MISURE TECNICHE E ORGANIZZATIVE

(PER I CLIENTI)

Queste misure tecniche e organizzative (Technical and Organizational Measures, "**TOMs**") sono parte integrante del Contratto/Addendum/Allegato/Programma/Sezione (o qualsiasi altro documento equivalente, secondo quanto applicabile) sul Trattamento dei dati personali tra Avaya (inclusi le società del Gruppo) e il Cliente (inclusi le società del Gruppo, se presenti), che li include tramite riferimento.

1. Controllo dell'accesso ai locali

Avaya deve impedire l'accesso fisico alle attrezzature per il Trattamento dei dati personali da parte di persone non autorizzate come segue:

1.1. Avaya deve implementare e mantenere misure di sicurezza fisica al fine di prevenire l'accesso non autorizzato. Ciò viene realizzato attraverso le seguenti misure:

1.1.1. un sistema di controllo elettronico degli accessi con conservazione dei registri per 90 giorni;

1.1.2. un impianto fisico di registrazione video 24 ore su 24, 7 giorni su 7, con conservazione dei registri per 30 giorni; e

1.1.3. rilevatori di intrusione/antifurto o impiego di agenti di sicurezza presso i locali.

1.2. Avaya limiterà l'accesso a varie zone presso i propri locali in base ai ruoli e rinnoverà periodicamente la convalida d'accesso per i titolari.

1.3. Avaya disporrà di misure di sicurezza del personale e dei visitatori per impedire l'accesso non autorizzato, che si ottiene con le seguenti misure:

1.3.1. il personale deve mostrare documenti identificativi;

1.3.2. i visitatori devono registrarsi;

1.3.3. i visitatori saranno ragionevolmente scortati dal personale; e

1.3.4. i visitatori devono indossare un badge che li identifichi facilmente come visitatori.

2. Controllo dell'accesso all'uso del sistema

Al fine di impedire l'accesso remoto alle attrezzature che trattano i Dati personali da parte di persone non autorizzate, Avaya deve attuare e mantenere le seguenti misure:

2.1. Avaya concederà l'accesso alle apparecchiature per il trattamento dei Dati personali solamente alle persone con

2.1.1. un ID utente univoco per l'accesso con processo di autorizzazione formale, e

2.1.2. una password univoca con le seguenti caratteristiche:

2.1.2.1. una password complessa, composta da otto caratteri e tre categorie di caratteri su quattro;

2.1.2.2. una durata massima della password di novanta giorni; e

2.1.2.3. il blocco dell'account per gli accessi non riusciti.

2.2. Avaya deve garantire agli individui l'accesso in base alla loro funzione lavorativa con i seguenti criteri:

2.2.1. accesso in base al ruolo;

2.2.2. accesso con privilegi minimi; e

2.2.3. accesso basato solo sulle esigenze informative.

2.3. Lo schermo degli endpoint verrà automaticamente bloccato dopo 20 minuti di inattività.

2.4. Avaya registrerà l'accesso alle attrezzature per il trattamento dei dati.

2.5. Avaya utilizzerà un'autenticazione a più fattori per l'accesso remoto alla rete privata virtuale (VPN) di Avaya.

2.6. Avaya implementerà e gestirà un'amministrazione centrale degli utenti.

2.7. Avaya provvederà direttamente a crittografare gli endpoint forniti.

3. Controllo dell'accesso ai dati personali

Avaya impedirà l'accesso remoto ai Dati personali da parte di persone non autorizzate implementando e mantenendo misure adeguate per impedire la lettura, la copia, l'alterazione o la rimozione non autorizzate di contenuti che includono Dati personali, l'immissione non autorizzata nella memoria, la lettura, l'alterazione o la cancellazione dei Dati personali memorizzati. Ciò sarà realizzato attraverso le seguenti misure:

3.1. Avaya concederà l'accesso ai Dati personali solamente alle persone con:

3.1.1. un ID utente univoco per l'accesso con processo di autorizzazione formale, e

3.1.2. una password univoca con le seguenti caratteristiche:

3.1.2.1. una password complessa, composta da otto caratteri e tre categorie di caratteri su quattro;

3.1.2.2. una durata massima della password di novanta giorni; e

3.1.2.3. il blocco dell'account per gli accessi non riusciti.

3.2. Avaya garantirà agli individui l'accesso ai Dati personali in base alla loro funzione lavorativa con i seguenti criteri:

3.2.1. accesso in base al ruolo;

3.2.2. accesso con privilegi minimi; e

3.2.3. accesso basato solo sulle esigenze informative.

3.3. Lo schermo degli endpoint verrà automaticamente bloccato dopo 20 minuti di inattività.

3.4. Avaya registrerà l'accesso alle attrezzature per il trattamento dei dati.

3.5. Avaya conserverà elenchi di controllo degli accessi (Access Control List, ACL).

3.6. Avaya eseguirà backup e recuperi dei dati, implementando una conservazione sicura dei supporti di backup e testando i backup.

3.7. Avaya implementerà e manterrà un programma formale di gestione delle modifiche al controllo degli accessi.

3.8. Avaya implementerà e manterrà politiche e standard interni comprendenti politiche e standard di sicurezza, sia a livello aziendale generale sia a livello di singola unità aziendale.

3.9. Avaya terrà periodicamente corsi di formazione obbligatori relativi alla protezione dei dati personali e monitorerà e rafforzerà la partecipazione alla formazione.

3.10. Avaya implementerà e manterrà programmi antivirus, che verranno monitorati e aggiornati a livello centrale ed effettuerà regolarmente scansioni antivirus.

3.11. Avaya eseguirà una cancellazione e/o eliminazione sicura dei dati.

4. Controllo della trasmissione

Avaya impedirà qualsiasi accesso non autorizzato ai Dati personali tramite l'implementazione di canali di comunicazione e registrazione sicuri, secondo quanto indicato di seguito:

4.1. Avaya utilizzerà una VPN con autenticazione a più fattori per l'accesso remoto.

4.2. Avaya utilizzerà firewall con le seguenti funzionalità e procedure:

4.2.1. ispezione stateful;

4.2.2. implementazione di regole predefinite di diniego dell'accesso ove non siano esplicitamente approvate regole di accesso;

4.2.3. accesso basato sui ruoli e con privilegi minimi basato sulle esigenze informative;

4.2.4. registrazione e segnalazione degli accessi; e

4.2.5. revisione annuale delle regole del firewall.

4.3. Avaya utilizzerà e-mail crittografate se sono state abilitate anche dal Cliente, utilizzando la TLS (Transport Layer Security) come metodo.

4.4. Avaya implementerà e manterrà politiche e standard di sicurezza, sia a livello aziendale generale sia a livello di singola unità aziendale.

5. Controllo dell'inserimento

Avaya garantirà la possibilità di verificare e stabilire se, e da chi, i Dati Personali siano stati inseriti, modificati o rimossi dall'apparecchiatura di elaborazione dei dati come segue:

5.1. le persone che accedono ai dati personali disporranno di un ID utente univoco e di autorizzazione per l'accesso.

5.2. Avaya implementerà e manterrà politiche e standard di sicurezza, sia a livello aziendale generale sia a livello di singola unità aziendale.

5.3. Le attrezzature per il trattamento dei Dati personali disporranno di funzionalità di registrazione.

5.4. Avaya garantirà agli individui l'accesso ai Dati personali solo in base alla loro funzione lavorativa con i seguenti criteri:

5.4.1. accesso in base al ruolo;

5.4.2. accesso con privilegi minimi; e

5.4.3. accesso basato sulle esigenze informative.

6. Controllo dell'organizzazione

6.1. Avaya assicurerà che, in caso di trattamento dei dati su commissione, i Dati personali vengano trattati rigorosamente in conformità alle istruzioni del Cliente.

6.2. Il Cliente fornirà istruzioni chiare ad Avaya in merito all'ambito del trattamento dei dati personali e Avaya rispetterà tali istruzioni.

7. Controllo della disponibilità

Avaya impedirà qualsiasi distruzione accidentale o la perdita dei Dati personali tramite misure appropriate, come indicato di seguito:

7.1. Avaya implementerà e manterrà, in base agli standard del settore, alimentazione elettrica ininterrotta, allarmi antincendio e fumo, sistemi antincendio, generatori, sistemi di raffreddamento e pavimenti sopraelevati.

7.2. Avaya implementerà e manterrà un piano di ripristino di emergenza e lo esaminerà e verificherà annualmente.

7.3. Avaya implementerà e manterrà una strategia di backup e procedure di backup.

7.4. Avaya implementerà e manterrà programmi antivirus e sistemi firewall.

8. Controllo della separazione dei dati

Avaya implementerà e manterrà misure appropriate per consentire il trattamento separato dei dati che sono stati raccolti per diversi scopi come segue:

8.1. Avaya separerà i Dati personali di clienti differenti conservando i Dati personali in database separati logicamente.

8.2. Avaya separerà i dati produttivi e i dati di test.

- FINE DELLE TOMs -