Misure tecniche e organizzative per la sicurezza dei dati di CSA Group

CSA Group e le sue società controllate e affiliate (collettivamente "CSA Group") si impegnano a proteggere i Suoi dati personali. Noi non condividiamo, vendiamo o accediamo ai dati eccetto per fornirLe i nostri servizi sotto contratto o per finalità cui Lei ha dato il Suo consenso.

Il presente documento riassume le politiche e le prassi sulla sicurezza dei dati che abbiamo implementato come parte del nostro programma di sicurezza. I termini "titolare del trattamento" e "responsabile del trattamento" recano le definizioni a loro assegnate dal Regolamento Generale sulla Protezione dei Dati (UE 2016/679 – RGPD).

Protezione delle nostre sedi fisiche e delle strutture per il trattamento dei dati

I dati personali si trovano su server in centri dati di Livello 1 o superiore (utilizzati dai responsabili dei trattamenti) o in stanze server dedicate e protette situate nelle sedi fisiche di CSA Group. Tutti i responsabili dei trattamenti e le sedi fisiche di CSA Group hanno implementato controlli di sicurezza per evitare che persone non autorizzate accedano fisicamente alle apparecchiature di trattamento dei dati che contengono dati personali. Essi includono l'utilizzo di quanto segue:

- Aree di sicurezza stabilite
- Controlli di autorizzazione all'accesso per dipendenti e terze parti
- Sistemi di allarmi di sicurezza
- Utilizzo di schede ID di prossimità e/o autenticazione biometrica per l'accesso
- Videosorveglianza e/o registri di accesso
- Procedure di accesso per i visitatori

Protezione dei nostri sistemi

CSA Group ha implementato misure per prevenire e rilevare l'intrusione nei suoi sistemi di trattamento dei dati da parte di persone non autorizzate. I controlli di sicurezza includono l'utilizzo di quanto segue:

- Controlli di accesso implementati tramite mansioni lavorative e l'utilizzo di procedure di autorizzazione
- Controlli di accesso privilegiati per amministratori, gestiti separatamente
- Registrazione dell'accesso
- Utilizzo di firewall dell'ultima generazione e restrizioni all'accesso basate sulla rete
- Rilevamento e prevenzione di malware in molteplici punti
- Utilizzo di identità gestite centralmente, password complesse, autenticazione multifattore e certificati digitali
- Monitoraggio delle intrusioni e risposta a violazioni rilevate e altri eventi di sicurezza o operativi

- Monitoraggio della conformità riguardo la sicurezza e scansione delle vulnerabilità
- Aggiornamenti di patch di sistema e aggiornamenti di software di sicurezza
- Valutazioni di terzi e test di penetrazione

Protezione dei nostri dati

L'accesso ai dati personali controllati o trattati da CSA Group o la divulgazione degli stessi sono protetti tramite regole di autorizzazione di accesso e/o crittografia. Le persone autorizzate con accesso ai sistemi contenenti dati personali possono accedere esclusivamente ai dati nelle misure consentite e nell'ambito concesso in base alle loro responsabilità lavorative e per fornire servizi o eseguire le loro mansioni come divulgato ai soggetti dei dati. Se i dati personali controllati da CSA Group vengono trattati da una terza parte, l'accesso ai dati personali deve disporre di controlli equivalenti. Questi controlli comprendono:

- L'accesso controllato ai dati personali tramite regole in base al ruolo, credenziali di accesso univoche e principio del privilegio minimo
- Utilizzo di crittografia durante il trasferimento e in periodi di pausa tramite algoritmi complessi
- Sistemi che mantengono registri di accesso per un ragionevole periodo di tempo
- Formazione e politiche di consapevolezza dei dipendenti sull'utilizzo e l'accesso ai dati personali
- Regolari revisioni di account, privilegi di accesso e attività degli amministratori

Garanzia di disponibilità dei nostri dati

CSA Group ha implementato misure per garantire che i dati personali siano protetti contro la perdita o la distruzione accidentali dovute a potenziali disastri presso i nostri responsabili dei trattamenti. Esse includono:

- Requisiti e contratti di assistenza in materia di prestazioni del sistema, tempo di attività, ridondanza, archiviazione di backup fisicamente separata e ripristino di emergenza, il tutto con adeguati sistemi di sicurezza e controlli dei processi
- Politiche e procedure di backup, programmi di ripristino di emergenza e test correlati
- Monitoraggio della disponibilità in tempo reale di sistemi e reti di applicazione

Gestione dei nostri responsabili dei trattamenti terzi

CSA Group continua a essere responsabile di qualsiasi dato personale elaborato da un responsabile dei trattamenti terzo e ha implementato misure per garantire che questi dati siano protetti almeno allo stesso livello di un trattamento diretto. Oltre a richiedere che il responsabile dei trattamenti esegua le attività descritte in precedenza, CSA Group esegue anche:

- Revisioni di due diligence su controlli di disponibilità e sicurezza del responsabile dei trattamenti, capacità di esecuzione, documentazioni finanziarie e altri rischi
- Revisioni di audit indipendenti o valutazioni del responsabile dei trattamenti
- Verifiche che un meccanismo legale sia stato stabilito per consentire legalmente a CSA Group di trasferire dati personali di residenti dell'Unione europea al responsabile dei trattamenti
- Richieste di stesura chiara di contratti e accordi, incluse clausole specifiche correlate all'uso e alla separazione dei dati e conferma che CSA Group mantenga la proprietà/il controllo esclusivo dei dati
- Gestione del livello di assistenza e utilizzo di manager delle relazioni presso responsabili dei trattamenti di importanza critica