MISURE TECNICHE E ORGANIZZATIVE

(PER I FORNITORI)

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 (incluse le società del Gruppo) e il Fornitore (incluse le società del Gruppo, se presenti), che le include tramite riferimento.

1. Controllo dell'accesso ai locali

Il Fornitore deve prendere le misure ragionevolmente necessarie per impedire l'accesso fisico alle attrezzature per il Trattamento dei dati personali da parte di persone non autorizzate come segue:

1.1. Implementare il controllo elettronico dell'accesso agli edifici che ospitano i Dati personali.

1.2. Implementare il controllo elettronico dell'accesso alle aree sensibili all'interno dell'edificio, quali centri dati, stanze telefoniche, armadi LAN e laboratori.

1.3. Assicurare che siano attuate politiche per garantire che solo le persone autorizzate ottengano l'accesso alle aree sensibili, quali centri dati, stanze LAN, armadi telefonici e qualsiasi altro luogo in cui i Dati personali sono elaborati o archiviati. Assicurare che tutti i diritti di accesso a tali aree vengano rinnovati semestralmente.

1.4. Creare e conservare registri di accesso per un minimo di 90 giorni.

1.5. Assicurare che le porte perimetrali e le aree sensibili siano monitorate e registrate tramite CCTV 24 su 24, 7 giorni su 7. Assicurare che tutte le registrazioni CCTV siano conservate per almeno 30 giorni.

1.6. Mantenere un sistema di allarme monitorato in modo attivo che protegga fisicamente le aree sensibili (incluse stanze LAN, laboratori e qualsiasi altra area in cui avverrà il trattamento dei Dati personali).

1.7. Assicurare che ci siano guardie di sicurezza presenti in qualsiasi sito aziendale che tratti Dati personali.

1.8. Assicurare che venga attuata una procedura per convalidare l'identità di un individuo prima di assegnare un badge identificativo.

1.9. I visitatori devono registrarsi e indossare un badge che li identifichi facilmente come visitatori. I visitatori devono essere scortati dallo staff durante la loro presenza presso il sito. Tutti i registri dei visitatori devono essere conservati per un minimo di un anno.

1.10. Limitare e controllare l'accesso al centro dati e alle strutture di archiviazione multimediale contenenti Dati personali per gli appaltatori esterni, quali guardie di sicurezza, servizi di pulizia.

1.11. Mantenere un programma di controllo delle chiavi documentato per la struttura con un registro principale delle chiavi. Le chiavi di armadi, locali delle attrezzature e armadi di cablaggio devono essere tenute sotto adeguata custodia, consegnate solo a personale autorizzato e monitorate per la restituzione.

1.12. Assicurare che i registri di controllo degli accessi siano controllati dall'amministratore per l'attività di allarme, inclusi gli allarmi di apertura o forzatura delle porte.

2. Controllo dell'accesso all'uso del sistema

Al fine di impedire l'accesso remoto alle sue attrezzature o alle applicazioni che trattano i Dati personali da parte di persone non autorizzate, il Fornitore deve prendere le misure ragionevolmente necessarie per attuare e mantenere i seguenti punti:

2.1. assicurare che a ciascun utente di un sistema (rete, server, database, applicazione) venga associato un identificatore univoco.

2.2. Assicurare che la creazione di account e privilegi di accesso richieda l'approvazione della direzione e venga controllata ogni 6 mesi.

2.3. Mantenere un elenco di controllo degli accessi (Access Control List, ACL) per tutti i sistemi contenenti Dati personali e controllarlo regolarmente.

2.4. Applicare la regola dei privilegi minimi e il principio del diritto di conoscere quando concede l'accesso a un utente.

2.5. Applicare la separazione delle funzioni.

2.6. Assicurare che siano attuati processi per sospendere le autorizzazioni di accesso entro 24 ore agli utenti per i quali termina il rapporto di impiego presso il Fornitore (cessazione, trasferimento, ecc.).

2.7. Disattivare gli account degli utenti dopo 90 giorni di inattività ed eliminarli dopo 120 giorni di inattività.

2.8. Assicurare che l'identità di ciascun utente sia verificata quando l'utente tenta di accedere tramite l'utilizzo di password, autenticazione a più fattori o dati biometrici. I tentativi di accesso riusciti e non riusciti devono essere registrati e conservati per 1 anno.

2.9. Impostare il blocco automatico dello schermo con protezione tramite password dopo oltre 20 minuti di inattività.

2.10. Le password degli utenti devono avere una lunghezza minima di 8 caratteri, e contenere almeno un carattere appartenente a 3 categorie diverse su 4 (lettere maiuscole, minuscole, numeri e caratteri speciali).

2.11. Le password degli account amministratore, di servizio e di sistema devono avere una lunghezza minima di 15 caratteri, e contenere almeno un carattere appartenente a 4 categorie diverse su 4 (lettere maiuscole, minuscole, numeri e caratteri speciali).

2.12. Le password devono scadere ogni 90 giorni.

2.13. Le nuove password devono essere differenti dalle ultime 10 password.

2.14. Un account deve bloccarsi automaticamente dopo 5 tentativi di accesso non riusciti.

2.15. Tutte le password predefinite del fornitore e le password di installazione fornite con nuovo hardware, nuovo software di sistema e nuove applicazioni devono essere ripristinate al momento dell'installazione.

2.16. Le password devono essere archiviate e trasmesse in formato crittografato.

2.17. La password e l'ID temporanei iniziali devono essere comunicati in modo protetto. Le password e gli ID non crittografati non devono mai essere inviati nella stessa e-mail.

2.18. Assicurare che l'identità dell'utente sia convalidata prima di consentire la reimpostazione della password o fornire la password agli utenti.

2.19. Standardizzare i server e le versioni e la configurazione del sistema operativo conformemente agli standard del settore in modo che resistano agli attacchi.

2.20. Assicurare che i sistemi che memorizzano o elaborano i Dati personali si trovino su segmenti di rete separati in base all'etichetta o al livello di classificazione delle informazioni memorizzate sui server per garantire che solo le persone autorizzate siano in grado di comunicare con i sistemi necessari per adempiere alle loro specifiche responsabilità.

2.21. Mantenere un processo di gestione delle patch documentato ed eseguire aggiornamenti sui sistemi con vulnerabilità critiche e ad alto rischio entro 2 settimane dal rilascio della patch e entro un mese su tutti gli altri. Inoltre, deve modificare immediatamente ogni patch come richiesto da Avaya.

2.22. Il software antivirus deve essere caricato e operativo su tutti i server e PC. I fornitori che trattano dati personali devono utilizzare altre tecniche di rilevamento di malware ove possibile (per esempio scansione delle e-mail, scansione del file system, scansione del traffico internet, ecc.).

2.23. Il software di scansione antivirus deve essere aggiornato almeno su base giornaliera e deve essere in grado di supportare aggiornamenti di firma urgenti e fuori ciclo.

2.24. Il software antivirus deve essere configurato in modo tale che gli utenti non autorizzati non siano in grado di disabilitarlo. Ove richiesto, persone autorizzate possono diabilitare il software.

3. Controllo dell'accesso ai Dati personali

Il Fornitore deve prendere le misure ragionevolmente necessarie per impedire 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. Mantenere una politica di classificazione e gestione dei dati scritta e un inventario dei dati registrati con una classificazione che indichi la posizione fisica ed elettronica.

3.2. Il Fornitore deve garantire che i Dati personali siano crittografati in transito utilizzando protocolli standard industriali non deprecati; per esempio. SSH/SCP/SFTPV2, TLSv1.2 o superiore.

3.3. Il fornitore deve garantire un livello di crittografia dei Dati personali standard per il settore e adeguato ai rischi presentati dal trattamento dei Dati personali a riposo. Ciononostante, tutti i backup di Dati personali devono essere crittografati su supporti di backup.

3.4. I Dati personali possono essere scaricati su PC del Fornitore, laptop, dispositivo mobile o memoria rimovibile solo se la crittografia del disco rigido è abilitata su tale dispositivo.

3.5. Assicurare la gestione e la rotazione periodica della chiave di crittografia.

3.6. I Dati personali non possono mai essere utilizzati in ambienti di sviluppo, test e/o simulazione, a meno che i Dati personali non siano pseudonimizzati e che tale utilizzo sia autorizzato da Avaya per iscritto.

3.7. Se vengono gestite, archiviate o in altro modo elaborate informazioni di un titolare di carta di credito, i sistemi del Fornitore devono avere la certificazione PCI DSS.

4. Controllo della trasmissione

Il Fornitore deve prendere le misure ragionevolmente necessarie per impedire qualsiasi accesso o modifica non autorizzati ai Dati personali durante la trasmissione attraverso l'implementazione di canali di comunicazione protetti e deve implementare la registrazione delle trasmissioni come segue:

4.1. assicurare che le reti perimetrali siano fisicamente o logicamente separate dalle reti interne contenenti Dati personali.

4.2. Impostare firewall tra: Internet e sistemi di web facing; sistemi di web facing e sistemi applicativi; sistemi applicativi e reti interne. Questi firewall devono essere dispositivi fisicamente separati.

4.3. Utilizza sistemi di rilevamento delle intrusioni di rete (Network Intrusion Detection System, IDS) nell'ambito della strategia di sicurezza della rete in aggiunta ai firewall. Tutti i registri NIDS devono essere monitorati regolarmente per rilevare potenziali tentativi di accesso non autorizzati ai Dati personali.

4.4. I firewall devono essere utilizzati con ispezioni stateful e le regole dei firewall devono essere verificate annualmente.

4.5. Limitare e controllare l'accesso alla rete wireless utilizzando i protocolli di sicurezza wireless standard del settore, con livelli non inferiori a WPA2.

4.6. Limitare e controllare l'accesso alla rete remota e richiedere l'uso della VPN con autenticazione a due fattori.

5. Controllo dell'inserimento

Il Fornitore deve prendere le misure ragionevolmente necessarie per garantire 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. ogni modifica di configurazione su server, reti, database, applicazioni aziendali contenenti Dati personali o modifica a Dati Personali deve essere registrata. I registri dei controlli devono garantire che le azioni possano essere ricondotte a un individuo e devono includere, come minimo, l'ora, la data e il tipo di azione. I registri dei controlli devono essere conservati per 1 anno.

5.2. I registri dei controlli, delle modifiche, degli eventi e del controllo degli accessi devono essere attivamente monitorati e sottoposti a verifica e aggregati centralmente per tutti i sistemi che elaborano o controllano i Dati personali a riposo e in transito utilizzando un meccanismo di raccolta collaudato nel settore, per esempio SIEM. Devono essere creati allarmi per accessi non autorizzati e anomalie. I registri dei controlli e i rapporti di anomalia devono essere forniti su richiesta.

5.3. Mantenere la gestione della configurazione includendo le configurazioni di base della sicurezza.

5.4. Effettuare il monitoraggio per rilevare e generare avvisi per modifiche non autorizzate.

5.5. Assicurare che le modifiche di emergenza richiedano un'approvazione da parte del management di livello appropriato prima della loro implementazione.

5.6. Assicurare che siano stabiliti, comunicati e attuati provvedimenti per le violazioni delle politiche.

6. Controllo dell'organizzazione

Il Fornitore deve prendere le misure ragionevolmente necessarie per programmare l'organizzazione interna in modo tale da soddisfare i requisiti specifici di protezione dei dati e attuare e mantenere le seguenti misure:

6.1. Mantenere una politica scritta per la sicurezza delle informazioni approvata annualmente dal team di gestione dei fornitori e pubblicata e comunicata a tutti i dipendenti del Fornitore e ai soggetti terzi interessati.

6.2. Mantenere una funzione dedicata per la sicurezza e la conformità al fine di progettare, mantenere e gestire la sicurezza a supporto della sua "piattaforma di fiducia" in linea con gli standard del settore. Tale funzione deve concentrarsi sull'integrità del sistema, sull'accettazione del rischio, sull'analisi e la stima dei rischi, sulla valutazione dei rischi, sulla gestione dei rischi e sulle dichiarazioni di applicabilità del trattamento e sulla gestione dei fornitori.

6.3. Sottoporsi regolarmente a revisioni di sicurezza indipendenti di terze parti e fornire rapporti di controllo, quali SSAE16 o ISAE3402.

6.4. Utilizzare servizi di terze parti indipendenti riconosciuti a livello di settore per condurre valutazioni di vulnerabilità e test di penetrazione di reti, sistemi, applicazioni e database in cui i Dati personali sono collocati a riposo, in transito e in uso. Il Fornitore deve classificare le vulnerabilità individuate e risolvere le vulnerabilità critiche entro 4 settimane dal rilascio delle patch e le vulnerabilità elevate secondo i standards del settore.

6.5. Mantenere la protezione dei dati, la consapevolezza della sicurezza e un programma di conformità, procedure e strumenti che affrontino le minacce alla sicurezza delle informazioni e le migliori pratiche; oltre a mantenere in atto politiche procedure e controlli per la sicurezza delle informazioni per proteggere i Dati personali.

6.6. Mantenere e fornire accesso ad Avaya dietro richiesta alle politiche, procedure e strumenti di rendicontazione che forniscano ad Avaya l'accesso alla documentazione pertinente e rapporti sull'attuazione, e, efficacia e se necessario, riparazione delle opportune salvaguardie relative al trattamento dei Dati personali.

7. Controllo della disponibilità

Il Fornitore deve prendere le misure ragionevolmente necessarie per impedire qualsiasi distruzione accidentale o la perdita dei Dati personali tramite misure appropriate, come indicato di seguito:

7.1. monitorare gli eventi di sicurezza e impostare processi di notifica e avviso su tutti i server, reti e database contenenti Dati personali.

7.2. Organizzare un processo di risposta agli incidenti di sicurezza.

7.3. Mantenere politiche, procedure e strumenti di pianificazione di emergenza che definiscano ruoli e responsabilità e forniscano una chiara guida e formazione sulla corretta gestione degli eventi contingenti tra cui: eventi di minaccia naturale, quali inondazioni, tornado, terremoti, uragani e tempeste di ghiaccio; eventi di minaccia accidentale, quali fuoriuscite di sostanze chimiche e guasti meccanici o elettrici; e atti intenzionali, quali violazioni della privacy e della sicurezza, minacce di bombe, aggressioni e furti.

7.4. Disporre di un piano di continuità operativa/di ripristino in caso di disastro per il ripristino dei processi e delle operazioni critiche dei servizi del Fornitore nei luoghi da cui sono forniti i servizi del Fornitore. Il Fornitore deve inoltre disporre di un piano annuale collaudato per supportare la reazione a una catastrofe in modo pianificato e collaudato.

7.5. Implementare e mantenere, in base agli standard del settore, alimentazione elettrica ininterrotta, allarmi antincendio e fumo, sistemi antincendio, generatori, sistemi di raffreddamento e pavimenti sopraelevati presso i data center che elaborano i Dati personali.

7.6. Eseguire backup completi dei database contenenti Dati personali in modo sicuro per assicurarne la disponibilità in linea con la criticità dei dati.

8. Controllo delle risorse

Al fine di assicurare la protezione delle attrezzature o applicazioni che trattano i Dati personali, il Fornitore deve prendere le misure ragionevolmente necessarie per attuare e mantenere le seguenti misure:

8.1. assicurare che siano in atto procedure e strumenti per identificare e tracciare tutte le attrezzature e i supporti utilizzati nel trattamento dei Dati personali.

8.2. Attribuire la responsabilità per tutte le attrezzature e i supporti a uno o più custodi.

8.3. Eseguire una revisione completa annuale dell'inventario delle risorse e un'approvazione dello stesso per verificarne l'accuratezza e identificare i dispositivi e i supporti mancanti.

9. Controllo delle applicazioni

Al fine di assicurare la protezione delle applicazioni che trattano i Dati personali, il Fornitore deve prendere le misure ragionevolmente necessarie per attuare e mantenere le seguenti misure:

9.1. Ove applicabile, prima del rilascio dell'applicazione, eseguire test di entrata e di vulnerabilità delle applicazioni via web e mitigare le vulnerabilità di elevata gravità.

9.2. Condurre test di penetrazione almeno una volta all'anno sul proprio ambiente informatico e fornire ad Avaya copie scritte dei risultati di tali test di penetrazione eseguiti dal Fornitore o dai suoi subappaltatori non più di 30 giorni dopo che il Fornitore ottiene i risultati o i rapporti.

9.3. Laddove le applicazioni (che tratteranno i Dati personali) verranno sviluppate per la fornitura dei servizi del Fornitore ad Avaya, assicurare che gli sviluppatori siano formati sulle migliori pratiche di sviluppo sicuro praticati nel settore.

9.4. Assicurare che le applicazioni che tratteranno i Dati personali siano sviluppate in modo sicuro utilizzando un processo formale e documentato del Fornitore, che fornisca la prova che non siano presenti vulnerabilità della sicurezza delle applicazioni prima di passare alla produzione. Saranno condotti ulteriori test almeno trimestralmente e dopo ogni cambiamento significativo. Come livello minimo, le vulnerabilità della sicurezza delle applicazioni devono includere le SANS Top 20 e le OWASP Top 10.

9.5. Le vulnerabilità della sicurezza delle applicazioni che riguardano i Dati personali devono essere corrette entro un periodo di tempo ragionevole a partire dalla loro identificazione.

9.6. Questi requisiti devono essere convalidati da strumenti quali la scansione dinamica delle applicazioni e/o l'analisi del codice statico.

10. Modifica e separazione del controllo dei dati

Il Fornitore deve prendere le misure ragionevolmente necessarie per implementare e mantenere le seguenti misure di controllo delle modifiche per il trattamento dei Dati personali:

10.1. mantenere processi di gestione delle modifiche che includano la documentazione dello scopo, dell'analisi dell'impatto sulla sicurezza, della pianificazione e dei risultati dei test e dell'autorizzazione del management per tutte le modifiche sui sistemi che trattano Dati personali.

10.2. La configurazione dei sistemi che gestiscono Dati personali deve essere convalidata prima del relativo rilascio nella rete di produzione.

10.3. Le modifiche agli ambienti di produzione contenenti Dati personali devono essere verificate e approvate dal management del Fornitore con la documentazione della disponibilità delle verifiche/approvazioni in caso di controllo.

10.4. Mantenere ambienti di sviluppo, test e simulazione separati fisicamente e/o logicamente dagli ambienti di produzione in cui vengono trattati i Dati personali.

10.5. Il Fornitore deve tenere separati fisicamente o logicamente i database per il trattamento dei Dati personali per Avaya.

- FINE DELLE TOMs -