'Appendice 2 al presente DPA.

ALLEGATO III

ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

L'elenco attuale dei sub-responsabili del trattamento per i servizi è disponibile sul sito Proofpoint Trust: https://www.proofpoint.com/us/legal/trust