

NOTA: Questa traduzione è stata generata automaticamente e viene fornita solo per comodità. Questa traduzione generata automaticamente non è paragonabile alla qualità di una traduzione umana e potrebbe contenere errori. Questa traduzione viene fornita "COSÌ COM'È" e senza alcuna garanzia in termini di accuratezza, completezza o affidabilità della traduzione. In caso di discrepanze tra la versione in lingua inglese e quella tradotta in una lingua estera, sarà da considerarsi valida unicamente la versione in lingua inglese.

ADDENDUM AL TRATTAMENTO DEI DATI

Data Revisione: 20 gennaio 2022.

Se il presente addendum al trattamento dei dati ("**addendum**") è espressamente incorporato per riferimento in un accordo (il "**Contratto principale**") tra Sophos Limited, società registrata in Inghilterra e Galles con numero 2096520, con sede legale presso The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, Regno Unito ("**fornitore**") e cliente del fornitore ("**cliente**"), il presente addendum fa parte del contratto principale ed è valido tra il fornitore e il cliente.

1. PREAMBOLO

- 1.1 Le parti hanno stipulato il contratto principale relativo alla fornitura da parte del fornitore al cliente di determinati prodotti e/o servizi (collettivamente, "**prodotti**").
- 1.2 Se l'accordo principale è un accordo MSP in forma simile all'accordo MSP che si trova all'indirizzo <https://www.sophos.com/it-it/legal/sophos-msp-partner-terms-and-conditions.aspx> ("**Contratto MSP**"), il cliente è un fornitore di servizi gestiti ("**MSP**"). Se il contratto principale è un contratto OEM in base al quale il cliente è autorizzato a distribuire, concedere in sublicenza o rendere disponibile a terze parti prodotti fornitori in combinazione con i prodotti del cliente come parte di un'unità in bundle ("**Contratto OEM**"), il cliente è un produttore di apparecchiature originali ("**OEM**"). In caso contrario, il cliente è un utente finale ("**utente finale**").
- 1.3 La fornitura dei prodotti può includere la raccolta, l'elaborazione e l'utilizzo dei dati del controllore da parte del fornitore per il cliente. Il presente addendum stabilisce gli obblighi delle parti in relazione a tale trattamento dei dati e completa i termini e le condizioni del contratto principale.
- 1.4 Il Contratto principale, il presente Addendum e i documenti espressamente menzionati nel Contratto principale e nel presente Addendum costituiscono l'intero accordo tra le parti in relazione ai dati personali raccolti, trattati e utilizzati dal fornitore per conto del cliente in relazione al Contratto principale, e sostituiscono tutti i precedenti accordi, intese e intese tra le parti in materia.

2. DEFINIZIONI

- 2.1 Nel presente addendum, i seguenti termini hanno i seguenti significati:

Per "**legislazione applicabile in materia di protezione dei dati**" si intende i) il regolamento UE 2016/679 del Parlamento europeo e del Consiglio relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati o "**GDPR**"); (ii) la direttiva sulla privacy elettronica (direttiva UE 2002/58/CE); e (iii) tutte le normative nazionali applicabili in materia di protezione dei dati, comprese quelle adottate in base ai (i) o (ii); in ogni caso possono essere modificate o sostituite di volta in volta.

"**beneficiario**" ha il significato che le è stato attribuito nell'accordo MSP.

"**Controller**" significa: (a) il cliente, se il cliente è un utente finale; (b) il beneficiario, se il cliente è un MSP; o (c) il cliente finale, se il cliente è un OEM.

Per "**dati del controller**" si intendono tutti i dati personali per i quali il controller è il controller ai sensi delle leggi sulla protezione dei dati applicabili.

"**cliente finale**" ha il significato che gli è stato dato nel contratto OEM.

Per "**Europa**" (e "**europa**") si intendono i) gli Stati membri dello spazio economico europeo ("**SEE**") e II) con effetto immediato a decorrere dalla data in cui la legislazione dell'Unione europea non si applica più al Regno Unito e al Regno Unito.

Per "**clausole contrattuali tipo UE**" o "**CSC UE**" si intendono le clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi ai sensi del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, approvato dalla decisione di esecuzione (UE) 2021/914 della Commissione europea del 4 giugno 2021;

"**clausole UE da controllore a processore**": Le clausole del modulo due per le SCC dell'UE;

Per "**clausole da processore a processore UE**" si intendono le clausole del modulo tre per i CSC dell'UE.

Per "**prodotti ospitati**" si intendono i prodotti elencati nell' **allegato 3**.

Per "**violazione dei dati personali**" si intende una violazione della sicurezza (diversa da quelle causate dal cliente o dai suoi utenti) che comporta la distruzione accidentale o illegale, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso a, Dati del controllore elaborati dal fornitore ai sensi del presente Addendum.

Per "**addendum del Regno Unito**" si intende l'addendum alle SCC dell'UE, indicato nella mostra, ove applicabile.

- 2.2 Nel presente addendum, i termini in lettere minuscole "**titolare**", "**titolare**", "**soggetto**", "**dati personali**" e "**trattamento**" (e relativi derivati) avranno il significato indicato nella legge applicabile sulla protezione dei dati.

3. **AMBITO**

- 3.1 L'oggetto e la durata del trattamento dei dati del controllore da parte del fornitore, compresa la natura e lo scopo del trattamento, i tipi di dati del controllore da trattare, e le categorie di soggetti interessati, saranno come descritto in: (i) il presente addendum; (II) il contratto principale; (III) qualsiasi istruzione nell' **allegato 1**; E (v) le istruzioni del cliente fornite in conformità alla clausola 4.
- 3.2 Il cliente è responsabile di garantire (i) che il controllore disponga di una base legale per il trattamento dei dati del controllore che saranno effettuati dal fornitore per suo conto, E (II) che il Titolare abbia ottenuto tutte le autorizzazioni necessarie da soggetti interessati che potrebbero essere necessarie per il trattamento dei dati del Titolare da parte del cliente e del fornitore (inclusi, senza limitazione, in relazione a categorie speciali di dati); E (III) che sia altrimenti conforme alle leggi sulla protezione dei dati applicabili e che assicurerà che le sue istruzioni al fornitore per il trattamento dei dati del controllore siano conformi sotto tutti gli aspetti.
- 3.3 Le restanti disposizioni del presente addendum descrivono i rispettivi obblighi delle parti in relazione ai dati del controllore per i quali: (i) il cliente è il controllore e il fornitore è il processore, se il cliente è un utente finale; o (II) il cliente è il processore per un controller di terze parti e il fornitore è il sottoprocessore, se il cliente è un MSP o un OEM.

4. ISTRUZIONI PER IL CLIENTE

- 4.1 Il fornitore elaborerà i dati del controllore in conformità con le istruzioni documentate del cliente, come stabilito esclusivamente nella clausola 3.1 , ad eccezione di:
- (a) Ove diversamente concordato per iscritto tra il fornitore e il cliente; oppure
 - (b) Ove richiesto dalla legge cui il fornitore è soggetto (in tal caso, il fornitore deve informare il cliente di tale requisito legale prima del trattamento, a meno che tale legge non vieti la fornitura di tali informazioni).
- 4.2 Se il fornitore viene a conoscenza che le istruzioni di trattamento del cliente violano le leggi sulla protezione dei dati applicabili (senza imporre alcun obbligo al fornitore di monitorare attivamente la conformità del cliente), ne informerà prontamente il cliente e sospenderà il trattamento dei dati del controllore.

5. DOVERI DEL FORNITORE

- 5.1 tutto il personale del fornitore che elabora i dati del Titolare deve essere adeguatamente formato in relazione ai propri obblighi di protezione, sicurezza e riservatezza dei dati e deve essere soggetto agli obblighi scritti di mantenimento della riservatezza.
- 5.2 il fornitore attuerà, a proprie spese, adeguate misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio e per proteggere i dati del Titolare contro una violazione dei dati personali. Tali misure tengono conto dello stato della tecnica, dei costi di attuazione e della natura, della portata, contesto e finalità del trattamento, nonché rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, in modo da garantire un livello di sicurezza adeguato al rischio. In particolare, le misure adottate dal fornitore comprendono quelle descritte **nell'allegato 2** del presente addendum. Il fornitore può modificare o modificare le misure tecniche ed organizzative descritte nell' **allegato 2** senza il preventivo consenso scritto del cliente, purché il fornitore mantenga almeno un livello equivalente di protezione. Su richiesta del cliente, il fornitore fornirà una descrizione aggiornata delle misure tecniche ed organizzative nel modulo presentato nell' **allegato 2**.
- 5.3 il fornitore deve attenersi ai requisiti specificati nella clausola 7 per l'impegno di qualsiasi sottoprocessore nell'elaborazione dei dati del controllore.
- 5.4 il fornitore deve attenersi ai requisiti specificati nella clausola 8 per assistere il cliente a rispondere a richieste di terzi, comprese eventuali richieste da parte di soggetti interessati di esercitare i propri diritti in base alle leggi sulla protezione dei dati applicabili.
- 5.5 al momento della conferma della violazione dei dati personali, il fornitore informerà il cliente senza indebiti ritardi e fornirà tutte le informazioni e la cooperazione tempestive che il cliente potrebbe ragionevolmente richiedere per l'ordine del cliente (e, se il cliente è un MSP o un OEM, il suo controllore) Per adempiere agli obblighi di segnalazione delle violazioni dei dati previsti dalla legge sulla protezione dei dati (e in conformità con i tempi richiesti dalla legge applicabile sulla protezione dei dati). Il fornitore dovrà inoltre adottare tutte le misure e le azioni necessarie per rimediare o mitigare gli effetti della violazione dei dati personali e tenere il cliente informato di tutti gli sviluppi in relazione alla violazione dei dati personali.
- 5.6 il fornitore fornirà al cliente (o, se il cliente è un MSP o un OEM, il suo controllore) tutta l'assistenza ragionevole e tempestiva che il cliente (o, se applicabile, il controllore) può richiedere per condurre una valutazione dell'impatto sulla protezione dei dati e, se necessario, consultare l'autorità competente per la protezione dei dati. Tale assistenza sarà fornita a spese del cliente.

5.7 il fornitore cancellerà i dati del controllore entro un ragionevole periodo di tempo successivo alla risoluzione o alla scadenza del presente Addendum, in ogni caso se e nella misura consentita dalla normativa europea applicabile.

5.8 il fornitore deve attenersi ai requisiti specificati nella clausola 6 per la fornitura al cliente (e, se il cliente è un MSP o OEM, il suo controllore) delle informazioni necessarie per dimostrare la conformità del fornitore agli obblighi stabiliti nel presente Addendum.

6. DIRITTI DI VERIFICA DEL CLIENTE

6.1 il cliente riconosce che il fornitore viene regolarmente sottoposto a verifica in base agli standard SSAE 18 SOC 2 da parte di revisori indipendenti di terze parti. Su richiesta, il fornitore dovrà fornire al cliente una copia del suo rapporto di verifica SOC 2, che sarà soggetto alle disposizioni di riservatezza del Contratto principale come informazioni riservate del fornitore. Il cliente riconosce e accetta che il revisore esterno che ha creato tale rapporto ("**autore**") non si assume alcuna responsabilità nei confronti del cliente o dei revisori del cliente a meno che e fino a quando il cliente non stipulerà un contratto separato con l'autore. Il fornitore dovrà inoltre rispondere a eventuali domande di verifica scritte ad esso presentate dal cliente, a condizione che quest'ultimo non eserciti tale diritto più di una volta all'anno.

7. SOTTOPROCESSORI

7.1 il cliente acconsente ai subprocessori esistenti del fornitore alla data del presente Addendum, elencati all'indirizzo <https://www.sophos.com/en-us/legal> ("**elenco subprocessori**"). Il fornitore non subapporterà il trattamento dei dati del controller a nessun altro processore di terze parti (ciascuno un "**nuovo processore**") senza previa notifica al cliente. Il fornitore notificherà preventivamente l'aggiunta di qualsiasi nuovo subprocessore (compresi i dettagli generali del trattamento che esegue o che eseguirà), la cui notifica può essere data pubblicando i dettagli di tale aggiunta nell'elenco dei subprocessori. Se il cliente non si oppone per iscritto alla nomina da parte del fornitore di un nuovo subprocessore (per motivi ragionevoli relativi alla protezione dei dati del controllore) entro 30 giorni dall'aggiunta del nuovo subprocessore all'elenco dei subprocessori da parte del fornitore, il cliente accetta che si riterrà di aver acconsentito a tale nuovo subprocessore. Se il cliente fornisce tale obiezione scritta al fornitore, il fornitore notificherà per iscritto al cliente entro 30 giorni che: (i) il fornitore non utilizzerà il nuovo subprocessore per elaborare i dati del controller; o (ii) il fornitore non è in grado o non è disposto a farlo. Se viene data la notifica di cui al paragrafo (ii), il cliente può, entro 30 giorni da tale notifica, Scegliere di risolvere il presente addendum e l'accordo principale relativo all'elaborazione interessata previa notifica scritta al fornitore e al fornitore per i clienti situati solo all'interno dello spazio economico europeo e del Regno Unito, autorizzare un rimborso proporzionale o un credito di eventuali commissioni prepagate per il periodo rimanente dopo la risoluzione. Tuttavia, se tale notifica di risoluzione non viene fornita entro tale termine, il cliente sarà considerato autorizzato al nuovo subprocessore. Il fornitore imporrà termini di protezione dei dati ai nuovi subprocessori per proteggere i dati del controllore allo stesso standard previsto dal presente Addendum e il fornitore rimarrà pienamente responsabile per qualsiasi violazione del presente Addendum causata da tali subprocessori.

8. RICHIESTE DI TERZI

8.1 il fornitore fornirà al cliente tutta l'assistenza ragionevole e tempestiva (o, se il cliente è un MSP o OEM, il controllore), a spese del cliente, per consentire al cliente di rispondere a: (i) qualsiasi richiesta da parte di un soggetto interessato di esercitare uno qualsiasi dei suoi diritti ai sensi della legge sulla protezione dei dati applicabile (compresi i suoi diritti di accesso, correzione, obiezione, cancellazione e portabilità dei dati, se applicabile); E (ii) qualsiasi altra corrispondenza, richiesta o reclamo ricevuto da un soggetto interessato, ente regolatore o altra terza parte in relazione al trattamento dei dati del controllore. Qualora tale richiesta, corrispondenza, richiesta o reclamo venga fatto direttamente al

fornitore, il fornitore dovrà informare prontamente il cliente fornendo i dettagli completi della stessa.

9. TRASFERIMENTI INTERNAZIONALI DI DATI

9.1 alcuni prodotti consentono al cliente di scegliere se ospitare i dati del controllore per tali prodotti in data center che possono essere situati in (i) Area economica europea, (II) Regno Unito o (iii) Stati Uniti d'America ("**Ubicazione centrale di immagazzinamento**"). Questa selezione avviene al momento dell'installazione, della creazione dell'account o del primo utilizzo del prodotto in questione. Una volta selezionata, la posizione di memorizzazione centrale non può essere modificata in un secondo momento.

9.2 il cliente riconosce e accetta che, indipendentemente dalla sede di archiviazione centrale selezionata (se pertinente), i dati del controllore possono essere esportati attraverso o verso altre giurisdizioni (all'interno e/o all'esterno del Regno Unito e dello spazio economico europeo): (i) al team globale di tecnici e ingegneri di Sophos per malware, minacce alla sicurezza e analisi false positive, nonché per scopi di ricerca e sviluppo, (II) per fornire supporto tecnico e al cliente, gestione degli account, fatturazione e altre funzioni accessorie, e (III) come espressamente descritto nella documentazione di cui alla clausola 3.1.

9.3 il fornitore non deve trasferire i dati del controllore (né consentire l'elaborazione dei dati del controllore da o verso) Un paese al di fuori dell'Europa, a meno che il trasferimento non sia effettuato in un paese ritenuto adeguato dalle leggi sulla protezione dei dati applicabili o che il fornitore non prenda le misure necessarie per garantire che il trasferimento sia conforme alle leggi sulla protezione dei dati applicabili, incluse, ad esempio, ma senza limitazioni, Mediante l'uso delle SCC dell'UE (modificate di volta in volta).

9.4 la restrizione di trasferimento descritta nella clausola 9.3 si applica anche ai trasferimenti di dati del controllore dallo spazio economico europeo al Regno Unito se e quando il Regno Unito cessa di essere soggetto al diritto dell'Unione europea.

9.5 Qualora la clausola 9.3 si applichi perché il fornitore o un'affiliata del fornitore elaborerà i dati del controllore in un paese al di fuori del Regno Unito o del SEE, in tal caso (e solo nella misura in cui per qualsiasi trasferimento di dati del controllore, Non sono disponibili altre misure riconosciute dalle leggi sulla protezione dei dati applicabili per consentire tali trasferimenti (ad esempio, senza limitazioni, Trasferimento a un destinatario in un paese che si ritiene fornisca un'adeguata protezione dei dati personali ai sensi delle leggi sulla protezione dei dati applicabili o trasferimento a un destinatario che ha ottenuto un'autorizzazione vincolante alle norme aziendali in conformità alle leggi sulla protezione dei dati applicabili)) per qualsiasi trasferimento dei dati del titolare, le parti convengono che:

A) per i trasferimenti dal SEE, si applicano le clausole del controllore dell'UE al processore e tali CSC dell'UE sono incorporate per riferimento nel presente addendum;

(b) per i trasferimenti dal Regno Unito, si applicano le clausole relative al controllore dell'UE per il processore (e tali CSC dell'UE sono qui incorporati per riferimento nel presente addendum), a condizione che tali clausole relative al controllore dell'UE per il processore siano soggette all'addendum del Regno Unito.

9.6 se la clausola 9.3 si applica perché il fornitore o un'affiliata del fornitore elaborerà i dati del controllore in un paese al di fuori del Regno Unito o del SEE allora in tal caso (e solo nella misura in cui per qualsiasi trasferimento di dati del controllore, Non sono disponibili altre misure riconosciute dalle leggi sulla protezione dei dati applicabili per consentire tali trasferimenti (ad esempio, senza limitazioni, Trasferimento a un destinatario in un paese

che si ritiene fornisca un'adeguata protezione dei dati personali ai sensi delle leggi sulla protezione dei dati applicabili o trasferimento a un destinatario che ha ottenuto un'autorizzazione vincolante alle norme aziendali in conformità alle leggi sulla protezione dei dati applicabili)) dove (Come previsto dalla clausola 3.3(II)) il cliente è il processore di un controllore di terze parti e il fornitore è il sottoprocessore, le parti concordano che:

A) per i trasferimenti dal SEE, si applicano le clausole UE dal processore al processore e tali SCC UE sono incorporati per riferimento nel presente addendum;

(b) per i trasferimenti dal Regno Unito, si applicano le clausole EU Processor to Processor (e tali SCC UE sono qui incorporati per riferimento nel presente addendum), a condizione che tali clausole EU Processor to Processor siano soggette all'addendum UK.

9.7 l'appendice alle SCC dell'UE deve essere compilata come indicato nell'allegato 4.

9.8 per ciascun modulo ai CCS dell'UE, ove applicabile:

- (a) La clausola facoltativa di docking di cui alla clausola 7 non si applica;
- (b) Si applica l'opzione 2 ai sensi della clausola 9. L'importatore di dati notifica all'esportatore di dati con 30 giorni di anticipo qualsiasi modifica prevista (mediante aggiunta o sostituzione) all'elenco dei sottoprocessori.
- (c) Nella clausola 11, la lingua facoltativa non si applica;
- (d) Ai fini dell'applicazione delle clausole 13, lettera a), si intende per:
 - Se l'esportatore di dati è stabilito in uno Stato membro dell'UE: L'autorità di vigilanza incaricata di garantire l'osservanza da parte dell'esportatore di dati del regolamento (UE) n. 2016/679 per quanto riguarda il trasferimento dei dati è l'autorità di vigilanza competente presso la quale è stabilito l'esportatore di dati e agisce come autorità di vigilanza competente.
- (e) Ai fini della clausola 17, le SCC dell'UE sono disciplinate dalla legge dello Stato membro dell'UE in cui è stabilito l'esportatore di dati;
- (f) Ai fini della clausola 18(b), le controversie saranno risolte dinanzi ai tribunali dello Stato membro dell'UE in cui è stabilito l'esportatore di dati.

10. DURATA

10.1 il presente addendum inizia con l'esecuzione da parte di entrambe le parti dell'accordo principale (o la data in cui l'accordo principale diventa effettivo, se successiva) e continua fino alla data precedente di: (i) la scadenza del diritto del cliente di utilizzare e ricevere i prodotti, come indicato nel Contratto principale o su qualsiasi diritto di licenza associato; e (II) la risoluzione del Contratto principale.

11. ALTRE NORMATIVE

11.1 le modifiche e le modifiche al presente addendum richiedono la forma scritta. Ciò vale anche per le modifiche e le modifiche apportate alla presente clausola 11.1.

11.2 in nessun caso la responsabilità del fornitore nei confronti del cliente in relazione a qualsiasi problema derivante o connesso al presente addendum potrà superare le limitazioni di responsabilità del fornitore stabilite nel Contratto principale. Le limitazioni di responsabilità del fornitore stabilite nel Contratto principale si applicheranno in modo aggregato sia nell'Addendum principale che nel presente Addendum, in modo tale che si applichi un

unico regime di limitazione di responsabilità sia nell'accordo principale che nel presente Addendum.

11.3 il presente addendum sarà governato e interpretato in conformità con le leggi di Inghilterra e Galles, indipendentemente dai principi relativi ai conflitti di legge. Nella misura consentita dalla legge applicabile, i tribunali inglesi avranno la giurisdizione esclusiva per determinare qualsiasi controversia o reclamo che possa sorgere da, sotto o in relazione al presente addendum.

11.4 in caso di conflitto con i termini del presente Addendum al trattamento dei dati e con i termini di qualsiasi SCC stipulato dalle parti, i termini del CCS dell'UE applicabile avranno la precedenza.

Mostra 1
Istruzioni per l'elaborazione dei dati

Il presente allegato 1 descrive l'elaborazione che il fornitore eseguirà per conto del cliente.

A) oggetto, natura e finalità delle operazioni di trasformazione

I dati del Controller saranno soggetti alle seguenti attività di elaborazione di base (specificare):

1. Fornitura dei prodotti acquistati dal cliente in base e in conformità al Contratto principale
2. Fornire servizi di gestione degli account e assistenza tecnica ai clienti

Il fornitore fornisce prodotti progettati per rilevare, prevenire e gestire o aiutare il fornitore a rilevare, prevenire e gestire le minacce alla sicurezza all'interno o contro sistemi, reti, dispositivi, file e altri dati resi disponibili dal cliente. Il contenuto delle informazioni contenute in tali sistemi, reti, dispositivi, file e altri dati è determinato esclusivamente dal cliente e non dal fornitore.

B) durata delle operazioni di trasformazione:

I dati del controller verranno elaborati per la seguente durata (specificare):

La durata specificata nell'accordo principale (o per la durata dell'accordo principale, se non diversamente specificato).

C) soggetti interessati

I dati del controller riguardano le seguenti categorie di soggetti (specificare):

I soggetti interessati includono le persone su cui i dati vengono forniti al fornitore tramite i prodotti da (o su indicazione) del cliente o degli utenti finali del cliente.

D) tipi di dati personali

I dati del controller riguardano le seguenti categorie di dati (specificare):

Dati relativi alle persone fornite al fornitore tramite i prodotti, da (o su indicazione) del cliente o degli utenti finali del cliente, come le informazioni di contatto

E) categorie speciali di dati (se del caso)

I dati del controller riguardano le seguenti categorie speciali di dati (specificare):

Se non diversamente specificato, i prodotti del fornitore non sono progettati per elaborare categorie particolari di dati.

Mostra 2 Misure tecniche e organizzative

Alcune di queste misure possono essere pertinenti o applicabili solo ai prodotti ospitati.

A) Controllo di accesso fisico.

- Sophos dispone di una politica di controllo dell'accesso fisico;
- Tutti i badge di accesso/ID di trasporto del personale;
- Le entrate alle strutture sono protette da badge o chiavi di accesso;
- Le strutture sono suddivise in (i) aree di accesso pubblico (come le aree di ricevimento), (II) aree di accesso al personale generale e (III) aree di accesso limitato alle quali possono accedere solo il personale con esigenze aziendali espresse;
- I badge e le chiavi di accesso controllano l'accesso alle aree riservate all'interno di ogni struttura in base ai livelli di accesso autorizzati di un individuo;
- I livelli di accesso per i singoli individui sono approvati dai membri del personale senior e verificati su base trimestrale;
- Il personale addetto alla reception e/o alla sicurezza è presente all'ingresso di siti più grandi;
- Le strutture sono protette da allarmi;
- I visitatori sono pre-registrati e i registri dei visitatori sono mantenuti.

B) Controllo dell'accesso al sistema.

- Sophos ha una logica politica di controllo degli accessi;
- La rete è protetta da firewall ad ogni connessione Internet;
- La rete interna è segmentata da firewall in base alla sensibilità delle applicazioni;
- GLI ID e altri controlli di rilevamento e blocco delle minacce vengono eseguiti su tutti i firewall;
- Il filtraggio del traffico di rete si basa su regole che applicano il principio del "minimo accesso";
- I diritti di accesso sono concessi solo al personale autorizzato nella misura e per la durata necessarie per svolgere i propri ruoli professionali e sono rivisti trimestralmente;
- L'accesso a tutti i sistemi e le applicazioni è controllato da una procedura di accesso sicura;
- Gli individui hanno ID utente e password univoci per il loro uso;
- Le password sono testate in modo rigoroso e le modifiche vengono applicate alle password deboli;
- Gli schermi e le sessioni si bloccano automaticamente dopo un periodo di inattività;
- I prodotti Sophos per la protezione da malware sono installati come standard;
- Vengono eseguite regolari scansioni di vulnerabilità su indirizzi e sistemi IP;
- I sistemi vengono patchati su un ciclo regolare con un sistema di prioritizzazione per il tracciamento rapido delle patch urgenti.

C) Controllo dell'accesso ai dati.

- Sophos ha una logica politica di controllo degli accessi;
- I diritti di accesso sono concessi solo al personale autorizzato nella misura e per la durata necessarie per svolgere i propri ruoli professionali e sono rivisti trimestralmente;
- L'accesso a tutti i sistemi e le applicazioni è controllato da una procedura di accesso sicura;
- Gli individui hanno ID utente e password univoci per il loro uso;
- Le password sono testate in modo rigoroso e le modifiche vengono applicate alle password deboli;

- Gli schermi e le sessioni si bloccano automaticamente dopo un periodo di inattività;
 - I laptop sono crittografati utilizzando i prodotti di crittografia Sophos;
 - I mittenti sono indirizzati a prendere in considerazione la crittografia dei file prima di inviare qualsiasi e-mail esterna.
- D) Controllo input.
- L'accesso a tutti i sistemi e le applicazioni è controllato da una procedura di accesso sicura;
 - Gli individui hanno ID utente e password univoci per il loro uso;
 - I prodotti Sophos Central utilizzano la crittografia a livello di trasferimento per proteggere i dati in transito;
 - La comunicazione tra il software client e il sistema backend Sophos viene eseguita tramite HTTPS per proteggere i dati in transito, stabilendo una comunicazione di trust tramite certificati e convalida del server.
- E) Controllo subappaltatore.
- I subappaltatori che hanno accesso ai dati intraprendono una procedura di verifica della sicurezza INFORMATICA prima dell'imbarco e, successivamente, secondo quanto richiesto;
 - I contratti contengono obblighi di riservatezza e di protezione dei dati adeguati basati sulle funzioni del subappaltatore.
- F) Controllo disponibilità.
- Sophos protegge i propri locali da incendi, inondazioni e altri rischi ambientali;
 - Sono disponibili generatori di riserva per mantenere gli alimentatori in caso di interruzioni di corrente;
 - I data center e le sale server utilizzano i controlli e il monitoraggio del clima;
 - Il sistema Sophos Central è a carico bilanciato e ha un failover tra tre siti, ognuno dei quali esegue due istanze del software, ognuno dei quali è in grado di fornire il servizio completo.
- G) Controllo segregazione.
- Sophos mantiene e applica un processo di controllo della qualità per la distribuzione di nuovi prodotti per i clienti;
 - Gli ambienti di test e produzione sono separati;
 - I nuovi software, sistemi e sviluppi vengono testati prima del rilascio nell'ambiente di produzione.
- H) Controllo organizzativo.
- Sophos dispone di un team dedicato alla sicurezza IT;
 - Il team Risk and Compliance gestisce i report e i controlli interni dei rischi, che includono la segnalazione dei rischi chiave per il management;
 - Un processo di risposta agli incidenti identifica e rimedia tempestivamente i rischi e le vulnerabilità;
 - Ogni nuovo dipendente si occupa della protezione dei dati e della formazione sulla sicurezza INFORMATICA;
 - Il reparto IT Security conduce campagne trimestrali di sensibilizzazione alla sicurezza.

Mostra 3
Prodotti ospitati

- Sophos Central
 - Sophos Cloud Optix
 - Central Device Encryption
 - Central Endpoint Protection
 - Central Endpoint Intercept X
 - Central Endpoint Intercept X Advanced
 - Central Mobile Advanced
 - Central Mobile Standard
 - Central Phish Threat
 - Central Intercept X Advanced for Server
 - Central Server Protection
 - Central Mobile Security
 - Central Web Gateway Advanced
 - Central Web Gateway Standard
 - Central Email Standard
 - Central Email Advanced
 - Central Wireless Standard
 - Qualsiasi altro prodotto Sophos somministrato e utilizzato tramite Sophos Central
-

Mostra 4

Dati di riferimento per LE CLAUSOLE CONTRATTUALI TIPO UE

APPENDICE 1 ALLE CLAUSOLE CONTRATTUALI TIPO UE

R: ELENCO DELLE PARTI

Esportatore/i di dati: *[identità e dati di contatto dell'esportatore/degli esportatori di dati, compresi i contatti con responsabilità per la protezione dei dati]*

Nome cliente: come fornito al fornitore in base al contratto principale

Indirizzo: come fornito al fornitore in base all'e-mail di contatto del contratto principale:

Nome/posizione della persona di contatto: Come fornito al fornitore in base al contratto principale

Attività relative ai dati trasferiti ai sensi delle presenti clausole: Come descritto nella precedente clausola 3

Ruolo (controller/processore): Centralina

Importatore/i di dati: *[identità e informazioni di contatto dell'importatore o degli importatori di dati e, se del caso, del suo responsabile e/o rappresentante per la protezione dei dati nell'Unione europea]*

Nome: Sophos Limited (per conto e per conto delle sue controllate UE e svizzere)

Indirizzo: The Pentagon, Abingdon Science Park Abingdon, OX14 3YP, Regno Unito

Numero di registrazione: 2096520

Nome, posizione e recapiti della persona di contatto: dataprotection@sophos.com

Attività relative ai dati trasferiti ai sensi delle presenti clausole: Come descritto nella precedente clausola 3.

Ruolo (controller/processore): Processore

B. DESCRIZIONE DEL TRASFERIMENTO

Categorie di soggetti i cui dati personali sono trasferiti:

Come descritto nella sezione C, allegato 1 precedente

Categorie di dati personali trasferiti:

Come descritto nella sezione D, allegato 1 precedente

Dati sensibili trasferiti (se applicabile) e applicate restrizioni o garanzie che tengano pienamente conto della natura dei dati e dei rischi connessi, come ad esempio una rigorosa limitazione dello scopo, restrizioni di accesso (compreso l'accesso solo al personale che ha seguito una formazione specializzata), tenendo un registro dell'accesso ai dati; restrizioni per i trasferimenti successivi o ulteriori misure di sicurezza:

Come descritto nella Sezione e, allegato 1 di cui sopra.

La frequenza del trasferimento (ad esempio, se i dati vengono trasferiti su base singola o continua).

Continuo

Natura del trattamento

Come descritto nella sezione A, allegato 1 di cui sopra.

Finalità del trasferimento e dell'ulteriore trattamento dei dati

Come descritto nella sezione A, allegato 1 di cui sopra.

Il periodo di conservazione dei dati personali o, se ciò non è possibile, i criteri utilizzati per determinare tale periodo

Per la durata del periodo contrattuale.

Per i trasferimenti ai (sub) trasformatori, specificare anche l'oggetto, la natura e la durata del trattamento

Come descritto nella precedente clausola 3.

AUTORITÀ DI VIGILANZA COMPETENTE

CFR. SOPRA IL PUNTO 9.8

ALLEGATO II – MISURE TECNICHE E ORGANIZZATIVE, COMPRESSE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI¹

Le misure sono esposte nel precedente allegato 2 .

ALLEGATO III – ELENCO DEI SOTTOPROCESSORI²

Non richiesto in quanto la clausola 9(a), l'opzione 1 **non** è stata selezionata.

¹ L'allegato II deve essere compilato per tutti i moduli, ad eccezione DEL MODULO 4.

² L'allegato III si applica solo AL MODULO 2 (controllore di trasferimento al processore) e AL MODULO 3 (processore di trasferimento al processore), dove è stata selezionata la clausola 9(a), opzione 1).