Gentile Cliente/Partner,

ci preme rassicurarti che abbiamo provveduto alle prescrizioni di legge in tema di trattamento e tutela dei dati e predisposto le procedure di controllo necessarie.

I dati che trattiamo sono il nostro asset più importante e per questo li proteggiamo con la massima cura. Questo avviene sia per i dati personali che per quelli anonimi, ma non per questo meno importanti, come ad esempio i segreti industriali e commerciali di cui veniamo a conoscenza, i marketing plans o i codici sorgente.

Compatibilmente con il contesto in cui operiamo e le risorse a nostra disposizione, abbiamo predisposto le migliori tecnologie informatiche per proteggere questi dati, il loro trattamento e per garantire la continuità del business in caso di avarie.

Per questo siamo orgogliosi di condividere con la massima trasparenza la nostra policy in tema di protezione dei dati.

Per qualsiasi delucidazione non esitare a contattarci.
Buona lettura

15 Febbraio 2018

Indice

Registro dei Trattamenti e DPIA

★ Prefazione

Questo documento è la nostra certificazione di compliance al *Regolamento EU/2016/679*, di seguito **GDPR**, e rappresenta un estratto sia del **REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO**[1] della nostra azienda che la **VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI**[2].
Per la sua stesura abbiamo preferito partire dalle soluzioni adottate per proteggere i dati per poi risalire nell'analisi dei rischi, seguendo quindi un approccio "bottom-up".
Per leggere meglio il documento troverai all'inizio una panoramica delle attività che svolgiamo, così potrai inquadrare più facilmente il contesto in cui operiamo.

★ Titolare del trattamento dei dati

Titolare

Haitex Srl con sede legale in via Filippo Corridoni 17, Sora 03039 (FR) ITALY, identificata con Partita Iva 02572290605 ed iscritta al Registro delle Imprese di Frosinone al numero REA FR-162075, Capitale Sociale 10.000 Euro interamente versati, iscritta dal 2014 al "Registro dei Trattamenti" del "Garante della Privacy" con notificazione numero 2014050700196175

[1] Art. 30 del GDPR
[2] DPIA, Art. 35 del GDPR

Contatti per esercitare i propri diritti

Amministratore Unico: **Claudio Miacci** - amministrazione@pec.haitex.it
Data Protection Officer: **Claudio Miacci** - amministrazione@pec.haitex.it
Stesura e progettazione: **Giovanni Gasparri** - giovanni@haitex.it

★ Inquadramento del contesto operativo

- ➔ La nostra azienda ha meno di 250 dipendenti;
- ➔ I dati vengono conservati ed elaborati in Italia;
- ➔ Operiamo nel settore informatico e ci occupiamo di e-commerce. Nello specifico:
  - ◆ Offriamo ai nostri partners una piattaforma software as a service;
  - ◆ Aiutiamo i nostri partners nella gestione di portali e-commerce e marketplaces;
  - ◆ Conduciamo campagne marketing per conto dei partners.

Per la definizione di "clienti" e "partners" fai riferimento al paragrafo "Soggetti interessati".

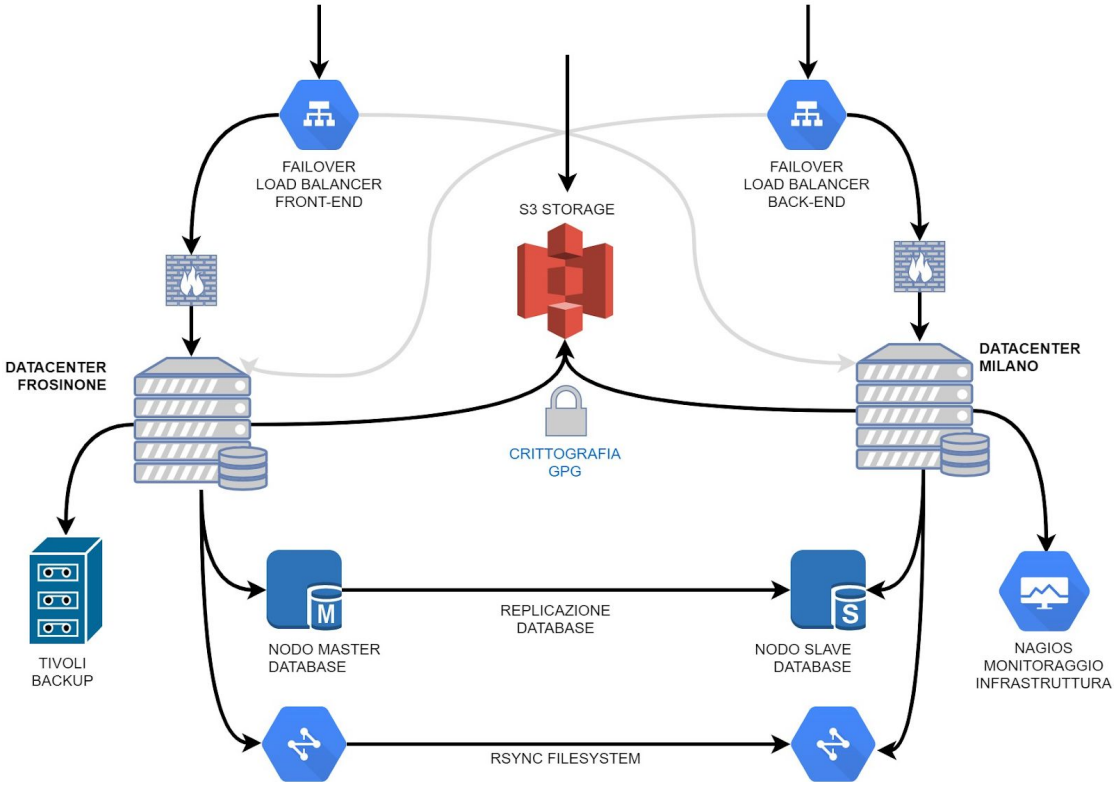
Non trattiamo dati considerati ad "alto rischio"[3] e pertanto la "Valutazione di impatto sulla protezione dei dati (DPIA)" non è obbligatoria ma facoltativa e consigliata. Per questo abbiamo deciso ugualmente di condurla.

★ Sintesi della compliance al GDPR

- ★ Trattiamo dati relativi a cittadini dell'Unione Europea;
- ★ Trasferiamo i dati personali ad altri soggetti, dandone preventiva informazione agli interessati;
- ★ I dati personali vengono trasmessi in forma crittografata;
- ★ I dati personali vengono conservati in maniera adeguata;
- ★ Forniamo agli interessati le opportune informazioni circa i trattamenti e le finalità ed otteniamo espliciti consensi facoltativi e separati prima del trattamento;
- ★ Con il presente documento forniamo agli interessati tutte le informazioni relative alle tecniche ed ai flussi di trattamento;
- ★ Adottiamo misure per cancellare automaticamente dati personali dopo che il relativo scopo è stato conseguito;
- ★ I dati personali vengono conservati in maniera corretta e crittografata, ove ritenuto necessario;
- ★ Abbiamo analizzato i fornitori dei servizi, anche tecnologici, per assicurarci che adottassero i requisiti minimi richiesti;
- ★ I fornitori dell'infrastruttura tecnologica (data processor) ed i dati personali che questi trattano sono collocati nel territorio dell'unione Europea;
- ★ Effettuiamo analisi periodiche per assicurarci che i processi vengano attuati correttamente;
- ★ Verifichiamo periodicamente i criteri di sicurezza;
- ★ Monitoriamo il comportamento di utenti privilegiati (ovvero che hanno accesso ai dati personali), per identificare attività anomale o sospette;
- ★ Abbiamo predisposto le procedure per notificare alle autorità eventuali violazioni dei dati (Data Breach).

[3] Art. 35 del GDPR

★ Schema logico dell'architettura informatica



I nostri server sono operativi ininterrottamente dal 2010 ed hanno erogato servizi con una disponibilità superiore al 99,9%. Abbiamo progettato i nostri sistemi software per continuare a funzionare anche in caso di guasti o di calamità naturali di importante entità, come ad esempio terremoti devastanti.
Per questo abbiamo collocato alcuni server presso il data center di Seeweb di Frosinone ed altri presso quello di Milano. I due data center sono autonomi e sincronizzati con una manciata di millisecondi di ritardo, garantendo così la business continuity in caso di eventi catastrofici. Disponiamo di due appliances, rispettivamente una per per il back-end e l'altra per il front-end, che si occupano di gestire il failover del traffico web in caso di guasti.
I dati presenti nel database sono oggetto di replicazione master/slave in tempo reale. Facciamo una volta al mese delle simulazioni per testare eventuali guasti di replicazione, distruzione e ricostruzione di un nodo ed almeno una volta l'anno la simulazione di inversione di ruolo tra master e slave.
I files presenti sulle macchine sono replicati tramite rsync ogni 5 minuti.
Alcuni files statici, come ad esempio i pdf delle fatture, sono invece conservati su uno storage S3 dopo essere stati singolarmente crittografati con GPG.
Disponiamo di un sistema di monitoraggio interno che ci avvisa immediatamente nel caso in cui si verifichi qualche anomalia del nostro impianto, di rete, o dei server esterni a cui ci colleghiamo (corrieri, banche, marketplaces, ERP).
Abbiamo 7 livelli indipendenti di backup che ci assicurano la massima protezione dei dati.
Utilizziamo solo il protocollo HTTPS con certificati di crittografia opportunamente dimensionati, tra cui anche Extended Validation. Il back-end è accessibile solamente dagli operatori che oltre a conoscere la password dispongono anche di un certificato SSL client da noi rilasciato.

Nei paragrafi che seguono potrai approfondire tutte le contromisure che abbiamo adottato ed i rischi che queste mitigano

★ Descrizione delle contromisure

Sistemi di backup

I dati dei nostri server vengono sottoposti a sette livelli simultanei ed indipendenti di backup:

- ➔ snapshot LVM del database, effettuato ogni 8 ore senza interruzione di servizio;
- ➔ backup crittografato su S3 degli ultimi 6 snapshots LVM del database;
- ➔ backup giornaliero e trasferimento della copia sugli altri server (in pronta disponibilità);
- ➔ backup giornaliero crittografato con archiviazione in storage S3;
- ➔ backup settimanale mediante il sistema Tivoli TSM di IBM;
- ➔ backup manuale e conservazione su dischi crittografati con BestCrypt Volume Encryption;
- ➔ rsync ogni 5 minuti dei files tra i due data center.

Tivoli TSM si occupa inoltre dell'assessment delle procedure di Disaster Recovery per i dati oggetto del backup. Il software assicura l'esecuzione dei backup in base alle politiche stabilite, verifica inoltre il contenuto delle copie di sicurezza e la loro congruità con gli archivi da proteggere.

Piano di Disaster Recovery e simulazioni

Disponiamo di un piano di disaster recovery che è soggetto a continue verifiche ed aggiornamenti.
Effettuiamo regolarmente delle simulazioni di disaster recovery.

Replicazione SQL

Abbiamo in funzione un sistema di replicazione in tempo reale dei dati SQL, pertanto riusciamo a garantire la business continuity.

Ridondanza geografica

Abbiamo collocato dei server in un data center di Frosinone e dei server in uno a Milano, in modo da ottenere una ridondanza geografica anche in situazioni di gravi calamità locali come ad esempio i terremoti. I data center vengono clonati mediante rsync ogni 5 minuti e mediante Replicazione SQL in tempo reale e pertanto sono autonomi.

Alta Disponibilità

Ogni server ha parametri garantiti (Memoria, Cpu, Rete) ed è in alta disponibilità. Ovvero realizzato su macchine multiprocessore multicore ridondate N+1 e con storage SAN ad alta disponibilità. Uptime garantito 99,9%.

Failover HTTPS

Abbiamo due sistemi di failover, ognuno dei quali è ridondato, che intervengono per lo smistamento del traffico web dal server guasto ad un altro server operativo, trasferendo anche le sessioni PHP in modo da non svuotare i carrelli dei clienti che stanno navigando sul sito.

Sovradimensionamento delle risorse

Ogni server è sovradimensionato ed in grado di supportare il carico di un eventuale altro server guasto.
Abbiamo schedulato ogni mese un assessment per verificare il giusto dimensionamento delle risorse hardware al fine di scongiurare l'effetto domino in caso di guasto di un nodo dell'architettura.

Assurance

Per ogni server abbiamo attivi dei piani di assurance al massimo livello che ci garantiscono l'intervento fisico e dedicato di uno specialista all'interno dei data center con disponibilità continua: 24 ore su 24, ogni giorno dell'anno, inclusi i festivi.

Monitoraggio

In caso di malfunzionamento del server o di un qualsiasi servizio abbiamo un sistema di monitoraggio interno basato su Nagios che ci avvisa immediatamente; Il provider ha un sistema di monitoraggio aggiuntivo ed indipendente che si somma al nostro.

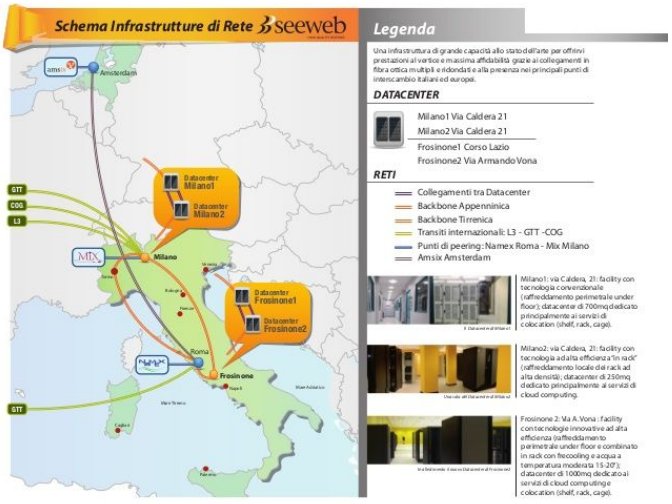
Banda garantita

Ogni nostro server ha a disposizione 1 Gbps di banda bilanciata garantita.

Penetration Test

Annualmente commissioniamo ad una società esterna un Security Assessment (che include penetration test), ovvero delle simulazioni di attacchi informatici finalizzate ad individuare e correggere eventuali vulnerabilità; Gli attacchi sono di due diverse tipologie tra di loro alternate: white box e black box.
Inoltre effettuiamo periodicamente dei penetration test interni.

Rete ridondata



I router dei data center sono tutti duplicati e raggiungibili tramite due percorsi; in questo modo, i servizi di Cloud Computing prescindono da una infrastruttura di rete che offre le giuste performance e un adeguato grado di ridondanza in modo da assicurare un servizio continuativo e con un elevato standard di qualità.
La banda internet viene fornita a Seeweb da alcune delle più importanti reti Tier 1 globali, cioè Cogent Communications, GTT e NTT: scelte per la loro affidabilità e perché insieme permettono di avere un servizio tra loro ridondato. La connettività del data center di Milano è organizzata in modo che nessuno dei fornitori condivida fibre o sale dati e quindi il nostro provider Seeweb è in grado di continuare a fornire il servizio anche in caso di guasti a uno degli altri data center del comprensorio di Via Caldera. Per una maggiore sicurezza, i data center di Frosinone hanno a disposizione una seconda connessione verso GTT in modo da essere completamente indipendenti da Milano anche in caso di eventi catastrofici. Parte del traffico è scambiata mediante interconnessioni dirette (peering): per questo Seeweb è connessa ai due più grandi punti di interscambio neutrali italiani, MIX a Milano e NAMEX a Roma, e in uno dei più importanti a livello europeo, AMS-IX di Amsterdam.

Logging

Tutte le principali operazioni che avvengono all'interno dei nostri sistemi informatici vengono registrate nei log per un periodo minimo di un mese

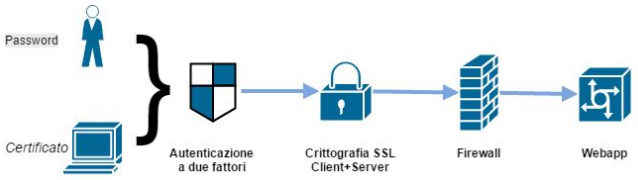
Firewall

Ogni server è dotato di firewall configurato in maniera aggressiva. Tutte le connessioni a porte e servizi non autorizzati sono bloccate, ad eccezione dei protocolli http/https.
Il nostro server database non è esposto al pubblico ma accessibile unicamente ai nostri server.
Nessun servizio che richiede autenticazione è attivo ed esposto al pubblico. Le pagine html utilizzate per l'autenticazione dei clienti (area privata) utilizzano invece la tecnologia invisible recaptcha v2.

Autenticazione a 2-fattori o 3-fattori

Utilizziamo sistemi di autenticazione a due fattori per consentire ai partners l'accesso al backend.

L'accesso ai server da parte dei nostri tecnici (amministratori di sistema) richiede autenticazione a 3 fattori (certificato ssl client + sblocco firewall + password). Ogni operatore dispone di credenziali di accesso uniche; Tutte le operazioni vengono registrate nei logs.



Intrusion Detection System

Utilizziamo sistemi antintrusione come psad, fail2ban e denyhosts, che bloccano i tentativi di accesso al server provenienti da un indirizzo ip dopo un certo numero di fallimenti.

Certificati Clients SSL

Per l'accesso al back-office richiediamo obbligatoriamente l'installazione del certificato come autenticazione a due fattori: Il server richiede che il terminale client abbia il certificato client di crittografia SSL/TSL PKCS-12 X.509 installato (two-way authentication) e firmato dalla nostra Certification Authority (Haitex Digital Strategy).

Aggiornamenti di sicurezza

Applichiamo costantemente gli aggiornamenti di sicurezza dei nostri server Debian.

No-FTP

Il servizio ftp non è mai stato aperto al pubblico. Viene utilizzato unicamente per comunicazioni interne in abbinamento con ulteriori misure precauzionali. È stato utilizzato invece il protocollo sftp basato su ssh per l'interscambio di alcuni dati con software ERP, ma che stiamo progressivamente migrando su uno storage esterno in tecnologia S3.

Crittografia S3

I documenti fiscali, così come i files contenenti dati personali, vengono archiviati sul nostro storage S3 dopo essere stati singolarmente crittografati con il più avanzato sistema di crittografia bilanciato, denominato GPG;
Le chiavi sono conservate su altri dispositivi (inaccessibili) e non sullo storage S3.

Mitigazione attacchi DoS/DDoS

Abbiamo configurato un sistema firewall in grado di droppare le connessioni ritenute parte di attacchi denial of service. Utilizziamo "Mod_evasive" come protezione contro attacchi DoS o DDoS al fine di strozzare le connessioni HTTP e HTTPS quando si superano le soglie specificate.

Certificati SSL

Utilizziamo unicamente certificati di crittografia SSL standard ed in alcuni casi di tipologia Extended Validation per tutto il traffico web; in questo modo siamo sicuri che i dati non possano essere intercettati da un MITM.

Web Application Firewall

Utilizziamo un algoritmo da noi sviluppato che immediatamente blocca a livello di firewall l'indirizzo ip che sta tentando questi tipi di attacco già dal primo tentativo: SQL Injection o Cross-Site Scripting (XSS). Il blocco dura al più 24 ore.

Antivirus

Scansioniamo periodicamente tutti i files con antivirus aggiornati per assicurarci che i nostri server non forniscano a clienti o a partner codice malevolo.

Mitigazione phishing/spam e mail deliverability

Utilizziamo le tecnologie DKIM e SPF al fine di garantire la deliverability dei messaggi email che partono dai nostri server. Queste aiutano i destinatari a proteggersi da eventuali attacchi phishing che sfruttano il nostro nome.

Versioning dei codici sorgente

Per la programmazione dei nostri applicativi utilizziamo Subversion per tenere traccia di tutte le variazioni apportate ai files. Questo ci consente di tornare indietro in caso di errori di programmazione.

Formazione

Il nostro personale è soggetto a continui aggiornamenti formativi erogati internamente alla nostra azienda.

Controllo accessi ai data center

L'accesso ai locali è regolato dalle procedure di sicurezza come da DPS predisposto ai sensi del d.lgs 196/2003, separatamente riassunte e le prescrizioni ISO:27001. I data center sono dotati di controllo accessi a doppio fattore a norma CEI EN 50133. I data center sono anche dotati di sorveglianza elettronica contro l'intrusione, l'incendio e le anomalie ambientali critiche (conformi alle norme CEI EN 50131, EN 50132, EN 50133, EN 50134, EN 50136, EN 50137, EN 50118) con segnalazione via radio e intervento in sede da parte di istituto di polizia privata autorizzato. Ai dati particolari hanno accesso solo ed esclusivamente gli incaricati grazie ad un sistema di verifica che gli permette di accedere alle parti degli elaboratori in cui sono conservati i dati particolari.

Surriscaldamento dei server

Per tutti i data center sono garantite le condizioni climatiche secondo raccomandazioni ASHRAE 2008. I data center dispongono di sistema ridondante di controllo del clima delle sale macchine con allarmi locali e remoti (teleallarmi su istituto di vigilanza) su valori critici.

Black-out e rischi elettrici

I data center sono dotati di sistema di alimentazione ridondante su doppia rete di distribuzione a norme EIE-CE per ogni fila di armadi con prese e spine di sicurezza antistrappo e anti fuoco. Impianto di sicurezza dell'alimentazione mediante impianto di terra certificato conforme L.626 e separazione galvanica delle sorgenti; Sistema di commutazione statica della sorgente duale di alimentazione per ogni armadio a servizio delle apparecchiature non dotate di alimentatori ridondanti; Condizionamento statico dell'alimentazione per ogni modulo tramite Gruppi di continuità statici on line.

Allagamento dei data center

I data center sono tutti al di sopra del piano campagna e molto oltre i livelli di piena storici; un sofisticato sistema di percolazione protegge da eventuali perdite di acqua degli impianti di refrigerazione;

Incendio nei data center

L'innovativo sistema di estinzione incendi (l'HI-FOG® Marioff water mist), in linea con gli standard NFPA 750 e UNI CEN/TS 14972, consente la coesistenza di operatori in campo mentre è in atto il processo di estinzione dell'incendio riducendo al minimo l'impatto sui servizi;
I data center di Milano sono protetti da sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5; la sede di Frosinone è protetta da sistema Vesda multiarea progressivo;

Altri rischi

La logica con cui sono stati scelti i sistemi di protezione è all'insegna della indipendenza dal vendor per le operazioni di aggiornamento/manutenzione e la disponibilità, per ogni componente di aggiornamenti e patch nel minor tempo possibile.

Le procedure di ripristino prevedono il recupero dei dati in un'opportuna area di spool non coincidente con l'area di produzione. I dati recuperati vengono poi sottoposti a validazione tramite ispezione manuale o automatica e quindi reimmessi negli archivi di produzione.
L'eventuale interruzione di servizio non collegata con la perdita di dati ma derivante da problemi di connessione e/o da malfunzionamento dei dispositivi hardware (server, terminali, router) viene trattata in maniera autonoma dalla gestione/conservazione degli archivi.
Gruppi elettrogeni diesel ad alta autonomia con capacità adeguata, avvio automatico e cicli di diagnostica bisettimanale automatici.

★ Criteri adottati per l'analisi dei rischi

Il rischio R è calcolato in funzione della probabilità P dell'accadimento dell'evento e dalla magnitudo M data dalle sue conseguenze.
Sono state utilizzate la seguenti scale:

P=1	Improbabile	M=1	lieve
P=2	poco probabile	M=2	medio
P=3	probabile	M=3	grave
P=4	altamente probabile	M=4	gravissimo

Stima del rischio: R = MxP

Rischio			
Basso	Medio	Alto	Altissimo
1<=R<=2	3<=R<=4	6<=R<=9	12<=R<16

★ Analisi dei Rischi

Errore Umano

Effetti	Perdita di dati, Malfunzionamento, Interruzione di servizio,Violazione dei dati
Probabilità	4 (Altamente probabile)
Magnitudo	3 (Grave)
Rischio	12 (Altissimo)
Contromisure	Sistemi di backup; Piano di Disaster Recovery e simulazioni; Assurance; Versioning dei codici sorgente; Formazione; Controllo accessi ai data center; Altri rischi;
Impatto sui diritti e le libertà degli interessati	In caso di **disservizio** gli interessati potrebbero temporaneamente non essere in grado di accedere ai sistemi informatici. Tuttavia possono esercitare i propri diritti contattandoci. In caso di **perdita** di dati non si evidenziano particolari limitazioni ai diritti degli interessati, se non la necessità di prestare nuovamente i consensi qualora si ritenesse necessario. In caso di **violazione** dei dati (ad esempio modifica involontaria o corruzione degli indici) potremmo trovarci nella condizione di non poter distinguere più i dati attendibili da quelli non attendibili e quindi potrebbe risultare problematico garantire agli interessati di esercitare i propri diritti se non siamo in grado di verificare i dati di identità del richiedente con quelli registrati sui nostri sistemi.

Attacchi informatici o azioni fraudolente

Effetti	Perdita di dati, Malfunzionamento, Interruzione di servizio,Violazione dei dati
Probabilità	4 (Altamente probabile)
Magnitudo	4 (Gravissimo)
Rischio	16 (Altissimo)
Contromisure	Sistemi di backup; Piano di Disaster Recovery e simulazioni; Replicazione SQL; Failover HTTPS; sovradimensionamento delle risorse; Assurance; Monitoraggio; Penetration Test; Firewall; Autenticazione a 2-Fattori o a 3-Fattori; Intrusion Detection System; Certificati Client SSL; Aggiornamenti di sicurezza; No-Ftp; Crittografia S3; Mitigazione attacchi DoS/DDoS; Certificati SSL; Web Application Firewall; Antivirus; Mitigazione phishing/spam e mail deliverability; Formazione; Controllo accessi ai data center; Altri rischi;
Impatto sui diritti e le libertà degli interessati	In caso di **disservizio** gli interessati potrebbero temporaneamente non essere in grado di accedere ai sistemi informatici. Tuttavia possono esercitare i propri diritti contattandoci. In caso di **perdita** di dati non si evidenziano particolari limitazioni ai diritti degli interessati, se non la necessità di prestare nuovamente i consensi qualora si ritenesse necessario. In caso di **violazione** dei dati (ad esempio modifica o injection) potremmo trovarci nella condizione di non poter distinguere più i dati attendibili da quelli non attendibili e quindi potrebbe risultare problematico garantire agli interessati di esercitare i propri diritti se non siamo in grado di verificare i dati di identità del richiedente con quelli registrati sui nostri sistemi. In caso di **sottrazione** dei dati si potrebbe verificare una limitazione delle libertà degli interessati, in quanto i dati potrebbero essere utilizzati per qualsiasi finalità, inclusi eventuali abusi o reati.

Guasti tecnici

Effetti	Perdita di dati, Malfunzionamento, Interruzione di servizio,Violazione dei dati
Probabilità	4 (Altamente probabile)
Magnitudo	3 (Grave)
Rischio	12 (Altissimo)
Contromisure	Sistemi di backup; Piano di Disaster Recovery e simulazioni; Replicazione SQL; Ridondanza geografica; Alta disponibilità; Failover HTTPS; sovradimensionamento delle risorse; Assurance; Monitoraggio; Banda garantita; Rete ridondata; Formazione; Surriscaldamento dei server; Black-out e rischi elettrici; Allagamento dei data center; Incendio nei data center; Altri rischi;
Impatto sui diritti e le libertà degli interessati	In caso di **disservizio** gli interessati potrebbero temporaneamente non essere in grado di accedere ai sistemi informatici. Tuttavia possono esercitare i propri diritti contattandoci. In caso di **perdita** di dati non si evidenziano particolari limitazioni ai diritti degli interessati, se non la necessità di prestare nuovamente i consensi qualora si ritenesse necessario. In caso di **violazione** dei dati (ad esempio modifica o injection) potremmo trovarci nella condizione di non poter distinguere più i dati attendibili da quelli non attendibili e quindi potrebbe risultare problematico garantire agli interessati di esercitare i propri diritti se non siamo in grado di verificare i dati di identità del richiedente con quelli registrati sui nostri sistemi.

Calamità Naturali

Effetti	Perdita di dati, Malfunzionamento, Interruzione di servizio,Violazione dei dati
Probabilità	1 (Improbabile)
Magnitudo	4 (Gravissimo)
Rischio	4 (Medio)

Contromisure	Sistemi di backup; Piano di Disaster Recovery e simulazioni; Replicazione SQL; Ridondanza geografica; Alta disponibilità; Failover HTTPS; sovradimensionamento delle risorse; Assurance; Monitoraggio; Banda garantita; Rete ridondata; Formazione;
Impatto sui diritti e le libertà degli interessati	In caso di **disservizio** gli interessati potrebbero temporaneamente non essere in grado di accedere ai sistemi informatici. Tuttavia possono esercitare i propri diritti contattandoci. In caso di **perdita** di dati non si evidenziano particolari limitazioni ai diritti degli interessati, se non la necessità di prestare nuovamente i consensi qualora si ritenesse necessario.

Problemi di rete

Effetti	Malfunzionamento, Interruzione di servizio
Probabilità	2 (Poco probabile)
Magnitudo	3 (Grave)
Rischio	6 (Alto)
Contromisure	Piano di Disaster Recovery e simulazioni; Replicazione SQL; Ridondanza geografica; Failover HTTPS; Sovradimensionamento delle risorse; Assurance; Monitoraggio; Banda garantita; Rete ridondata;
Impatto sui diritti e le libertà degli interessati	In caso di **disservizio** gli interessati potrebbero temporaneamente non essere in grado di accedere ai sistemi informatici. Tuttavia possono esercitare i propri diritti contattandoci.

Accesso fisico non autorizzato ai dati presenti sui server

Effetti	Malfunzionamento, Interruzione di servizio, Violazione
Probabilità	2 (Poco probabile)
Magnitudo	4 (Gravissimo)
Rischio	8 (Alto)
Contromisure	Controllo accessi ai data center
Impatto sui diritti e le libertà degli interessati	In caso di **disservizio** gli interessati potrebbero temporaneamente non essere in grado di accedere ai sistemi informatici. Tuttavia possono esercitare i propri diritti contattandoci. In caso di **perdita** di dati non si evidenziano particolari limitazioni ai diritti degli interessati, se non la necessità di prestare nuovamente i consensi qualora si ritenesse necessario. In caso di **violazione** dei dati (ad esempio modifica o injection) potremmo trovarci nella condizione di non poter distinguere più i dati attendibili da quelli non attendibili e quindi potrebbe risultare problematico garantire agli interessati di esercitare i propri diritti se non siamo in grado di verificare i dati di identità del richiedente con quelli registrati sui nostri sistemi. In caso di **sottrazione** dei dati si potrebbe verificare una limitazione delle libertà degli interessati, in quanto i dati potrebbero essere utilizzati per qualsiasi finalità, inclusi eventuali abusi o reati.

★ Tipi di dati trattati

Categoria	Descrizione
Dati Comuni	Sono tutte quelle informazioni come il nome, cognome, partita I.V.A., codice fiscale, indirizzo (compreso quello di posta elettronica), numeri di telefono, numero patente, che consentono di individuare una persona fisica o giuridica, sia essa anche un ente od associazione;
Dati Personali	Sono ad esempio i dati relativi ai gusti personali, alle preferenze di acquisto e altri dati non comuni;

Dati Anonimi	Dati che non sono riferibili ad una persona fisica identificata o identificabile o dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato

★ Soggetti interessati

Categoria	Descrizione
Partners	Merchants (Persone giuridiche) che utilizzano i nostri sistemi e servizi di commercio elettronico. Dipendenti e collaboratori dei partners autorizzati ad accedere al back-office del sito
Clienti	Visitatori del sito di commercio elettronico ed acquirenti
Haitex	Dipendenti e collaboratori di Haitex, inclusi gli amministratori di sistema

★ Categorie di dati trattati

Categoria	Descrizione	Tipologia
Anagrafici	Dati comuni e dati personali dei clienti del sito, dei Partners, dei dipendenti e collaboratori della nostra azienda o del Partner. Includono ad esempio il nome, il cognome e la ragione sociale), di chi paga gli ordini, di chi riceve le spedizioni e degli intestatari dei documenti fiscali	**Dati Comuni**
Identificativi	Ad esempio l'indirizzo IP, i cookie, le sessioni o il codice identificativo del dispositivo mobile. Il tipo di dispositivo in uso. Documenti di identità di clienti e partners	**Dati Personali**
Fatturazione	Ad esempio il codice fiscale, la partita iva e l'indirizzo per l'emissione di documenti fiscali. Le transazioni finanziarie (pagamenti). Le preferenze di pagamento. I documenti fiscali veri e propri	**Dati Personali**
Spedizione	Ad esempio l'indirizzo di spedizione, le lettere di vettura e le altre preferenze di spedizione	**Dati Personali**
Contatti	Ad esempio l'indirizzo email, gli indirizzi postali ed i numeri telefonici. Richieste di informazioni inviate da clienti	**Dati Personali**
Consumi	Ordini. Dati idonei a rivelare gusti, preferenze, abitudini di vita o di consumo (ad esempio l'elenco degli oggetti acquistati). Oggetti inseriti nei carrelli che non si sono tramutati in ordine. Oggetti visti di recente. Agevolazioni fiscali richieste negli ordini: Aliquote iva agevolata e detrazioni fiscali e relativi documenti richiesti	**Dati Personali**
Lingua	Dati idonei a rivelare l'appartenenza ad un gruppo linguistico (ad esempio la lingua preferita di navigazione del "portale/sito")	**Dati Personali**
Nazionalita	Dati idonei a rivelare l'origine nazionale (ad esempio la nazione di residenza, di nascita o da cui il cliente naviga nel sito)	**Dati Personali**
Pubblici	Ad esempio le recensioni ed i feedback lasciati dal cliente in merito a transazioni di commercio elettronico	**Dati Pubblici**
Affari Riservati	Dati sugli affari dei partners o della nostra azienda, tra cui: Documenti Fiscali, Magazzino Fiscale, Magazzino Virtuale, Ordini, Vendite, Clienti, Fornitori, Prezzi di Acquisto, Storico prezzi di Vendita, Prezzi riservati alle varie fasce B2B/B2P, dati relativi a servizi esterni (come ad esempio ebay, amazon), Lettere di vettura per le spedizioni degli ordini e tariffario delle spedizioni, Costi delle spedizioni e dei servizi	**Dati Personali,** **Dati Anonimi**

	esterni, Feeds per l'interscambio dati con ERP e marketplace esterni, Reports, Analisi, Codici Coupon. Contratti tra noi e i partners, tra partners e canali esterni	
Affari Pubblici	Schede descrittive dei prodotti che il Partner mette in vendita, inclusive di immagini, pdf, checklist, correlazioni	**Dati Pubblici**
Comunicazioni	Comunicazioni scambiate tramite email o sito tra clienti e partners e tra partners e noi. Tickets di assistenza aperti dal partner	**Dati Personali**
Admin	Dati accessibili agli amministratori di sistema: log delle attività svolte sul frontend, sul backend, dagli operatori da terminale e dai cron. Programmi applicativi, configurazioni di servizi e di sistemi operativi per il funzionamento della piattaforma e per l'analisi di mercato; Sistemi di monitoraggio; Personalizzazioni della piattaforma, Transazioni finanziarie (escluso trattamento diretto di carte di credito), Backup. Dati per il disaster recovery e la business continuity, per la replicazione dei sistemi. Dati amministrativi. Dati anonimi per lo studio dei comparatori di prezzo, dei carrelli abbandonati, dei patterns di acquisto, per gli A/B test e le statistiche, per l'attuazione della balanced scorecard dei Partner. Chiavi di crittografia GPG, certificati radice, certificati di revoca, certificati SSL clients, certificati di firma digitale e per l'autenticazione di dispositivi. Regole di firewall	**Dati Personali,** **Dati Anonimi**
Credenziali	Credenziali degli amministratori di sistema. Credenziali dei partners per l'accesso alla webapp o a sistemi esterni (come ad esempio marketplaces e comparatori)	**Dati Personali**

★ Finalità del trattamento dei dati

Le nostre finalità sono:

- ➔ consentire ai clienti di acquistare online e di soddisfare le proprie necessità di consumo;
- ➔ consentire ai partner di esporre e vendere online i propri prodotti per mezzo della nostra piattaforma software;
- ➔ gestire campagne marketing, fornire consulenza e supporto tecnico ai partner per migliorare le performance;
- ➔ fornire assistenza tecnica agli utenti del sito in caso di problemi di natura tecnica.

In maniera più estesa le nostre finalità includono trattamenti dei dati per:

Fornitura di beni e servizi

Gestire ordini, fornire prodotti e servizi, elaborare pagamenti, comunicare con clienti e partner in merito a ordini, prodotti, servizi ed offerte promozionali; rispondere a richieste dei clienti; aggiornare i nostri archivi; gestire gli account personali dei clienti ed offrire la consultazione dei propri dati e la possibilità di esprimere commenti sulle transazioni ("feedback");

Attività di marketing

Effettuare comunicazioni commerciali non sollecitate di cui abbiamo acquisito preventivamente il consenso facoltativo, attività di remarketing e retargeting utilizzando strumenti di terze parti; Statistiche e monitoraggio dell'efficacia dei nostri servizi.

Personalizzazione e Profilazione

Personalizzare la visualizzazione di contenuti e migliorare la navigazione sul sito e l'esperienza di acquisto dei clienti. Grazie a questo trattamento ad esempio possiamo mostrare l'elenco degli articoli visti di recente e consigliare prodotti e servizi che potrebbero essere di interesse.

★ Inventario e collocazione dei dati trattati

L'infrastruttura tecnologica di Haitex è collocata in ITALIA presso i data center del provider SEEWEB, selezionato per l'alta qualità dei servizi erogati. Seeweb è da sempre attenta ad offrire ai clienti il massimo della qualità dei servizi che propone, per questo si è dotata delle più importanti certificazioni di qualità e di processo oggi disponibili, ovvero: **CISPE, ISO 9001:2015, ISO 27001:2013, ISO 14001:2015.**

	Categorie di dati trattati per ogni soggetto interessato		
Collocazione Logica	**Clienti**	**Partners**	**Haitex**
Cloud Servers	Anagrafici, Identificativi, Fatturazione, Spedizione, Contatti, Consumi, Lingua, Nazionalita, Comunicazioni, Pubblici	Affari Riservati, Affari Pubblici, Comunicazioni, Credenziali, Anagrafici, Contatti	Admin, Credenziali, Anagrafici, Affari Riservati
S3 Cloud Object Storage	Fatturazione	Affari Riservati	Backup, Admin
Cloud Drive	Nessuno	Affari Riservati, Credenziali	Affari Riservati
End-points	Nessuno	Affari Riservati, Credenziali	Admin, Affari Riservati

★ Attività di trattamento

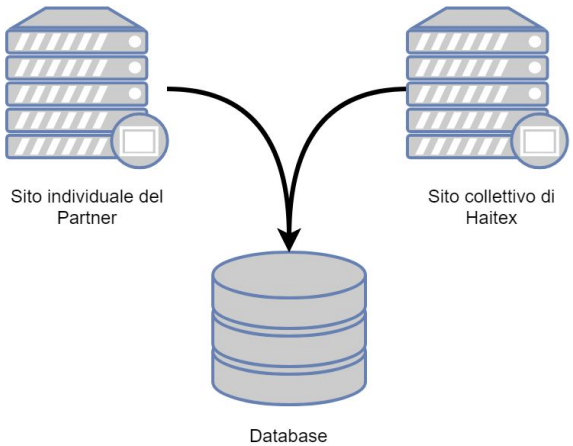
Categorie di dati	Categorie di Soggetti	Descrizione funzionale del trattamento, motivazione e durata della conservazione
Anagrafici, Identificativi, Spedizione, Contatti, Consumi, Lingua, Nazionalità, Comunicazioni	Clienti	**Raccolta**: i dati vengono immessi direttamente dai clienti all'interno del sito, fornendo un consenso informato prima del trattamento. **Utilizzo**: conserviamo questi dati per consentire al cliente di effettuare ordini successivi in maniera facilitata. Inoltre per consentire al cliente l'accesso all'area privata, da cui può consultare i propri dati, lo storico degli ordini (anche per effettuare ordini simili), dei documenti fiscali e delle comunicazioni. Conserviamo i dati anche per finalità statistiche anonime. **Elaborazione**: effettuiamo statistiche sui dati per valutare l'efficacia delle campagne marketing o per migliorare la qualità dei servizi che eroghiamo. Effettuiamo attività di profilazione, per la quale richiediamo un consenso esplicito facoltativo. **Conservazione**: i dati vengono conservati per un periodo non superiore ai 10 anni dall'ultima attività registrata, trascorso tale termine vengono resi anonimi o cancellati. I dati provenienti da Amazon vengono resi trascorsi 30 giorni dall'avvenuta spedizione. **Necessità**: i dati raccolti sono necessari per poter ottemperare al contratto di compravendita con i clienti. Per questo il consenso è obbligatorio. Per le attività di profilazione invece richiediamo un consenso separato e facoltativo e per noi è necessario al fine di ottimizzare i costi delle campagne pubblicitarie oltre che evitare di infastidire il cliente con pubblicità non attinenti ai propri interessi. **Liceità**: il trattamento è lecito perchè l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Inoltre perché il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; **Modificazione**: su richiesta dei clienti o dei partners possiamo modificare i dati per aggiornarli. **Destinatari/Comunicazione**: quando un cliente richiede informazioni o acquista prodotti di un Partner per mezzo della nostra piattaforma, comunichiamo a questo Partner (e solo a lui) i dati per consentirgli di rispondere alla richiesta ed evadere l'ordine. Il partner diviene titolare dei dati in questione; **Diffusione**: i dati non vengono diffusi in alcun modo; **Restrizioni**: il cliente può esercitare il diritto di opposizione o di applicare delle limitazioni al trattamento. **Blocco e oblio**: il cliente può richiedere autonomamente ed in qualsiasi momento il blocco dell'area privata. Inoltre può richiedere a noi l'anonimizzazione o la cancellazione dei propri dati personali (diritto all'oblio). **Portabilità**: il cliente può esercitare il diritto di accesso ed alla portabilità dei dati. **Proporzionalità ed adeguatezza del trattamento**: i dati raccolti sono quelli minimi necessari per erogare il servizio; il trattamento dei dati è lecito, proporzionale ed adeguato agli scopi per cui sono stati raccolti.
Fatturazione	Clienti	**Raccolta**: i dati vengono immessi direttamente dai clienti all'interno del sito, fornendo un consenso informato prima del trattamento.

		Utilizzo: conserviamo questi dati per emettere documenti fiscali al cliente e per consentirgli di esercitare il diritto di recesso, il diritto di garanzia e di ristampare in futuro vecchi documenti fiscali. I documenti emessi sono infatti consultabili e scaricabili dall'area privata. Conserviamo i dati anche per obblighi di legge e per le finalità fiscali dei nostri partners. **Elaborazione**: elaboriamo i dati fiscali raggruppandoli per cliente in modo da quantificare i volumi di spesa effettuati. Esportiamo report fiscali come ad esempio la prima nota o il registro dei corrispettivi. **Conservazione**: i dati vengono conservati a tempo indeterminato e per almeno 10 anni perché imposto dalla legge in materia fiscale. **Necessità**: i dati raccolti sono necessari per poter ottemperare al contratto di compravendita con i clienti. Per questo il consenso è obbligatorio. Qualora il cliente volesse rinunciare alla possibilità di consultazione delle fatture attraverso la propria area privata può richiederne il blocco. **Liceità**: il trattamento è lecito perchè l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Inoltre perché il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; Inoltre perchè il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; **Modificazione**: i documenti emessi non possono essere modificati, pertanto il cliente non può esercitare questo diritto sui documenti fiscali già emessi. **Destinatari/Comunicazione**: quando un cliente acquista prodotti di un Partner per mezzo della nostra piattaforma, comunichiamo a questo Partner (e solo a lui) i dati per consentirgli di emettere i documenti fiscali. Il partner è titolare dei dati in questione; **Diffusione**: i dati non vengono diffusi in alcun modo; **Restrizioni**: il cliente non può esercitare il diritto di opposizione o di applicare delle limitazioni al trattamento. **Blocco e oblio**: il cliente può richiedere autonomamente ed in qualsiasi momento il blocco dell'area privata. Non può però richiedere l'anonimizzazione o la cancellazione dei propri dati personali (diritto all'oblio) sui documenti fiscali. **Portabilità**: il cliente può esercitare il diritto di accesso ed alla portabilità dei dati. **Proporzionalità ed adeguatezza del trattamento**: i dati raccolti sono quelli minimi necessari per erogare il servizio; il trattamento dei dati è lecito, proporzionale ed adeguato agli scopi per cui sono stati raccolti.
Pubblici	Clienti	**Raccolta**: i dati vengono immessi facoltativamente dai clienti all'interno del sito o di altri siti, in forma anonima, utilizzando uno pseudonimo oppure il nome reale a propria discrezione. **Utilizzo**: Conserviamo i feedback e le recensioni per consentire agli utenti di conoscere il grado di qualità dei siti che gestiamo. **Elaborazione**: Facciamo statistiche per valutare la soddisfazione dei clienti e per capire cosa dobbiamo migliorare al fine di soddisfare maggiormente i clienti. Utilizziamo anche questi dati per assicurarci che i partners lavorino con alti standard qualitativi. **Conservazione**: i dati vengono conservati a tempo indeterminato. **Necessità**: i dati non personali non sono soggetti a questa valutazione. **Liceità**: i dati non personali non sono soggetti a questa valutazione. **Modificazione**: il cliente può richiedere la modificazione dei dati; **Destinatari/Comunicazione**: i dati vengono diffusi sul sito internet; **Diffusione**: i dati vengono diffusi sul sito internet; **Restrizioni**: il cliente non può esercitare il diritto di opposizione o di applicare delle limitazioni al trattamento in quanto i dati in questione non sono personali. **Blocco e oblio**: il cliente può richiedere l'anonimizzazione dei dati ma non il blocco. **Portabilità**: il cliente può esercitare il diritto di accesso ed alla portabilità dei dati. **Proporzionalità ed adeguatezza del trattamento**: i dati non personali non sono soggetti a questa valutazione.
Anagrafici, Contatti	Partners	**Raccolta**: i dati vengono forniti direttamente dai partners contestualmente o successivamente alla stipula del contratto con la nostra azienda per l'erogazione dei nostri servizi informatici. **Utilizzo**: conserviamo questi dati per consentire l'erogazione dei nostri servizi e li archiviamo per proteggerci da eventuali azioni legali. **Elaborazione**: i dati vengono visualizzati ed immessi all'interno dei nostri archivi informatici. **Conservazione**: i dati vengono conservati per un periodo non superiore ai 10 anni dall'ultima attività registrata, trascorso tale termine vengono resi anonimi o cancellati. **Necessità**: i dati raccolti sono necessari per poter ottemperare al contratto di compravendita con i clienti. Per questo il consenso è obbligatorio. Per le attività di

		profilazione invece richiediamo un consenso separato e facoltativo e per noi è necessario al fine di ottimizzare i costi delle campagne pubblicitarie oltre che evitare di infastidire il cliente con pubblicità non attinenti ai propri interessi. **Liceità**: il trattamento è lecito perchè l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Inoltre perché il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; **Modificazione**: su richiesta dei clienti o dei partners possiamo modificare i dati per aggiornarli. **Destinatari/Comunicazione**: quando un cliente richiede informazioni o acquista prodotti di un Partner per mezzo della nostra piattaforma, comunichiamo a questo Partner (e solo a lui) i dati per consentirgli di rispondere alla richiesta ed evadere l'ordine. Il partner diviene titolare dei dati in questione; **Diffusione**: i dati non vengono diffusi in alcun modo; **Restrizioni**: il cliente può esercitare il diritto di opposizione o di applicare delle limitazioni al trattamento. **Blocco e oblio**: il cliente può richiedere autonomamente ed in qualsiasi momento il blocco dell'area privata. Inoltre può richiedere a noi l'anonimizzazione o la cancellazione dei propri dati personali (diritto all'oblio). **Portabilità**: il cliente può esercitare il diritto di accesso ed alla portabilità dei dati. **Proporzionalità ed adeguatezza del trattamento**: i dati raccolti sono quelli minimi necessari per erogare il servizio; il trattamento dei dati è lecito, proporzionale ed adeguato agli scopi per cui sono stati raccolti.
Affari Riservati, Credenziali	Partners	**Raccolta**: i dati vengono forniti direttamente dai partners oppure raccolti da noi nel tempo. **Utilizzo**: conserviamo questi dati per consentire l'erogazione dei nostri servizi. I dati in questione sono coperti da specifiche clausole di non disclosure agreement". **Elaborazione**: i dati possono essere utilizzati per qualsiasi tipo di elaborazione. **Conservazione**: i dati vengono conservati fino alla risoluzione del contratto. Trascorso questo termine verranno riconsegnati agli interessati, resi anonimi, o distrutti. **Necessità**: i dati raccolti sono necessari per poter ottemperare al contratto di erogazione dei nostri servizi. **Liceità**: il trattamento è lecito perché è necessario all'esecuzione di un contratto di cui l'interessato è parte. Inoltre i dati in questione sono coperti da specifiche clausole contrattuali di "non disclosure agreement"; **Modificazione**: su richiesta possiamo modificare i dati per aggiornarli. **Destinatari/Comunicazione**: in alcuni casi ci troviamo nella necessità di fornire un sottoinsieme di dati a fornitori esterni, come ad esempio Google, Facebook, Trovaprezzi. E' nostro impegno comunque fornire solo un insieme limitato di dati con il solo ed unico scopo di promuovere gli affari del partner e certo non di arrecargli danno; **Diffusione**: i dati non vengono diffusi in alcun modo; **Restrizioni**: il partner può esercitare il diritto di opposizione o di applicare delle limitazioni al trattamento. **Blocco e oblio**: il partner può richiedere a l'anonimizzazione o la cancellazione dei propri dati personali (diritto all'oblio). **Portabilità**: il partner può esercitare il diritto di accesso ed alla portabilità dei dati. **Proporzionalità ed adeguatezza del trattamento**: i dati raccolti sono quelli minimi necessari per erogare il servizio; il trattamento dei dati è lecito, proporzionale ed adeguato agli scopi per cui sono stati raccolti.
Comunicazioni, Affari pubblici	Partners	**Raccolta**: i dati vengono forniti direttamente dai partners oppure dai clienti. **Utilizzo**: conserviamo questi dati (che includono ad esempio le schede prodotto, i prezzi, le disponibilità ma anche le comunicazioni bidirezionali tra clienti e partner) per consentire l'erogazione dei nostri servizi, per tenere traccia di tutte le richieste relative alle compravendite o alle mancate vendite e per offrire al cliente la possibilità di consultare lo storico di tutte le comunicazioni. Visualizziamo alcune comunicazioni al fine di individuare eventuali carenze nelle descrizioni dei prodotti o nel sito che devono essere risolte per aumentare le vendite. A campione prendiamo anche visione delle comunicazioni per consigliare il partner sulle migliori tecniche comunicative e per smascherare eventuali pratiche scorrette di partners a danno dei clienti o della nostra azienda. **Elaborazione**: i dati possono essere utilizzati per qualsiasi tipo di elaborazione. **Conservazione**: i dati vengono conservati per un periodo non superiore a 10 anni oltre la data di risoluzione del contratto. Trascorso questo termine i dati verranno resi anonimi, o distrutti. Conserviamo i dati oltre la scadenza del contratto con il partner per consentire al cliente la fruizione dello storico (che potrà continuare ad accedere allo storico) anche quando il contratto tra noi ed il partner è cessato.

		Necessità: i dati raccolti sono necessari per poter ottemperare al contratto di erogazione dei nostri servizi e per offrire al cliente lo storico di tutte le comunicazioni. **Liceità**: il trattamento è lecito perché è necessario all'esecuzione di un contratto di cui l'interessato è parte. Inoltre i dati in questione sono coperti da specifiche clausole contrattuali di "non disclosure agreement"; **Modificazione**: su richiesta possiamo modificare i dati per aggiornarli. **Destinatari/Comunicazione**: i dati non vengono comunicati ad altri soggetti. **Diffusione**: i dati non vengono diffusi in alcun modo; **Restrizioni**: il partner può esercitare il diritto di opposizione o di applicare delle limitazioni al trattamento. **Blocco e oblio**: il partner può richiedere l'anonimizzazione o la cancellazione dei propri dati personali (diritto all'oblio). **Portabilità**: il partner può esercitare il diritto di accesso ed alla portabilità dei dati. **Proporzionalità ed adeguatezza del trattamento**: i dati raccolti sono quelli minimi necessari per erogare il servizio; il trattamento dei dati è lecito, proporzionale ed adeguato agli scopi per cui sono stati raccolti.
Credenziali, Anagrafici	Haitex	Conserviamo i dati anagrafici dei nostri collaboratori e le credenziali di accesso ai nostri sistemi fino alla risoluzione del rapporto di collaborazione. **Conservazione Massima: Fino alla risoluzione del rapporto di collaborazione** **Portabilità: Consentita - Diritto all'Oblio: Consentito - Anonimizzazione: Consentita**
Affari Riservati, Admin, Backup	Haitex	Conserviamo i dati riservati della nostra azienda con la massima cura perché rappresentano il nostro principale asset. Questi includono il know-how, le procedure, l'architettura, i documenti commerciali e tecnici, le progettazioni, il codice sorgente, etc. **Conservazione Massima: Tempo Illimitato** **Portabilità: Consentita - Diritto all'Oblio: Consentito - Anonimizzazione: Consentita**

★ Sistemi di raccolta dei dati personali



Raccogliamo i dati personali prevalentemente per mezzo di due canali principali. Un sito collettivo di nostra proprietà (www.haistore.it) ei vari siti individuali dei partners.
Su tutti i siti che gestiamo, siano essi di nostra proprietà o di proprietà dei partners, gli unici metodi di acquisizione dei dati personali sono quelli che seguono:

- Registrazione
- Ordine
- Richiesta informazioni
- Avvisami quando il prodotto torna disponibile
- Avvisami quando il prodotto scende di prezzo
- Iscrizione alla newsletter
- Contatto telefonico
- Contatto via email
- Raccolta automatica

Registrazione

Mediante il processo di registrazione, i clienti ci inviano spontaneamente i propri dati personali con lo scopo di ottenere un account gratuito all'interno di uno o più siti che gestiamo. Uno dei motivi per cui i clienti si iscrivono è quello di poter accedere a prezzi riservati al sistema B2B. Durante la fase di registrazione, il cliente, oltre ad inviarci spontaneamente i propri dati, accetta il regolamento del sito ed esprime il consenso preventivo, informato, facoltativo e separato per:

- essere contattato telefonicamente per comunicazioni commerciali non sollecitate;
- essere contattato via email per comunicazioni commerciali non sollecitate;
- essere profilato per fini di marketing;

La registrazione avviene solamente sul sito individuale del Partner.
La nostra azienda è titolare dei dati raccolti. Per le stesse finalità e contestualmente alla raccolta, i dati vengono comunicati al partner, che ne diviene a sua volta titolare.
Durante la fase di registrazione il cliente deve obbligatoriamente accettare il regolamento del sito e può prestare facoltativamente tre consensi separati, rispettivamente per la profilazione, per la ricezione di comunicazioni non sollecitate via email, per la ricezione di comunicazioni non sollecitate via telefono.
Contestualmente alla registrazione la piattaforma genera un messaggio email transazionale indirizzato al cliente, al partner e ad alla nostra azienda come conferma di accettazione del regolamento e riporta tutti i consensi prestati con la sintesi dei diritti dell'utente, il collegamento all'informativa estesa sulla privacy ed al download di questo documento.
L'informativa per la privacy è inclusa nel regolamento del sito in versione integrale. Tuttavia per ulteriori approfondimenti il cliente può scaricare il presente documento dall'indirizzo https://www.haistore.it/GDPR_Compliance.pdf
Il cliente può consultare, prestare o revocare i consensi, accedendo autonomamente all'interno della propria area privata oppure contattando la nostra azienda.

Ordine

Mediante il processo di ordinazione, i clienti ci inviano spontaneamente i propri dati personali con lo scopo di effettuare un acquisto. Durante la fase di ordinazione, il cliente, oltre ad inviarci spontaneamente i propri dati, accetta il regolamento del sito ed esprime il consenso preventivo, informato, facoltativo e separato per:

- essere contattato telefonicamente per comunicazioni commerciali non sollecitate;
- essere contattato via email per comunicazioni commerciali non sollecitate;
- essere profilato per fini di marketing;

I consensi non prestati durante la fase di ordinazione sono interpretati dalla piattaforma come intenzione di revoca di eventuali consensi eventualmente prestati precedentemente.
L'ordine avviene sia sul sito individuale del Partner che sul sito collettivo.
La nostra azienda è titolare dei dati raccolti. Per le stesse finalità e contestualmente alla raccolta, i dati vengono comunicati al partner, che ne diviene a sua volta titolare.
Contestualmente alla ricezione dell'ordine la piattaforma genera un messaggio email transazionale indirizzato al cliente, al partner e ad alla nostra azienda come conferma di accettazione del regolamento e riporta tutti i consensi prestati e revocati con la sintesi dei diritti dell'utente, il collegamento all'informativa estesa sulla privacy ed al download di questo documento.
L'informativa per la privacy è inclusa nel regolamento del sito in versione integrale. Tuttavia per ulteriori approfondimenti il cliente può scaricare il presente documento dall'indirizzo https://www.haistore.it/GDPR_Compliance.pdf

Richiesta Informazioni, Avvisami quando il prodotto torna disponibile, Avvisami quando il prodotto scende di prezzo, Iscrizione alla newsletter

Mediante questi processi, i clienti ci inviano spontaneamente i propri dati personali con lo scopo di iscriversi alla newsletter, di ottenere informazioni su prodotti, ordini o di altra natura oppure di ricevere una notifica che il prodotto di proprio interesse ha subito un ribasso del prezzo o una variazione di disponibilità. Durante questi processi, il cliente, oltre ad inviarci spontaneamente i propri dati, accetta il regolamento del sito ed esprime il consenso preventivo, informato, facoltativo e separato solamente per:

- essere contattato via email per comunicazioni commerciali non sollecitate;

La raccolta avviene sia sul sito individuale del Partner che sul sito collettivo, ed i dati sono di titolarità sia del Partner in questione che della nostra azienda.
Contestualmente alla ricezione della richiesta, la piattaforma genera un messaggio email transazionale indirizzato al cliente, al partner e ad alla nostra azienda come conferma di accettazione del regolamento e riporta tutti i consensi prestati e revocati con la sintesi dei diritti dell'utente, il collegamento all'informativa estesa sulla privacy ed al download di questo documento.
L'informativa per la privacy è inclusa nel regolamento del sito in versione integrale. Tuttavia per ulteriori approfondimenti il cliente può scaricare il presente documento dall'indirizzo https://www.haistore.it/GDPR_Compliance.pdf

Contatto telefonico, Contatto via e-mail

In alcuni casi i clienti ci telefonano o ci chiedono di essere chiamati via telefono e ci inviano spontaneamente i propri dati personali con lo scopo di ottenere un servizio.

L'informativa per la privacy è inclusa nel regolamento del sito in versione integrale. Tuttavia per ulteriori approfondimenti il cliente può scaricare il presente documento dall'indirizzo https://www.haistore.it/GDPR_Compliance.pdf
Il cliente può consultare, prestare o revocare i consensi, accedendo autonomamente all'interno della propria area privata oppure contattando la nostra azienda.

Dati raccolti sui Marketplaces

Una nota particolare va espressa in merito ai dati che vengono raccolti per il tramite di marketplaces esterni, che possono essere utilizzati per le sole finalità transazionali e non per altre finalità. I dati raccolti tramite Amazon vengono resi anonimi dopo 30 giorni dalla spedizione.

Soggetti a cui comunichiamo i dati

Partners

All'interno della nostra piattaforma confluiscono tutti i dati personali che vengono raccolti. Per le stesse finalità per cui sono stati raccolti e con i relativi consensi/revoche, comunichiamo i dati personali al partner interessato, che ne acquisisce la titolarità. La titolarità ed il trattamento dei partner è ristretto ai soli dati di propria pertinenza e non ai dati degli altri partners.

Poiché il numero di partners è in rapida evoluzione, conserviamo in un apposito registro l'elenco di tutti i soggetti a cui abbiamo, anche in passato, comunicato dati personali.

Tutti i partners hanno comunque sottoscritto un apposito contratto con la nostra azienda in cui molte procedure, anche relative alla sicurezza dei dati, sono state regolamentate.

Data processors esterni

In alcuni casi comunichiamo i dati personali anche a soggetti esterni, comunque residenti nell'Unione Europea, al fine di poter erogare una parte dei nostri servizi.

Seeweb	Seeweb è il nostro fornitore dell'infrastruttura tecnologica su cui risiedono i nostri server ed i nostri archivi dati
Sendinblue	Utilizziamo in alcuni casi il servizio sendinblue per l'invio di comunicazioni email massive
Trovaprezzi	Inviamo a Trovaprezzi alcuni dati sugli acquisti effettuati dagli utenti provenienti dalla propria piattaforma al fine di consentire l'esecuzione del trusted program e di raccogliere le recensioni da parte degli utenti
Bestshopping	Inviamo a Bestshopping alcuni dati sugli acquisti effettuati dagli utenti provenienti dalla propria piattaforma al fine di consentire l'emissione di rimborsi agli utenti (cashback)
Google	Utilizziamo google analytics per migliorare la qualità dei servizi che eroghiamo e per offrire la traduzione automatica delle pagine di nostri siti agli utenti.
Facebook	In alcuni casi usiamo i servizi pubblicitari di facebook ad esempio per il remarketing

Incaricati e responsabili del trattamento dei dati

Disponiamo di un elenco aggiornato di tutte le persone nominate incaricati o responsabili del trattamento dei dati personali, conservato separatamente al presente documento.
Ad ogni incaricato o responsabile sottoponiamo la nostra policy in materia di privacy, eroghiamo uno specifico corso di formazione e raccogliamo la firma di accettazione dell'incarico.

Distribuzione dei compiti e delle responsabilità

In questa sezione sono descritte sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Amministrazione	Fatturazione attiva, Acquisti e gestione fornitori, Controllo della corretta erogazione dei servizi (ciclo produttivo), Adempimenti societari, Controllo dell'acquisizione nuovi clienti, Contabilità	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati quali salvataggi, ripristini, ecc
Commerciale	Cercare nuove aziende quali potenziali clienti, Formulare offerte commerciali, Controllare la situazione contabile dei clienti	acquisizione e caricamento dei dati, consultazione.
Tecnica	Erogazione dei servizi informatici (Ciclo produttivo)	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati quali salvataggi, ripristini, ecc
Datacenter (esterna)	Hosting dei Dati	Backup dei Dati, Alta disponibilità dei dati, Controllo Sicurezza fisica dell'accesso ai dati.
Contabilità (esterna)	Contabilità e adempimenti fiscali	acquisizione e caricamento dei dati, consultazione, comunicazione a terzi ove richiesto, manutenzione tecnica dei propri programmi, gestione tecnica operativa della propri base dati quali salvataggi, ripristini, ecc