GDPR - la protezione dei dati personali

GDPR

Il Regolamento Generale sulla protezione dei dati (GDPR) è il quadro giuridico per il trattamento dei dati personali in Europa che introduce requisiti rigorosi che definiscono nuovi standard in materia di compliance, sicurezza e protezione dei dati.

CoreTech e il GDPR

Oltre a garantire la propria conformità, **CoreTech si impegna a offrire servizi e risorse in grado di consentire ai clienti di conformarsi agli eventuali requisiti del GDPR** a cui sono tenuti ad adeguarsi in merito alle loro attività. A tal proposito CoreTech ha rilasciato nuove funzionalità ed altre lo saranno.

Data Center in Italia

CoreTech è un azienda 100% italiana e i data center si trovano in Italia.

CoreTech è membro CISPE

CoreTech ha recentemente annunciato la propria conformità con il Codice di condotta del CISPE di cui sono membri anche Amazon AWS, Aruba, Register e OVH.
Il codice di condotta CISPE consente ai clienti del cloud di valutare la conformità del loro fornitore di infrastrutture cloud agli obblighi di protezione dei dati sotto il GDPR.
Questo rassicura ulteriormente i clienti riguardo alla loro capacità di controllare i loro dati in un ambiente protetto, sicuro e conforme.

Definizione del GDPR

Al fine di evitare errate interpretazioni degli obblighi normativi, di seguito vengono definite le espressioni essenziali per comprendere il GDPR:

- **dati personali**: qualsiasi informazione relativa a una persona fisica identificata o identificabile, cioè l'interessato. È considerata una persona fisica identificabile una persona fisica che può essere identificata, direttamente o indirettamente.
- **trattamento**: qualsiasi operazione o insieme di operazioni eseguite con o senza il supporto di processi automatizzati e applicate a dati o insiemi di dati personali (raccolta, registrazione, trasmissione, storage, conservazione, datamining, consultazione, utilizzo, interconnessione, ecc...).

- **Responsabile del trattamento dei dati**: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, da solo o con altri soggetti, determina i mezzi e le finalità del trattamento. Nel testo del GDPR viene indicato come titolare del trattamento dei dati.
- **Incaricato del trattamento dei dati**: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del responsabile del trattamento. Nel testo del GDPR viene indicato come responsabile del trattamento dei dati.

CoreTech come incaricato del trattamento dei dati

Questo è certamente il caso in cui le tue aspettative su CoreTech sono più incisive. CoreTech riveste il ruolo di "incaricato del trattamento" quando tratta dati personali per conto di un responsabile del trattamento.
È la situazione che si verifica quando si utilizzano i servizi CoreTech e si archiviano i dati personali su un'infrastruttura CoreTech. Entro i limiti dei suoi vincoli tecnici, CoreTech tratterà i dati ospitati esclusivamente secondo le tue indicazioni, e per tuo conto.

L'impegno di CoreTech in qualità di incaricato del trattamento dei dati

Nel ruolo di incaticato del trattamento dei dati, CoreTech si impegna in particolare a eseguire le seguenti azioni:

- **trattare i dati personali esclusivamente ai fini della corretta esecuzione dei servizi**: CoreTech non utilizzerà mai le tue informazioni per altri scopi (marketing, ecc...)
- **non trasferire i tuoi dati al di fuori dell'UE** o al di fuori di Paesi riconosciuti dalla Commissione Europea come possessori di un livello di protezione insufficiente
- **informarti di qualsiasi eventuale ricorso ad altri incaricati che potrebbero trattare i tuoi dati personali** anche se, ad oggi, nessun servizio che preveda l'accesso ai contenuti archiviati dall'utente viene esternalizzato al di fuori di CoreTech
- **implementare standard elevati di sicurezza** al fine di garantire un alto livello di sicurezza ai nostri servizi
- **avvisarti il prima possibile** in caso di violazione dei dati
- **assisterti nell'adempiere ai tuoi obblighi normativi** fornendoti un'adeguata documentazione dei nostri servizi

CoreTech come responsabile del trattamento dei dati

CoreTech riveste il ruolo di "responsabile del trattamento dei dati" quando determina i mezzi e le finalità del "proprio" trattamento di dati personali.

È il caso in cui CoreTech raccoglie i dati per fatturazione, miglioramento del servizio e delle prestazioni, operazioni di vendita, gestione commerciale, ecc..., ma anche quando CoreTech tratta i dati personali dei propri dipendenti. In questo caso, i "tuoi" dati ospitati sui servizi CoreTech, non sono interessati, diversamente da alcune informazioni che riguardano te o i tuoi dipendenti (ad esempio informazioni relative a identità e coordinate del tuo contatto in CoreTech nell'ambito di una richiesta di Supporto). Questo è il motivo per cui CoreTech ci tiene a spiegare le garanzie messe in atto per assicurare la protezione di questi dati personali:

- **limitare la raccolta dei dati a quelli strettamente necessari**: così facendo, quando si ordina un servizio si inseriscono soltanto i dati richiesti da CoreTech per fornire prestazioni relative alla fatturazione, all'assistenza o adempiere agli obblighi legali nell'ambito della conservazione dei dati
- **non utilizzare i dati personali per scopi diversi** da quelli per cui sono stati originariamente raccolti
- **conservare i dati personali per un periodo limitato**. Ad esempio, i dati trattati per scopi relativi alla gestione delle relazioni tra i clienti e CoreTech (cognome, nome, indirizzo, email, ecc...), sono conservati dall'azienda per l'intera durata del contratto e i successivi 36 mesi. Alla fine di questo periodo, vengono definitivamente cancellati da tutti i supporti e backup
- **non trasferire questi dati a terzi** che non facciano parte delle società collegate a CoreTech che sono coinvolte nell'esecuzione del contratto. Durante le migrazioni all'interno del Gruppo, alcuni dati possono essere trasferiti al di fuori dell'Unione Europea sulla base delle regole aziendali implementate dal Gruppo CoreTech
- **implementare adeguate misure tecniche e organizzative** al fine di garantire un alto livello di sicurezza

Misure di sicurezza

È essenziale distinguere tra la sicurezza dei dati ospitati dal cliente e la sicurezza delle infrastrutture che ospitano questi dati.

Sicurezza dei dati ospitati dal cliente

il cliente è l'unico responsabile della sicurezza delle proprie risorse e dei sistemi applicativi implementati per l'utilizzo dei servizi. CoreTech mette a disposizione degli strumenti per supportare il cliente nella protezione dei propri dati. Ogni servizio ha i suoi strumenti specifici; di seguito alcuni di essi:

- Backup Granulare dei dati (di servizi specifici)
- Backup istanze server (per server cloud)
- Logging delle attività (a servizi specifici)
- Logging degli accessi (alla piattaforma)
- Agent di monitoraggio Sygma (per server cloud)
- Ticket System per tracciatura comunicazioni

Sicurezza delle infrastrutture

CoreTech si impegna a garantire la massima sicurezza delle proprie infrastrutture, in particolare implementando una politica di sicurezza dei sistemi informativi e rispondendo alle esigenze di numerose leggi e certificazioni. CoreTech adotta le misure necessarie per preservare la sicurezza e la riservatezza dei dati personali trattati, in particolare per impedire che vengano violati, danneggiati o che soggetti terzi non autorizzati vi accedano.

CoreTech si impegna in particolare a implementare:

- **misure di sicurezza fisica** per impedire a persone non autorizzate di accedere alle infrastrutture sulle quali sono archiviati i dati del cliente
- **personale di sicurezza** incaricato di garantire la sicurezza fisica dei locali CoreTech 24 ore su 24, 7 giorni su 7
- **un sistema di gestione delle autorizzazioni** per permettere di accedere ai locali e ai dati soltanto alle persone che ne hanno necessità nell'ambito della loro attività
- **un sistema fisico e/o logico per mantenere separati i clienti tra di loro** (a seconda dei servizi)
- **forti processi di autenticazione per utenti e amministratori** grazie a una severa politica di gestione delle password
- **processi e dispositivi per tracciare tutte le azioni eseguite sul proprio sistema informativo** e, in conformità con le norme vigenti, segnalare eventuali incidenti che riguardino i dati dei clienti

RESPONSABILITÀ CONDIVISA

Cosa si intende per responsabilità condivisa?

In riferminto alla conformità e sicurezza dei dati, sia CoreTech che il cliente sono entrambi responsabili anche se su fronti diversi.
CoreTech si occuperà quindi della manutenzione, dell'aggiornamento e della protezione dell'infrastruttura fisica su cui vengono eseguiti tutti i servizi cloud.
Solo su richiesta esplicita del cliente o al rilascio delle password di accesso, CoreTech potrà intervenire a livello tecnico sul servizio acquistato.

Qui sotto, in base al servizio CoreTech utilizzato, sono riportate nel dettaglio le competenze di responsabilità condivisa. Invitiamo tutti i clienti a prendere visione delle proprie responsabilità in relazione ai servizi utilizzati.
CoreTech si impegna ad applicare tutti gli standard di riferimento per garantire la sicurezza delle informazioni.

Server Cloud

CoreTech

- Mantenere l'infrastruttura software aggiornata con le versioni dei software più stabili e sicuri rilasciate dal produttore
- Tenere sotto monitoraggio l'infrastruttura dei sistemi di virtualizzazione, hypervisor e storage al fine di garantire la continuità di servizi
- Controllare la presenza di eventuali anomalie relative alla sicurezza che si evidenzino attraverso i log o alert del sistema

Cliente

- Impostare delle password di accesso al server e ai software in esso installato con livello di difficoltà conforme alle policy definite e cambio password secondo gli standard di riferimento (es ISO 27002)
- Custodire con cura i dati di accesso ai server e limitarne la divulgazione
- Intervenire tempestivamente in caso di segnalazioni da parte di CoreTech su problemi inerenti la sicurezza del proprio server

- Disattivazione del servizio se a seguito di segnalazione da parte di altri service provider, il server stesse attuando dei comportamenti anomali (spam, phishing, contenuti inerenti al terrorismo, frode, sito hackerato)
- Informare il cliente in caso durante il monitoraggio o le analisi dei log dovessero essere riscontrati problemi sul server

- Configurare correttamente i job di backup dei propri dati con gli strumenti messi a disposizione da CoreTech e chiedere supporto in caso di dubbi sulle configurazioni
- Verificare giornalmente gli esiti dei backup dei dati
- Verificare periodicamente il corretto funzionamento del backup della VM consultando gli esiti dal pannello Sygma
- Organizzare periodicamente con CoreTech i test di restore della VM al fine di accertarsi della corretta esecuzione dei backup della VM
- Controllare periodicamente i registri eventi e log dei sistemi operativi presenti sul proprio server al fine di prevenire eventuali problemi
- Informare tempistivamente CoreTech in caso di anomalie che possano determinare un problema di sicurezza dei dati

Web Hosting

CoreTech

- Controllo giornaliero dei Backup. La retention dei backup è di 35 giorni (5 settimane)
- Mantenere i server di Web Hosting aggiornati con le versioni dei software più stabili e sicuri rilasciate dal produttore
- Verifica giornaliera relativamente allo stato di aggiornamento dell'antivirus integrato
- Tenere sotto monitoraggio il server web al fine di garantire la continuità di servizio
- Controllare la presenza di eventuali anomalie relative alla sicurezza che si evidenzino attraverso i log o alert del sistema
- Informare il produttore dei software attinenti ai web server qualora venga a conoscenza di falle relative alla sicurezza del sistema
- Disattivazione del servizio se a seguito di segnalazione da parte di altri service provider, il sito si sta comportando in modo anomalo (spam, phishing, contenuti inerenti al terrorismo, frode, sito hackerato)

Cliente

- Impostare delle password di accesso al pannello di gestione Plesk, al sito FTP o al sistema di gestione del sito web (esempio accesso admin di WordPress) con livello di difficoltà conforme alle policy definite e cambio password secondo gli standard di riferimento (es ISO 27002)
- Custodire con cura i dati di accesso Plesk, FTP e sito web e limitarne la divulgazione
- Intervenire tempestivamente in caso di segnalazioni da parte di CoreTech su problemi inerenti la sicurezza del proprio sito web
- Procedere ad aggiornate periodicamente gli elementi attinenti la sicurezza del proprio sito web (ad esempio aggiornamento della versione di WordPress)
- Effettuare almeno una volta al mese un backup personale del proprio sito web
- Verificare periodicamente la funzionalità integrata di Restore dei dati del proprio sito web
- Controllare settimanalmente eventuali anomalie relativamente all'utilizzo di risorse del proprio sito qeb
- Informare tempistivamente CoreTech in caso di anomalie che possano determinare un problema di sicurezza dei dati

Posta Elettronica

CoreTech

- Controllo giornaliero dei Backup. La retention dei backup è di 60 giorni
- Verifica giornaliera relativamente allo stato di aggiornamento dell'antivirus integrato
- Verifica giornaliera relativamente alla presenza dei server nelle Black List pubbliche
- Mantenere i sistemi di posta aggiornati con le versioni dei software più stabili e sicuri rilasciate dal produttore
- Tenere sotto monitoraggio il server di posta al fine di garantire la continuità di servizio
- Controllare la presenza di eventuali anomalie relative alla sicurezza che si evidenzino attraverso i log o alert del sistema

Cliente

- Impostare delle password di accesso al servizio di posta con livello di difficoltà conforme alle policy definite e cambio password secondo gli standard di riferimento (es ISO 27002)
- Custodire con cura i dati di accesso alle caselle di posta e limitarne la divulgazione
- Informare i propri utenti circa il buon utilizzo della posta elettronica relativamente alla sicurezza e ai pericoli di phishing e virus
- Intervenire tempestivamente in caso di segnalazioni da parte di CoreTech su problemi inerenti la casella di posta
- Effettuare periodicamente un backup del proprio archivio di posta su propri sistemi di memorizzazione per avere una copia dell'archivio nel caso si voglia procedere a cambiare fornitore

- Avvisare il cliente qualora, attraverso la lettura dei log del mailserver, si evidenzino situazioni che possano mettere in pericolo gli account di posta elettronica e i dati in esso contenuti
- Informare il produttore del software del mailserver qualora venga a conoscenza di falle relative alla sicurezza del sistema
- Modifica immediata di password, qualora l'account fosse stato hackertato e stesse spedendo spam, delete di tutte le mail in coda relative allo specifico account (sia esse valide o di spam). Avviso al cliente per opportune verifiche e cambio password
- Su richiesta del cliente, disponibilità ad effettuare esportazione degli archivi di posta su supporti magnetici o in aree di interscambio (attività da quantificare economicamente)
- Evitare l'utilizzo delle caselle di posta per fare SPAM o invii massivi di email non autorizzate dai destinatari
- Informare tempestivamente CoreTech in caso di anomalie che possano determinare un problema di sicurezza dei dati
- Valutare nelle proprie procedure aziendali la periodicità o l'evento per il cambiamento delle password

Backup

CoreTech

- Controllo giornaliero dello stato dei server e degli storage 1Backup
- Mantenere i sistemi aggiornati con le versioni dei software più stabili e sicuri rilasciate dal produttore
- Tenere sotto monitoraggio i server per garantire la continuità di servizio

Cliente

- Controllare giornalmente l'esito dei backup
- Configurare adeguatamente i job di backup e relative retention secondo le proprie esigenze
- Effettuare una prova di restore almeno con frequenza mensile/bimestrale
- Impostare delle password di accesso al servizio complesse
- Custodire con cura i dati di accesso degli agenti di Backup e limitarne la divulgazione
- Custodire con cura la password di cifratura dei dati se diversa da quella usata per l'agente di Backup
- Informare tempistivamente CoreTech in caso di anomalie che possano determinare un problema di sicurezza dei dati
- Intervenire tempestivamente in caso di segnalazioni da parte di CoreTech su problemi inerenti il servizio

DOCUMENTI

- Guida all applicazione del Regolamento UE 2016 679
- Regolamento UE 2016 679.
- Regolamento Gazzetta Ufficiale
- Servizi SLA
- GDPR
- DPA | Data Processing Agreement
- Contratto
- DPA | Data Processing Agreement