**MegaBite GDPR and compliance guide**

MegaBite custodisce i dati personali dei clienti di terze parti con delega alla responsabilità dei dati. I documenti e le pratiche per la salvaguardia dei diritti dei clienti in materia di protezione dei dati e privacy sono i seguenti:

- DPA

20250521 - MegaBite - Allegato B - DPA template

L'Accordo di Protezione dei Dati (DPA) tra la società e un'altra parte, in conformità con il GDPR, che disciplina il trattamento dei dati personali da parte di FENG in qualità di Responsabile del Trattamento per conto del Titolare. Stabilisce obblighi e diritti delle parti, specificando la natura, la finalità e la durata del trattamento, le misure di sicurezza adottate e le modalità di gestione di eventuali violazioni dei dati (data breach). Regola inoltre l'uso di sub-responsabili e il trasferimento di dati verso paesi terzi.

- Presa visione dell'informativa privacy

20250118 - MegaBite - template privacy policy.pdf

Questo flag è necessario da parte del cliente e compare sul form di iscrizione al programma così: "Ho preso visione dell'informativa della Privacy e acconsento al trattamento dei miei dati personali ai sensi dell'art. 13 D.Lgs. 30/6/2003 n.196 e dell'art. 13 regolamento UE 2016/679"

Documento riassuntivo sulle pratiche legali utilizzate da MegaBite ®
Milano, 12/1/2025 FENG SRL

L’informativa sulla privacy redatta ai sensi dell’art. 13 del Regolamento UE 679/2016 (GDPR) descrive il trattamento dei dati personali effettuato dal Cliente. Illustra le tipologie di dati raccolti, come dati identificativi, di navigazione e relativi al programma di fidelizzazione, le finalità del trattamento, tra cui l’adesione al programma, l’analisi delle abitudini di consumo e attività di marketing, e le basi legali che lo giustificano. Inoltre, stabilisce i tempi di conservazione dei dati, le misure di sicurezza adottate per proteggerli e i diritti degli interessati, come l’accesso, la rettifica, la cancellazione e la limitazione del trattamento. L’informativa specifica anche le modalità di contatto del titolare del trattamento e il diritto di presentare un reclamo all’autorità competente in caso di violazioni.

- Consenso per finalità di fidelizzazione e profilazione

Questo flag è necessario da parte del cliente e compare sul form di iscrizione al programma così:
“Acconsento al trattamento dei miei dati personali per finalità di fidelizzazione e profilazione, inclusi l’invio di informazioni e promozioni commerciali su prodotti e servizi, anche a distanza, e la conduzione di indagini di gradimento e ricerche di mercato. vedi informativa privacy.”

- Consenso per comunicazioni promozionali (opzionale)

Questo flag non è necessario da parte del cliente e compare sul form di iscrizione al programma così:
“Acconsento al trattamento dei miei dati personali per l’invio di comunicazioni commerciali e promozionali, tramite e-mail, SMS, telefono o posta, da parte di soggetti terzi, come partner commerciali, compagnie assicurative o altre società.”

I consensi sono sempre revocabili e se ne tiene conto nella gestione delle notifiche push inviabili tramite mobile wallet.

- Diritto all'Oblio

Il diritto all'oblio, previsto dall'articolo 17 del GDPR, consente a un individuo di richiedere la cancellazione dei propri dati personali.
Questo diritto è esercitabile dal cliente tramite un link inserito nell'Area Personale e in tutte le email che riceve da MegaBite dopo la profilazione,

- Banner Cookie e Privacy policy

MegaBite è un servizio white label e può utilizzare domini e sottodomini di proprietà del cliente. Sulle pagine web sviluppate da MegaBite si possono inserire i banner che vengono usati sul sito principale del Cliente o possono essere generati gratuitamente da Iubenda o su commissione in un formato personalizzato.

- Caratteristiche tecniche di sicurezza del sistema MegaBite

MegaBite adotta un'infrastruttura sicura e conforme alle normative europee sulla protezione dei dati. Tutti i server sono localizzati in Italia o all'interno dell'Unione Europea. Per assicurare la massima protezione delle informazioni, i dati dei Clienti sono segregati in database distinti. La piattaforma è sottoposta a rigorosi controlli di sicurezza, **Extended Vulnerability Assessment** trimestrali per l'identificazione e la mitigazione proattiva di vulnerabilità, oltre a cyberattacchi controllati annuali per verificare l'impenetrabilità del sistema. Queste misure, unite a protocolli di sicurezza avanzati, garantiscono un ambiente conforme, affidabile e resiliente alle minacce informatiche.