MESSAGENET S.p.A.

MISURE DI SICUREZZA

Il presente documento riporta, come previsto nell'art. 10.4 del contratto, le misure di sicurezza adottate da MESSAGENET in qualità di Responsabile del trattamento di dati personali di cui il Cliente è Titolare.

Le SEDI dove sono conservati i dati adottano le seguenti misure di sicurezza a fronte dei rischi di distruzione anche accidentale, perdita e archiviazione, trattamento, accesso e divulgazione non autorizzati o illeciti:

- presenza di sistemi di allarme antincendio collegati a società di vigilanza;
- accesso selezionato alle aree server;
- misure di prevenzione da incendio e allagamento e da intrusione e furto (accesso selezionato, videosorveglianza, antifurto e vigilanza) a protezione del datacenter dove risiedono i server dei sistemi di produzione.

Le RETI, i SISTEMI e gli APPLICATIVI che conservano e trattano tali dati adottano le seguenti misure di sicurezza a fronte dei rischi di distruzione anche accidentale, perdita e archiviazione, trattamento, accesso e divulgazione non autorizzati o illeciti:

- centralità del database come sorgente di tutte le informazioni e backup dei database, replicati su più sedi;
- penetration test effettuato periodicamente;
- uso di firewall, antivirus, rete sezionata ove necessario;
- linee guida per lo sviluppo che contengono elementi di prevenzione di SQL injection e buffer overflow;
- uso, ove possibile, di programmi con accessi non privilegiati (non-root) e con stratificazione dei controlli (uso di API di mediazione);
- procedure di registrazione e assegnazione delle credenziali di accesso degli utenti che prevedono un'identificazione tramite la verifica di un numero di cellulare o di un documento di identità verificato anche sul sito della Polizia di Stato;
- rimozione dei dati dai dischi prima dello smaltimento e distruzione di CD e DVD nel trita documenti

Inoltre gli incaricati al trattamento di tali dati devono rispettare, oltre a tutti gli obblighi indicati nell'art. 10.4 del contratto e alle misure di sicurezza previste per legge, anche le seguenti policy:

- sui dispositivi mobili (PC portatili, smartphone ecc.) non è consentita la copia di dati personali
- rispetto ai rischi di social engineering, la policy data agli incaricati nei confronti di richieste esterne è molto rigida e obbliga in modo stretto a non fornire alcun dato personale se non a fronte di un preventivo accertamento dell'identità degli interlocutori, in qualsiasi contesto
- per quanto possibile date le ridotte dimensioni aziendali, è prevista la separazione dei ruoli in modo che nessuno abbia accesso completo ai diversi sistemi aziendali.
- è consentito l'uso esclusivo di strumenti interni all'azienda o approvati dall'azienda per trattare dati personali (es: NO gmail, NO dropbox, NO altri sistemi cloud-based senza che vi sia un contratto con adeguate garanzie tra l'azienda ed il fornitore)
- utilizzo di sistemi client costruiti e controllati in modo da massimizzarne la sicurezza (uso con credenziali non privilegiate; hardening dei client)
- policy sulle credenziali di accesso degli incaricati:
    - devono essere modificate regolarmente - e comunque al massimo ogni 6 mesi, ovvero ogni 3 mesi qualora siano trattati dati sensibili;
    - devono essere costituite da almeno 8 caratteri alfanumerici;
    - devono essere custodite con assoluto riserbo;

    - non devono contenere riferimenti agevolmente riconducibili al dipendente;
- è fatto esplicito divieto di utilizzare le credenziali di tutti i sistemi che trattano dati personali su sistemi differenti di qualsiasi genere ed è severamente vietato l'utilizzo delle credenziali utilizzate in azienda per usi extra lavorativi.
- qualsiasi credenziale usata nei sistemi di test deve essere differente dalle credenziali utilizzate in produzione.

Ricorso ad altri responsabili

MESSAGENET, per effettuare i trattamenti per conto del Titolare, ricorre ai seguenti responsabili, nominati a tal fine e sottoposti agli stessi obblighi in materia di protezione dei dati stabiliti dal contratto, pretendendo le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della legge e del Regolamento:

- KPNQWest Italia Srl per:
    - Data centre fisico
    - Servizio Messagenet Box

Misure di sicurezza in capo al Titolare

Il Cliente disporrà di credenziali di accesso, costituite da user-id e password, che potranno essere rigenerate in qualsiasi momento. Spetta al Cliente scegliere password robuste e mantenerle riservate.