I SERVIZI E PRODOTTI VERTICAL BOOKING IN RELAZIONE ALLE PRESCRIZIONI DEL GDPR

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Vertical Booking s.r.l				
Partita Iva	IT02657150161				
Indirizzo	**Piazza Pontida, 7**				
Città	**Bergamo**	Cap	**24122**	PV	**BG**
Legale Rappresentante	**Alberto Guadalupi**				

INCARICATI DEL TRATTAMENTO
Addetti allo sviluppo, controllo qualità, help desk, consulenti applicativi

DATI DI CONTATTO			
Titolare del trattamento	Vertical Booking s.r.l		+39 035232366
Rappresentante del titolare	Alberto Guadalupi		+39 035232366

DESCRIZIONE
Vertical Booking è un software di prenotazione online per hotel e catene alberghiere. La suite completa comprende Booking Engine, Synchro Channel Manager, Metasearch Manager, CRO (Central Reservation Office), Connettività e Rappresentanza GDS, Strumenti di Marketing e Intelligence e App Mobile (iOs/Android). La piattaforma Vertical Booking raccoglie e memorizza i dati personali dei soggetti prenotanti che effettuano la prenotazione dai diversi canali distributivi con cui Vertical Booking è connesso. I canali di distribuzione possono essere classificati in

- canali diretti, ossia canali senza intermediazione,
- canali indiretti.

Tra i canali diretti rientrano il modulo booking engine collegato al sito web della struttura alberghiera o della catena alberghiera e il modulo CRO (Central reservation Office), il modulo Service Provider (SP) e il modulo DMS.

I moduli Booking Engine, CRO, DMS sono configurabili da parte del cliente (hotel) che può scegliere quanti e quali dati del prenotante raccogliere e se raccogliere oltre ai dati del referente della prenotazione anche i dati degli altri ospiti.

Tra i canali indiretti rientrano gli IDS (Internet Distribution System) come OTA (Online travel agent), TO (Tour operator), WHOLESALERS e i GDS.

La quantità e la tipologia dei dati dei prenotanti ricevuti dai canali indiretti non sono sotto il controllo della piattaforma Vertical Booking.

La piattaforma Vertical Booking raccoglie e memorizza i dati di carta di credito associati alla prenotazione secondo le direttive PCI-DSS a cui si rimanda per ulteriori dettagli (https://www.pcisecuritystandards.org/).

Nel caso in cui il cliente abbia richiesto una connessione con un gestionale alberghiero (PMS), Vertical Booking trasferisce i dati relativi al prenotante e alla prenotazione al gestionale alberghiero tramite un'interfaccia programmatica.

La piattaforma Vertical Booking memorizza i dati relativi al profilo (nome, cognome, indirizzo email, username e password) con cui gli utenti si collegano al back office della piattaforma.

FINALITA' DEL TRATTAMENTO

L'accesso ai dati personali da parte di Vertical Booking è effettuato per operazioni di assistenza e manutenzione dell'applicativo.

CATEGORIA INTERESSATI

Soggetti privati, Aziende, dipendenti delle strutture/catene alberghiere, dipendenti Vertical Booking, partner e rivenditori delle soluzioni Vertical Booking

CATEGORIE DI DATI PERSONALI

Si individuano le seguenti categorie di dati personali

DATI IDENTIFICATIVI

Dati identificativi del soggetto prenotante ed eventualmente degli altri ospiti.

CARTE DI CREDITO

Dati di carta di credito associati alla prenotazione a garanzia della stessa.

UBICAZIONE e SPOSTAMENTI

Intrinsecamente alla prenotazione è associata l'ubicazione dell'albergo e quindi anche l'ubicazione del soggetto che ha soggiornato per quel periodo nella struttura.

La piattaforma permette anche di prenotare servizi come escursioni e transfer, quindi può memorizzare anche dati relativi agli spostamenti del soggetto.

DATI RELATIVI AI SERVIZI EROGATI PRESSO LE STRUTTURE RICETTIVE/SPA

La piattaforma permette di configurare e prenotare servizi in aggiunta al soggiorno alberghiero o indipendentemente dal soggiorno alberghiero.

DATI PROFILI UTENTI PERSONALE INTERNO VERTICAL BOOKING

I dati dei profili utenti utilizzati dal personale di Vertical Booking s.r.l per accedere al sistema

DATI PROFILI UTENTI CREATI DAL CLIENTE

I dati dei profili utenti creati dai clienti per accedere e gestire i dati di propria competenza all'interno della piattaforma.

DATI DI FATTURAZIONE CLIENTI VERTICAL BOOKING S.r.l

I dati memorizzati a scopi amministrativi dei clienti Vertical Booking

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

DATACENTER EQUINIX a Milano (ML2)

Datacenter in cui risiedono fisicamente i server e le apparecchiature necessarie

DATACENTER EQUINIX a Parigi per DISASTER RECOVERY (PA2)

Datacenter che ospita il sito di disaster recovery

PARTNER COMMERCIALI

Vertical Booking può comunicare i dati di contatto del cliente (struttura ricettiva) a partner (Expedia, Booking.com) per finalità informative e commerciali.

SERVIZI IN OUTSOURCING

Vertical Booking utilizza come server di posta in ricezione ed in uscita per le comunicazioni relative al dominio verticalbooking.com GSuite di Google. Le mail inviate dai clienti verso l'assistenza tecnica potrebbero contenere dati identificativi sono memorizzate presso i server di Google.

Vertical Booking utilizza un fornitore esterno per gestire l'autenticazione a due fattori tramite OTP (one time password), la società Authy - a Twilio company, 375 Beale St, Suite 300, San Francisco, CA 94105.

Vertical Booking utilizza un servizio di invio mail esterno per gli utenti che hanno attivo il modulo Guest Review (nome commerciale: Stambol).

TRASFERIMENTO DATI ALL'ESTERO

DISASTER RECOVERY (FRANCIA)

I dati vengono trasferiti nel sito di disaster recovery presso Equinix PA2 - Data center IBX di Parigi per effettuare le operazioni di sincronizzazione e backup disaster recovery.

VERIFICA DELLE SICUREZZE A LIVELLO APPLICATIVO

Vertical Booking mette a disposizione del cliente (struttura ricettiva) la possibilità di visualizzare la lista degli utenti attivi e degli utenti non più attivi che hanno accesso alla piattaforma e hanno visibilità sui dati personali di cui il cliente è titolare.

Vertical Booking permette al cliente di gestire, ossia inserire, rimuovere, modificare gli utenti e di stabilire i permessi con cui hanno accesso al sistema.

TERMINI PER LA CANCELLAZIONE DEI DATI

I dati personali dei prenotanti hanno una data di scadenza di 15 anni dal loro inserimento nel sistema. Il cliente può richiedere che i dati personali vengano cancellati tramite una richiesta scritta all'assistenza tecnica che provvede ad attuare la procedura di cancellazione.

I dati di carta di credito vengono cancellati dal sistema automaticamente dopo 15 giorni dalla data di checkout della prenotazione.

MISURE DI SICUREZZA IMPLEMENTATE NEL SOFTWARE

Di seguito vengono riportate le misure di sicurezza nel sistema applicativo.

Profili di accesso

L'applicazione garantisce che il cliente abbia visibilità soltanto sui dati di cui è titolare definendo il concetto di competenza.

Esistono i seguenti livelli di competenza:

- Supervisor: accesso amministrativo per scopi di assistenza, manutenzione al sistema ed è concesso soltanto al personale di Vertical Booking. L'accesso supervisor è consentito soltanto da indirizzi IP certificati oppure tramite VPN.
- Area: garantisce accesso alla gestione ed alla visualizzazione delle strutture/catene alberghiere che appartengono ad una area commerciale.
- Gruppo: garantisce accesso alla gestione e alla visualizzazione dei dati di un gruppo di alberghi
- Hotel: garantisce accesso ad una particolare struttura ricettiva

Gestione delle credenziali di accesso

- User name: l'accesso al sistema avviene attraverso l'identificazione univoca del soggetto che vi accede. In fase di setup del sistema viene consegnata al titolare una credenziale che utilizzerà per accedere al sistema. Con questa credenziale viene identificato all'interno del sistema e le operazioni che esegue vengono tracciate e memorizzate in un log delle operazioni.
- Password: Per accedere alla piattaforma è necessario fornire una password associata allo username. La complessità della password deve avere le seguenti caratteristiche:
    - Lunghezza di 8 caratteri
    - Deve contenere un carattere maiuscolo
    - Deve contenere un carattere minuscolo
    - Deve contenere un carattere numerico
    - Deve contenere un carattere speciale preso dal seguente alfabeto `[$%*:,£)(@#;+_\-]
    - La password deve essere diversa dalle 5 precedenti

Gestione dei profili di accesso

- Il cliente non può creare utenti che abbiano una competenza superiore alla propria
- Il cliente ha la possibilità di creare altri utenti che avranno visibilità sui dati di cui il cliente è titolare secondo un profilo di accesso scelto dal cliente e che abbiano una competenza uguale o inferiore alla propria.
- Disattivazione/Disabilitazione delle credenziali: il cliente può disabilitare gli utenti creati, reimpostare la data di scadenza delle password e rimuovere utenti creati.
- Visibilità dati di carta di credito: in fase di creazione l'utente non ha il permesso di visualizzare le carte di credito e neanche il permesso di concedere la visibilità dei dati di carta ad altri utenti.

Il cliente può richiedere all'assistenza tecnica di essere abilitato ad assegnare il permesso di visibilità sulle carte di credito per gli utenti di propria competenza.

Tecniche di crittografia

- Crittografia della password: la password viene crittografata con un algoritmo di hashing crittograficamente sicuro e memorizzata con un "salt". L'hash viene calcolato tramite una procedura di key stretching per combattere gli attacchi brute force
- Two factor authentication: per visualizzare i dati di carta di credito il cliente deve superare un'autenticazione a due fattori. Il primo fattore di autenticazione consiste nel fornire la coppia username + password descritta sopra.

Il secondo fattore di autenticazione prevede una delle seguenti modalità:

- Identificazione tramite un indirizzo IP certificato
- OTP (one time password) tramite registrazione dell'utente e verifica effettuato dalla piattaforma Authy (www.authy.com)

Strumenti di log

Il cliente ha la possibilità di visualizzare le operazioni che gli utenti di sua competenza hanno eseguito sulla piattaforma tramite una sezione che offre degli strumenti di estrazione log.

Carte di credito

La gestione ad ogni livello dell'accesso alle carte di credito è gestito secondo le direttive PCI-DSS.

MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL

Nell'assistenza tramite email i tecnici Vertical Booking inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.

I dati relativi alle carte di credito non vengono mai trasmessi dal personale Vertical Booking tramite email o comunicati telefonicamente.

Nel caso in cui il personale Vertical Booking riceva comunicazioni (posta elettronica) contenenti dati relativi alle carte di credito, è tenuto a:

1. segnalare l'evento al personale che effettua i controlli di sicurezza
2. comunicare al cliente che i dati delle carte non devono essere trasmessi su canali non sicuri

ASSISTENZA ATTRAVERSO COLLEGAMENTO HTTPS

L'assistenza tecnica per accedere con competenza supervisor alla piattaforma deve effettuare l'accesso da uno degli IP dell'ufficio o tramite VPN (Virtual Private Network).

ASSISTENZA ATTRAVERSO COLLEGAMENTO SSH TRAMITE VPN

Per operazioni di manutenzione e amministrazione dei sistemi i tecnici Vertical Booking accedono ai sistemi tramite protocollo ssh con autenticazione a due fattori.

MISURE DI SICUREZZA IMPLEMENTATE PRESSO I DATACENTER

L'infrastruttura hardware e software di Vertical Booking risiede presso il datacenter Equinix ML2 Milano all'indirizzo Via Savona, 125, 20144 Milano MI.

Il sito di Disaster Recovery è situato presso Equinix PA2, all'indirizzo 114 Rue Ambroise Croizat Saint Denis, France 93200

Controllo degli accessi

L'accesso al Data Center è regolamentato secondo le procedure e gli standard di Equinix.

Soltanto il personale autorizzato Vertical Booking può fornire accesso al Data Center per interventi di manutenzioni o visite al datacenter.

Firewalling

Il networking del Datacenter è separato dalle reti pubbliche. I flussi dati tra il networking del Datacenter e l'esterno vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati.

Certificazioni DATACENTER

Di seguito le certificazioni per il sito Equinix ML2 e per il sito Equinix PA2 (consultabili anche presso il sito www.equinix.com)

ML2:

- ISO14001:2004
- ISO 27001
- ISO 50001
- ISO9001:2008
- OHSAS 18001
- PCI DSS

PA2:

- HDA
- ISO14001:2004
- ISO 27001
- ISO 50001
- ISO9001:2015
- OHSAS 18001
- PCI DSS
- SOC 1 Type II
- SOC 2 Type II

Timbro e Firma per accettazione

VERTICAL BOOKING S.R.L.
Piazza Pontida, 7 - 24122 BERGAMO
Partita IVA 02657150161