Politica sulla Sicurezza delle Informazioni

Politica sulla Sicurezza delle Informazioni

Introduzione

Il 25 maggio 2018, il Regolamento Generale sulla Protezione dei Dati (GDPR) è diventato legge in tutti gli Stati dell'Unione Europea ed è progettato per offrire una legislazione efficace per l'elaborazione dei dati del 21° secolo. I principi fondamentali sono in gran parte i medesimi della Legge sulla protezione dei dati italiana (D.Lgs. 196/2003 c.d. Codice Privacy), tuttavia il GDPR ha inserito cambiamenti e miglioramenti chiave che è importante comprendere.

In questo documento, ti guideremo attraverso alcuni punti chiave del GDPR e come la Società li ha implementati in qualità di Responsabile del Trattamento dei tuoi dati. Si prega di notare che questo documento descrive solo come la Società gestisce i dati in qualità di Responsabile del trattamento. A scanso di equivoci, questi ultimi sono i dati che trasferisci alla Società allo scopo di trasmettere le tue comunicazioni o per permettere alla Società di fornirti i servizi richiesti. Tali dati saranno indicati in questo documento come dati dell'utente finale, ossia dati che tu controlli e che affidi alla Società affinché vengano trattati per tuo conto. Se desideri informazioni su come la Società tratta i tuoi dati in qualità di Titolare del Trattamento, puoi visualizzare la nostra Informativa Privacy sul nostro sito web.

Consenso

Il Consenso è una delle basi legali per il Trattamento dei dati. Ai sensi del GDPR, i requisiti per l'utilizzo del consenso come base legale sono molto elevati. Il consenso deve essere ottenuto, registrato e gestito in modo completo.

Il servizio che ti forniamo significa che la Società è il Responsabile del trattamento dei dati che condividi con noi ai fini della trasmissione delle comunicazioni e tu sei il Titolare del trattamento. La Società agisce esclusivamente in base alle tue istruzioni ed elabora i tuoi dati per inviare comunicazioni ai tuoi utenti finali.

La Società non ottiene, registra o gestisce il consenso degli interessati per conto dell'utente. È, quindi, tua responsabilità in qualità di Titolare del trattamento assicurarti di avere e di poter dimostrare, ove necessario, di avere ottenuto dagli interessati il consenso necessario per trasmettere le comunicazioni utilizzando le informazioni fornite. La Società non interagisce direttamente con i tuoi utenti finali: tutte le comunicazioni

vengono inviate su tue istruzioni come se provenissero direttamente da te e la Società è trasparente nel processo di consegna delle comunicazioni.

Sistemi informativi

I sistemi informativi della Società si basano su un sistema sviluppato internamente per la raccolta e il trattamento dei Dati dei Clienti e dei Destinatari.

La Società e, all'interno di essa, ciascuna funzione, utilizzano un sistema di gestione dei flussi informativi coordinati tra loro. L'interconnessione avviene attraverso linea VPN.

I Data Center della Società sono in outsourcing presso:

1. Brennercom S.p.a. - Sede datacenter: Via Ernesto Sestan 5 - 38121 Trento (TN);
2. BT Italia SPA - Sede datacenter: Via Darwin, 85 - 20019 Settimo Milanese (MI).

Ciascun Data Center ospita server, storage, gruppi di continuità e tutte le apparecchiature che consentono di governare i processi, le comunicazioni, i servizi che supportano qualsiasi attività aziendale. I Data Center garantiscono il funzionamento 24 ore al giorno, tutti i giorni dell'anno, di qualsiasi sistema informativo, sono dotati di tutti i sistemi di sicurezza fisica e logica previsti dal Codice Privacy e sono certificati ANSI/TIA/EIA-942 (Tier 4) e ISO/IEC/27001.

Conservazione dei dati

La Società è consapevole che un'eccessiva conservazione dei dati non è conforme sia alle vecchie sia alle nuove regole sulla protezione dei dati. Di conseguenza, la Società conserva i tuoi dati di messaggistica per non più di due anni dalla data in cui hai inviato la comunicazione, salvo diversa disposizione di legge.

Tutti i campi contenenti dati di identificazione personale vengono oscurati dopo il periodo di conservazione, prima di essere eliminati definitivamente. I dati di messaggistica sono limitati al numero di cellulare e al contenuto del messaggio.

L'archiviazione dei dati di identificazione personale avviene in ambienti protetti (c.d. Server Farm), con accesso controllato, separati da tutte le altre reti della Società. L'hardware all'interno di questi ambienti protetti è di proprietà della Società.

Ogni sei mesi viene eseguita una verifica periodica per la cancellazione dei Dati per i quali sia decorso il termine di conservazione e che non siano stati cancellati dai sistemi automatici. La verifica per la cancellazione automatica dei Dati avviene ogni 24 ore.

Le informazioni e i Dati di cui la Società venga a conoscenza in ragione dell'utilizzo dei Servizi da parte dei Clienti (quali, a titolo esemplificativo ma non esaustivo i Dati Relativi al Traffico e il contenuto degli SMS/MMS e e-mail) sono conservati in conformità all'espresso consenso prestato con il contratto dal Cliente (artt. 122 e 123 del Codice Privacy e art. 7 GDPR), per un periodo non superiore a 24 mesi per finalità di:

a) di accertamento e repressione di reati;

b) di documentazione in caso di contestazione della fattura o per la pretesa del pagamento anche in sede giudiziale;

c) di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto;

d) di consultazione da parte del Cliente o dei Clienti Finali;

e) di organizzazione interna, di interventi di manutenzione e di rilevamenti statistici, oltre che per soddisfare eventuali richieste di consegna e/o visualizzazione dei dati avanzate da soggetti autorizzati quali, a titolo esemplificativo, autorità amministrative, giudiziarie o forze di pubblica sicurezza.

Misure di protezione dei dati

Aree e locali

I locali nei quali si svolge il trattamento, presso le sedi della Società, sono protetti da dispositivi antincendio, gruppo statico di continuità (UPS) e impianto di condizionamento.

I Server presso i Data Center sono protetti da ogni dispositivo di sicurezza previsto dalla vigente normativa.

Custodia e archiviazione di atti, documenti e supporti

Agli incaricati sono state date disposizioni, per iscritto, di accedere ai soli Dati Personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati e di rivolgersi al Responsabile Interno del Trattamento in caso di dubbio.

Gli incaricati possono prelevare dagli archivi i soli atti e documenti loro affidati per lo svolgimento delle rispettive mansioni, con l'obbligo di controllarli e custodirli, durante il trattamento, e di restituirli al termine, riponendoli negli archivi.

Atti e documenti sono conservati in appositi armadi o cassetti con serratura.

Misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici, anche attraverso l'uso dei Data Center, la Società ha adottato le seguenti misure:

a) realizzazione e gestione di un sistema di autenticazione informatica in grado di accertare l'identità dell'utilizzatore, di modo che a ogni strumento elettronico possa accedere solo il soggetto autorizzato;

b) realizzazione e gestione di un sistema di autorizzazione che limita l'accesso degli Incaricati ai soli dati e trattamenti strettamente necessari per lo svolgimento delle relative mansioni;

c) realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi;

d) prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili.

Sistema di Autenticazione

Il Sistema di Autenticazione regola gli accessi a tutti gli strumenti elettronici secondo quanto segue:

a) l'amministratore di sistema assegna a ciascun Incaricato un codice per l'identificazione (username), mentre ciascun Incaricato crea una parola chiave (password), obbligandosi a mantenerla riservata e a modificarla come di seguito specificato; username e password rappresentano le Credenziali per l'accesso al sistema;

b) a ogni incaricato corrisponde una sola coppia di username e password, di modo che non sia possibile che due Incaricati possano accedere agli strumenti elettronici utilizzando le medesime Credenziali;

c) ciascun Incaricato si obbliga:

    1. a custodire con diligenza i dispositivi attribuitigli in uso esclusivo, sia all'interno sia all'esterno degli uffici della Società;

2. in caso di smarrimento, a segnalare immediatamente la circostanza all'amministratore di sistema e al superiore gerarchico ovvero, o all'eventuale diverso soggetto indicato al momento dell'attribuzione del dispositivo;

3. a non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza (impostazione di salvaschermo con sblocco mediante Credenziali);

4. modificare la password al primo accesso e, comunque, almeno ogni sei mesi (tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari);

5. elaborare la password secondo le indicazioni dell'amministratore di sistema;

6. mantenere username e password riservate e garantirne la segretezza.

7. Periodicamente, e comunque almeno una volta ogni 12 mesi, l'Amministratore di Sistema verifica la sussistenza delle condizioni per la conservazione e rinnovo delle Credenziali.

Malfunzionamenti, attacchi informatici e Virus

La protezione di strumenti e dati da malfunzionamenti, attacchi informatici e programmi che contengono codici maligni è regolata dalle seguenti misure.

a) per la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'art. 615 quinquies c.p. (danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento), la Società, anche attraverso i Data Center, si è dotata di idonei strumenti elettronici e programmi di protezione che vengono costantemente aggiornati;

b) gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere per minimizzare il rischio di contagio;

c) la protezione degli elaboratori in rete dall'accesso abusivo di cui all'articolo 615 ter c.p. (introduzione abusiva in un sistema informatico o telematico, protetto da misure di sicurezza) avviene mediante l'impiego di sistemi di protezione (adottati anche dai Data Center) che difendono gli elaboratori della rete aziendale collegata a Internet da accessi non autorizzati (firewall);

d) la protezione da malfunzionamenti degli strumenti elettronici avviene mediante l'utilizzo di programmi per prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere i difetti insiti negli strumenti stessi.

Supporti rimovibili

I supporti rimovibili (chiavette USB, HD esterni, CD-ROM, DVD, dischi riscrivibili ecc.) sono custoditi e utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti. In particolare, sono conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati.

Una volta cessate le ragioni per la conservazione, i Dati sono cancellati dai supporti, e i supporti sono formattati o distrutti, di modo che i Dati siano inintelligibili e non ricostruibili tecnicamente.

Data Recovery

Per salvaguardare il recupero dei dati da danneggiamento, distruzione o perdita, anche accidentale vengono adottate le seguenti misure:

a. i documenti cartacei, e gli eventuali supporti diversi da quelli elettronici, contenenti dati personali sono periodicamente digitalizzati e i relativi supporti, ove applicabile, vengono archiviati;

b. per i trattamenti effettuati con strumenti elettronici si utilizzano sistemi RAID e procedure di backup, attraverso cui viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, affidate ai Data Center, protetti da sistemi di controllo ambientale (condizionamento, impianti antincendio, ecc.) nonché da dispositivi di sicurezza fisici (porte blindate, videosorveglianza, allarmi, gruppi di continuità, ecc.) e logici (firewall, back-up, antispyware ecc.), con certificazione ISO/IEC/27001;

c. per gli eventi catastrofici è prevista una procedura di ripristino dati partendo dall'ultimo back-up effettuato;

d. la continuità operativa è garantita localmente, oltre che dai sistemi approntati dai Data Center, da gruppi statici di continuità (UPS);

e. esecuzione periodica di prove di ripristino e di test di salvataggio.

Controlli sulla sicurezza

Il Responsabile Interno del Trattamento aggiorna le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, o di accesso non autorizzato o di trattamento non consentito. A tale fine, ogni sei mesi si tiene una riunione tra il Titolare, il Responsabile Trattamento e le altre figure apicali.

In ogni caso, al fine di verificare l'efficacia delle misure di sicurezza adottate, il Responsabile Interno del Trattamento, con l'ausilio dell'amministratore di sistema, provvede periodicamente, anche con controlli a campione, a eseguire una o più delle seguenti attività:

a. verificare l'accesso fisico ai locali dove si svolge il trattamento;

b. verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti Dati Personali;

c. monitorare l'efficacia e il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli Incaricati, anche con l'adozione di strumenti automatici di reportistica e di sintesi, al fine di individuare eventuali tentativi di accesso illecito al sistema o l'esecuzione di operazioni non corrette, o sospette;

d. verificare l'integrità dei Dati e delle copie di backup;

e. verificare la sicurezza delle trasmissioni in rete;

f. verificare che i supporti rimovibili non riutilizzati o riutilizzabili vengano distrutti, ove sia venuta meno la necessità della loro conservazione;

g. verificare il livello di formazione degli Incaricati;

h. verificare il corretto utilizzo delle Credenziali, anche al fine di aggiornare password eventualmente scadute o disabilitare Credenziali non più utilizzate.

Dati in transito / crittografia

Tutti i trasferimenti di informazioni sugli utenti finali dei clienti da hardware e reti di proprietà e controllati dalla Società avvengono tramite connessioni VPN, questo è il modo in cui i dati vengono trasmessi agli operatori di rete per la consegna delle comunicazioni

Le connessioni da te ai nostri sistemi sono protette a seconda del metodo utilizzato:

Se ti connetti a noi utilizzando le nostre applicazioni web, ti consigliamo di utilizzare la connessione TLS 1.2.

Se si utilizza un'automazione SFTP per trasferire file, questa è protetta tramite SSH.

Se ti connetti a noi utilizzando una delle nostre API, la sicurezza della connessione dipenderà dalla tua integrazione, ti consigliamo vivamente di utilizzare HTTPS nella tua integrazione con noi, piuttosto che HTTP.

Monitoraggio

La nostra piattaforma è costantemente monitorata dal nostro team operativo. La Società dispone di un team di reperibilità dedicato che garantisce che tutte le piattaforme siano monitorate 24 ore su 24, 7 giorni su 7, 365 giorni l'anno, qualsiasi problema venga sollevato con le parti interessate e sarà soggetto alle nostre solide procedure di gestione degli incidenti per garantire che la piattaforma rimanga sicura e priva di errori.

Sosteniamo i mezzi di segnalazione delle vulnerabilità del settore ed esaminiamo regolarmente tutte le vulnerabilità note del settore, valutando quotidianamente le nuove minacce. Laddove scopriamo che stiamo utilizzando un componente potenzialmente vulnerabile, questo rischio viene valutato nel contesto delle nostre operazioni aziendali e dell'ambiente e, se appropriato, correggeremo il problema il prima possibile.

Disponiamo di processi per garantire che tutte le apparecchiature per l'archiviazione dei dati vengano distrutte fisicamente e in sicurezza alla fine del loro ciclo di vita, non ricicliamo i supporti e conserviamo copie dei certificati di distruzione dei supporti del nostro fornitore certificato e di fiducia.

Conduciamo test di penetrazione su base annuale utilizzando un fornitore terzo certificato. Inoltre, eseguiamo scansioni di vulnerabilità interne ed esterne utilizzando fornitori di scansioni autorizzati e applicazioni di valutazione delle vulnerabilità.

I sistemi informativi della Società, poi, sono sottoposti annualmente a un "Cyber Security Assessment" da parte della Capogruppo Commify UK Ltd e da parte di alcuni clienti.

Formazione e istruzione dei dipendenti

Tutti i dipendenti sono soggetti a un rigoroso controllo preliminare all'assunzione in linea con la nostra politica di assunzione, devono completare con successo i test attitudinali e fare eseguire una serie di controlli prima che venga presentata un'offerta completa di lavoro. Questi controlli includono: istruzione, occupazione, diritto al lavoro. Ulteriori controlli sono richiesti per determinati ruoli (es. legati alla finanza).

Tutti i dipendenti, poi, vengono formati sull'importanza della sicurezza dei dati e apprendono le misure che devono adottare per proteggere i dati personali, aziendali e dei clienti come parte del loro processo di assunzione e regolarmente come parte della nostra continua iniziativa di e-learning.

Tutto il personale, infine, ha obblighi di riservatezza chiaramente definiti come parte del contratto di lavoro.

Rischi

La Società valuta continuamente tutti i rischi relativi sistemi, personale, risorse e attività operative. Le valutazioni del rischio descrivono in dettaglio i piani di trattamento che fungono da raccomandazioni per aiutare l'azienda a ridurre l'impatto e / o la probabilità del rischio identificato. I rischi e i piani di trattamento vengono riesaminati regolarmente.

Le componenti di rischio relative sono:

a. rischio di area - dipende dal luogo ove gli strumenti sono ubicati ed è legato ai seguenti fattori:

   i. verificarsi di eventi distruttivi (incendi, allagamenti, cortocircuiti);

   ii. accesso da parte di terzi malintenzionati ai locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici);

b. rischio guasti tecnici - interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti);

c. rischio di penetrazione logica nelle reti di comunicazione;

d. rischio di sabotaggio e errore umano.

Violazione dei dati

La Società adotta tutte le misure di cui sopra per proteggere i tuoi dati come parte delle nostre attività di elaborazione dei dati. La Società, infatti, è dotata di una procedura per la gestione delle violazioni di dati personali (*Data Breach*). In caso di violazione dei dati, ti informeremo entro 24 ore dal momento in cui siamo venuti a conoscenza di qualsiasi problema di sicurezza che abbia portato a una violazione dei dati, inclusi i dati dei clienti.

La Società, inoltre, dispone di misure di sicurezza implementate nei nostri sistemi IT, reti e pratiche aziendali generali per rilevare e rispondere ai problemi di sicurezza in modo efficace.

Responsabile della protezione dei dati

La Società dispone di un team dedicato che risponde a tutte le domande, richieste, problemi relativi alla protezione dei dati. La Società, inoltre, ha nominato, come richiesto dal GDPR, un Responsabile della Protezione dei Dati (RDP – DPO).

Qualsiasi domanda tu abbia in relazione alla protezione dei dati puoi rivolgerti al tuo account manager, o al team di supporto.

Trasferimenti di dati

La Società trasmette le tue informazioni agli operatori telefonici (o di rete secondo i casi) allo scopo di consegnare la tua comunicazione al telefono degli utenti finali o all'apparecchiatura di terminazione di rete. Questo tipo di trasferimento è intrinseco alla fornitura dei nostri prodotti e servizi.

Per la comunicazione SMS in Italia utilizziamo solo le nostre connessioni dirette alle reti mobili italiane per garantire che possiamo rintracciare i tuoi dati dai nostri sistemi al telefono dell'utente finale.

Per tutte le reti di terze parti che utilizziamo (es. per la consegna di SMS all'estero), abbiamo condotto un audit per garantire che ogni fornitore abbia adottato misure tecniche e organizzative adeguate richieste per offrire standard di sicurezza sostanzialmente simili a quelli descritti in questo documento per la nostra infrastruttura.

Abbiamo anche stipulato (o stiamo per concludere) contratti con tutte le terze parti che consolidano gli obblighi di protezione dei dati di tutte le parti ed estendono i requisiti

minimi dettagliati in qualsiasi Accordo sul trattamento dei dati tra te e noi ai nostri fornitori.

Accordi sul trattamento dei dati

La Società ha un Accordo standard sul trattamento dei dati (DPA) che può essere utilizzato dai nostri clienti per garantire il rispetto dei propri obblighi in qualità di titolare del trattamento ai sensi del GDPR. Il nostro DPA è disponibile su richiesta del tuo account manager e fa parte, come allegato, delle Condizioni Generali di Contratto che sono disponibili sul sito https://www.mobyt.it.

Valutazione dell'impatto sulla protezione dei dati (DPIA)

Comprendiamo che alcuni tipi di trattamento possono richiedere ai nostri clienti di completare una DPIA per dimostrare di aver considerato i diritti e le libertà degli interessati prima di impegnarsi nelle attività di trattamento proposte. La Società è un fornitore di servizi per comunicazioni aziendali e non ha visibilità del contenuto che invii tramite la nostra piattaforma. Se le tue attività di trattamento sono considerate ad alto rischio o stai trattando categorie speciali di dati, potresti richiedere il nostro contributo alla tua DPIA. Si prega di inoltrare eventuali richieste di questo tipo al proprio account manager.

Aggiornata a Settembre 2020