Orderlion GmbH

Accordo sul trattamento dei dati (DPA)

Versione 2.2 · In vigore dal 1° ottobre 2026 · Orderlion GmbH

Nota: la versione inglese di questo documento è la versione facente fede. Questa versione italiana è una traduzione automatica fornita esclusivamente per facilitarne la comprensione.

Il presente accordo sul trattamento dei dati ("DPA") costituisce parte integrante del contratto tra **Orderlion GmbH**, Himmelpfortgasse 17/7, 1010 Vienna, Austria ("**Orderlion**", il responsabile del trattamento) e il cliente identificato nel Modulo d'ordine ("**Cliente**", il titolare del trattamento) per la piattaforma Orderlion (il "Contratto"). Esso è concluso in forma elettronica (Art 28(9) GDPR) mediante incorporazione nel Contratto secondo il Modulo d'ordine e la Sezione 12 delle CGC. Per la materia della protezione dei dati, il presente DPA prevale sulle CGC.

1. Ruoli e ambito di applicazione

1.1 Per i dati personali trattati sulla piattaforma per conto del Cliente (in particolare i dati degli acquirenti del Cliente e del loro personale, i dati degli ordini, le comunicazioni e il contenuto delle email trattato tramite Inbox: congiuntamente "**Dati personali del Cliente**", descritti nell'Allegato 1), il Cliente è titolare del trattamento e Orderlion è responsabile del trattamento.

1.2 Il presente DPA non si applica ove Orderlion sia essa stessa titolare del trattamento (ad es. dati di contatto del personale del Cliente per la gestione dell'account, la fatturazione e l'assistenza, nonché dati d'uso pseudonimizzati per le analisi di prodotto ai sensi della Sezione 3.5); tale trattamento è descritto nell'Informativa sulla privacy di Orderlion.

2. Descrizione del trattamento

L'oggetto, la durata, la natura e la finalità del trattamento, i tipi di dati personali e le categorie di interessati sono indicati nell'**Allegato 1**.

3. Istruzioni

3.1 Orderlion tratta i Dati personali del Cliente esclusivamente sulla base delle istruzioni documentate del Cliente, anche con riguardo ai trasferimenti verso paesi terzi, salvo che sia tenuta al trattamento dal diritto dell'Unione o degli Stati membri; in tal caso Orderlion informa il Cliente di tale obbligo giuridico prima del trattamento, salvo che la legge lo vieti per rilevanti motivi di interesse pubblico.

3.2 Le istruzioni documentate consistono in: il presente DPA, il Contratto, la configurazione della piattaforma da parte del Cliente (inclusa la modalità di trattamento Inbox prescelta e l'opzione di hosting nell'UE) e ulteriori istruzioni in forma testuale. Le istruzioni che richiedono servizi eccedenti l'ambito del Contratto possono essere fatturate alle tariffe standard di Orderlion.

3.3 Orderlion informa il Cliente senza ingiustificato ritardo qualora, a suo giudizio, un'istruzione violi il GDPR o altre disposizioni in materia di protezione dei dati dell'Unione o degli Stati membri, e può sospendere l'esecuzione di tale istruzione fino a quando non sia confermata o modificata.

3.4 Il Cliente incarica e autorizza Orderlion a creare statistiche aggregate e anonimizzate a partire dai Dati personali del Cliente ai fini del miglioramento del prodotto, a condizione che i risultati non contengano dati personali e non identifichino il Cliente, i suoi utenti o i suoi acquirenti. L'anonimizzazione è effettuata nell'ambito di tale istruzione.

3.5 **Analisi di prodotto.** Orderlion tratta inoltre dati d'uso pseudonimizzati degli utenti della piattaforma (un identificativo utente pseudonimo insieme all'utilizzo delle funzionalità, agli eventi di interazione e alle informazioni sul dispositivo; non nomi, dati di contatto, contenuti degli ordini o contenuto delle email) in qualità di titolare del trattamento autonomo per migliorare, mettere in sicurezza e sviluppare i propri servizi, come descritto nella sua Informativa sulla privacy; si applica la Sezione 1.2. Orderlion non comunica tali dati d'uso a terzi diversi dai propri responsabili del trattamento, non li utilizza per fare pubblicità agli acquirenti del Cliente e li cancella o anonimizza al più tardi 2 anni dopo la raccolta.

4. Riservatezza

Orderlion garantisce che tutte le persone autorizzate a trattare i Dati personali del Cliente siano vincolate da obblighi di riservatezza contrattuali o legali, che sopravvivono alla cessazione del loro incarico.

5. Sicurezza del trattamento

Orderlion attua e mantiene le misure tecniche e organizzative indicate nell'**Allegato 3** (Art 32 GDPR). Orderlion può aggiornare tali misure a condizione che il livello complessivo di sicurezza non sia sostanzialmente ridotto.

6. Sub-responsabili del trattamento

6.1 Il Cliente concede un'autorizzazione scritta generale al ricorso ai sub-responsabili del trattamento elencati nell'**Allegato 2**. L'elenco aggiornato dei sub-responsabili del trattamento è pubblicato all'indirizzo www.orderlion.com/it/subprocessors e indica la data dell'ultimo aggiornamento.

6.2 Orderlion informa il Cliente di qualsiasi aggiunta o sostituzione prevista di sub-responsabili del trattamento almeno **30 giorni** prima dell'incarico, mediante email al contatto designato dal Cliente e mediante aggiornamento dell'elenco pubblicato. La comunicazione contiene le informazioni necessarie a valutare la modifica.

6.3 Il Cliente può opporsi entro il termine di preavviso per ragionevoli motivi attinenti alla protezione dei dati, in forma testuale. In tal caso le parti cercano anzitutto una soluzione in buona fede (incluse alternative tecniche che evitino il nuovo sub-responsabile del trattamento per i dati del Cliente). Se non viene trovata alcuna soluzione entro 30 giorni dall'opposizione, il Cliente può risolvere i servizi interessati con rimborso pro-rata dei corrispettivi prepagati per i servizi risolti; questo è il rimedio esclusivo per un'opposizione a un sub-responsabile del trattamento. Se il Cliente non si oppone entro il termine di preavviso, la modifica si considera approvata.

6.4 Orderlion impone a ogni sub-responsabile del trattamento, per contratto, obblighi in materia di protezione dei dati sostanzialmente equivalenti a quelli previsti dal presente DPA, in particolare garanzie sufficienti di adeguate misure tecniche e organizzative. Su richiesta, Orderlion fornisce al Cliente una copia delle pertinenti condizioni contrattuali del sub-responsabile del trattamento (con omissione dei segreti commerciali). Orderlion resta pienamente responsabile nei confronti del Cliente per l'adempimento degli obblighi in materia di protezione dei dati da parte dei propri sub-responsabili del trattamento.

7. Trattamento tramite IA

7.1 La funzionalità Inbox e le altre funzionalità di IA trattano i Dati personali del Cliente utilizzando modelli linguistici di grandi dimensioni dei sub-responsabili del trattamento IA indicati nell'Allegato 2, inclusa la regione di hosting e la configurazione di conservazione di ciascun fornitore.

7.2 **Nessun addestramento.** Orderlion non utilizza i Dati personali del Cliente per addestrare, perfezionare o migliorare modelli di apprendimento automatico disponibili al di fuori dell'account del Cliente stesso, e garantisce

contrattualmente che i propri sub-responsabili del trattamento IA non utilizzino i Dati personali del Cliente trasmessi tramite Orderlion per addestrare i propri modelli.

7.3 **Opzione IA ospitata nell'UE.** Su richiesta scritta del Cliente in fase di configurazione, confermata da Orderlion, il trattamento tramite IA per l'account del Cliente è effettuato esclusivamente su infrastruttura situata nell'UE. Per tali account, l'estrazione degli ordini avviene su modelli Anthropic Claude forniti tramite AWS Bedrock nell'UE (Francoforte), e OpenAI non è utilizzato. L'Allegato 2 individua la catena di trattamento applicabile a questa opzione.

7.4 **Conservazione presso i fornitori.** I sub-responsabili del trattamento IA conservano i contenuti trasmessi esclusivamente secondo le configurazioni di conservazione indicate nell'Allegato 2.

7.5 Gli output di IA sono estrazioni e suggerimenti soggetti ai meccanismi di verifica descritti nel Contratto; la piattaforma non adotta decisioni basate unicamente sul trattamento automatizzato che producano effetti giuridici nei confronti degli interessati (Art 22 GDPR).

8. Diritti degli interessati

Orderlion inoltra al Cliente, senza ingiustificato ritardo, qualsiasi richiesta di un interessato ricevuta in relazione ai Dati personali del Cliente, e non vi risponde se non secondo istruzioni. Tenendo conto della natura del trattamento, Orderlion assiste il Cliente con adeguate misure tecniche e organizzative (incluse le funzioni di esportazione, correzione e cancellazione della piattaforma) nell'adempimento delle richieste ai sensi del Capo III GDPR.

9. Violazione dei dati personali

9.1 Orderlion notifica al Cliente una violazione dei dati personali che riguardi i Dati personali del Cliente **senza ingiustificato ritardo, al più tardi entro 72 ore dal momento in cui ne viene a conoscenza**.

9.2 La notifica descrive, per quanto noto: la natura della violazione (ove possibile: le categorie e il numero approssimativo di interessati e di record interessati), un punto di contatto, le probabili conseguenze e le misure adottate o proposte. Le informazioni possono essere fornite in fasi successive senza ingiustificato ritardo, man mano che divengono disponibili.

9.3 La valutazione del rischio ed eventuali notifiche alle autorità di controllo (Art 33) e agli interessati (Art 34) sono responsabilità del Cliente; Orderlion presta una ragionevole cooperazione e non notifica alle autorità o agli interessati per conto del Cliente, salvo che sia diversamente concordato separatamente.

10. Assistenza (Art 32-36 GDPR)

Tenendo conto della natura del trattamento e delle informazioni a sua disposizione, Orderlion assiste il Cliente nel garantire il rispetto degli Artt 32-36 GDPR (sicurezza, notifiche di violazione, valutazioni d'impatto sulla protezione dei dati, consultazione preventiva). L'assistenza che ecceda sostanzialmente le informazioni disponibili dal presente DPA, dai suoi allegati e dalla documentazione pubblicata può essere fatturata alle tariffe standard di Orderlion.

11. Dimostrazione della conformità e audit

11.1 Orderlion mette a disposizione le informazioni necessarie a dimostrare la conformità all'Art 28 GDPR: il presente DPA e i suoi allegati, le misure tecniche e organizzative vigenti e risposte scritte a ragionevoli questionari di audit (in regime di riservatezza).

11.2 Ove tali informazioni siano insufficienti a dimostrare la conformità, ovvero ove un audit sia richiesto da un'autorità di controllo o faccia seguito a una violazione dei dati personali che riguarda il Cliente, il Cliente (o un revisore indipendente da esso incaricato, non concorrente di Orderlion) può svolgere un audit, inclusa un'ispezione presso i

locali di Orderlion: al massimo una volta ogni 12 mesi, con un preavviso di almeno 30 giorni, durante l'orario lavorativo, in regime di riservatezza e senza interferenze irragionevoli con le operazioni. Ciascuna parte sostiene i propri costi; se l'audit rivela una non conformità sostanziale, Orderlion sostiene i ragionevoli costi di audit del Cliente.

12. Trasferimenti internazionali

12.1 I Dati personali del Cliente sono ospitati in produzione su infrastruttura nell'UE (AWS Francoforte). I trasferimenti a sub-responsabili del trattamento al di fuori dell'UE/SEE avvengono solo come documentato nell'Allegato 2 e solo con un valido meccanismo di trasferimento ai sensi del Capo V GDPR: una decisione di adeguatezza (incluso il Quadro UE-USA per la protezione dei dati per i destinatari certificati) o le clausole contrattuali tipo (2021/914, Modulo 3) concluse da Orderlion con il sub-responsabile del trattamento, con misure supplementari ove necessario.

12.2 Qualora un meccanismo di trasferimento su cui si fa affidamento cessi di essere valido (ad es. invalidazione di una decisione di adeguatezza), Orderlion attua un meccanismo valido alternativo senza ingiustificato ritardo; le clausole contrattuali tipo fungono da soluzione di ripiego per i destinatari certificati ai sensi del Data Privacy Framework.

12.3 L'autorizzazione da parte del Cliente dei trasferimenti documentati nell'Allegato 2 costituisce la sua istruzione documentata con riguardo ai trasferimenti (Art 28(3)(a) GDPR).

13. Restituzione e cancellazione

13.1 Per **30 giorni** dopo la fine del Contratto, il Cliente può esportare i Dati personali del Cliente in formati standard tramite la piattaforma o, su richiesta, con l'assistenza di Orderlion.

13.2 Trascorso il periodo di esportazione, Orderlion cancella i Dati personali del Cliente dai propri sistemi attivi, completando l'operazione al più tardi **90 giorni** dopo la fine del Contratto, salvo che il diritto dell'Unione o degli Stati membri ne imponga la conservazione. I dati nei sistemi di backup non sono cancellati attivamente ma scadono con la normale rotazione dei backup, al più tardi 30 giorni dopo la cancellazione dai sistemi attivi; fino alla scadenza restano protetti dalle misure di cui all'Allegato 3, non sono ripristinati per l'uso attivo e, se un ripristino di altri dati riproduce Dati personali del Cliente cancellati, la cancellazione viene nuovamente eseguita.

13.3 Su richiesta, Orderlion conferma la cancellazione per iscritto (ambito: completamento nei sistemi attivi e calendario di scadenza dei backup).

14. Responsabilità

Il regime di responsabilità del Contratto (Sezione 10 delle CGC) si applica alle pretese tra le parti ai sensi o in connessione con il presente DPA. La responsabilità legale nei confronti degli interessati (Art 82 GDPR) e la piena responsabilità di Orderlion per i propri sub-responsabili del trattamento (Sezione 6.4) restano impregiudicate.

15. Durata e modifiche

15.1 Il presente DPA si applica finché Orderlion tratta Dati personali del Cliente e sopravvive alla fine del Contratto fino al completamento della cancellazione ai sensi della Sezione 13.

15.2 Le modifiche al presente DPA seguono il meccanismo della Sezione 1.4 delle CGC; le modifiche relative ai sub-responsabili del trattamento seguono la Sezione 6 del presente DPA. Le versioni precedenti del presente DPA restano disponibili all'indirizzo www.orderlion.com/it/dpa.

15.3 Si applica il diritto austriaco come previsto dal Contratto; il foro competente è quello previsto dal Contratto.

Allegato 1 - Descrizione del trattamento

1. Oggetto. Fornitura e gestione della piattaforma Orderlion per il Cliente: una piattaforma cloud multi-tenant per l'ordinazione attraverso la quale gli acquirenti commerciali del Cliente effettuano ordini, che sono acquisiti, strutturati e trasferiti al sistema ERP proprio del Cliente, unitamente alle connesse funzioni di comunicazione, notifica, autenticazione, monitoraggio ed estrazione supportata da IA.

2. Durata. Per la durata del Contratto. Alla cessazione si applica il calendario di restituzione e cancellazione di cui alla Sezione 13 del presente DPA, che prevale sui periodi di conservazione indicati di seguito.

3. Natura e finalità del trattamento.

Attività di trattamento	Natura e finalità	Dati personali trattati	Interessati	Conservazione durante la durata
Inbox: ricezione dei messaggi di ordine	Ricezione e archiviazione dei messaggi di ordine degli acquirenti inoltrati dal Cliente al proprio indirizzo Inbox di Orderlion. La ricezione è gestita da Mailgun o AWS SES, che consegnano a Orderlion tramite webhook.	Indirizzi email del mittente e del destinatario; oggetto; corpo del messaggio; allegati; file vocali e audio per gli ordini via segreteria telefonica; metadati delle email	Utenti acquirenti e loro personale	Contenuto grezzo dei messaggi: 90 giorni ove il messaggio contenga un ordine, 30 giorni in caso contrario
Inbox: estrazione degli ordini supportata da IA	Conversione del contenuto dei messaggi in dati d'ordine strutturati. Il contenuto è trasmesso tramite API ai fornitori di IA incaricati indicati nell'Allegato 2 ed elaborato secondo i prompt predefiniti di Orderlion. I messaggi vocali sono trascritti su infrastruttura UE prima dell'estrazione.	Testo semplice del corpo del messaggio e degli allegati, inclusi eventuali dati personali che il mittente vi abbia incluso; trascrizioni audio; campi d'ordine estratti	Utenti acquirenti e loro personale	Come sopra
Assistente IA, report e raccomandazioni	Risposta a quesiti aziendali sui dati della piattaforma propri del Cliente, generazione di report automatizzati per il personale del Cliente e produzione di campagne di raccomandazione di prodotto. Output di natura meramente consultiva.	Identificativi utente; cronologia degli ordini e dati della piattaforma necessari per ciascuna funzionalità; domande poste e risposte generate	Utenti acquirenti, personale del Cliente	1 anno
Creazione ed elaborazione degli ordini	Registrazione ed elaborazione degli ordini effettuati sulla piattaforma e trasferimento degli ordini confermati al sistema ERP del Cliente.	Identificativo dell'utente acquirente; riferimento cliente; righe d'ordine (articoli, quantità, prezzi); data e ora dell'ordine; dettagli di consegna; identificativo del membro del personale del Cliente che ha creato l'ordine, ove un ordine sia effettuato per conto di un acquirente	Utenti acquirenti, personale del Cliente	2 anni, trascorsi i quali il collegamento tra il record dell'ordine e l'utente ordinante viene rimosso
Checkout e registrazione dei pagamenti	Registrazione dei pagamenti degli ordini effettuati sulla piattaforma per le scritture del Cliente e per la visualizzazione da parte del Cliente e dell'acquirente.	Identificativo dell'utente acquirente; importo totale del pagamento; stato del pagamento; marcature temporali. Le credenziali di carte e bancarie sono trattate esclusivamente dal fornitore di pagamento e non sono conservate da Orderlion.	Utenti acquirenti	2 anni

Attività di trattamento	Natura e finalità	Dati personali trattati	Interessati	Conservazione durante la durata
Invito, registrazione e onboarding degli utenti acquirenti	Invito degli utenti acquirenti da parte del Cliente e creazione dei loro account, per consentire l'accesso, l'assegnazione dell'account e l'attribuzione degli ordini effettuati. Gli inviti sono sempre attivati dal Cliente e sono inviati per email e, ove il Cliente fornisca un numero di cellulare, tramite SMS. Per impostazione predefinita l'SMS contiene il link di invito, il codice di invito e il nome del Cliente. Il Cliente può modificare il messaggio ed è responsabile di qualsiasi ulteriore contenuto che vi includa.	Nome (facoltativo); indirizzo email di lavoro; numero di telefono cellulare ove utilizzato per l'invito; riferimento dell'invito; assegnazione all'account del Cliente	Utenti acquirenti	1 anno dopo l'ultima attività
Autenticazione e controllo degli accessi	Verifica dell'identità dell'utente al momento dell'accesso e limitazione dell'accesso ai dati che ciascun utente è autorizzato a visualizzare.	Indirizzo email; hash della password con salt; marcature temporali di accesso; identificativi di sessione	Utenti acquirenti, personale del Cliente	1 anno dopo l'ultima attività
Messaggistica all'interno della piattaforma	Fornitura della messaggistica tra il personale del Cliente e i suoi utenti acquirenti, inclusa la consegna delle notifiche dei messaggi.	Identificativi utente del mittente e del destinatario; testo e allegati del messaggio; marcature temporali; metadati di consegna delle notifiche	Utenti acquirenti, personale del Cliente	1 anno
Notifiche transazionali	Invio di notifiche transazionali quali conferme d'ordine e aggiornamenti di stato, tramite email e notifiche push mobili, per conto del Cliente.	Nome e indirizzo email del destinatario oppure token push del dispositivo; contenuto della notifica; marcature temporali di invio	Utenti acquirenti, personale del Cliente	4 settimane
Monitoraggio della sicurezza (livello di controllo degli accessi)	Registrazione delle azioni degli utenti rilevanti per la sicurezza nel livello interno di controllo degli accessi della piattaforma, in particolare azioni distruttive o che modificano i permessi, per garantire la tracciabilità e supportare l'indagine sugli incidenti di sicurezza.	Identificativo utente; tipo di azione e oggetto interessato; marcatura temporale; metadati tecnici inclusi indirizzo IP e sessione	Utenti acquirenti, personale del Cliente	1 anno
Assistenza per le richieste di esercizio dei diritti degli interessati	Gestione delle richieste ai sensi degli Articoli da 12 a 23 GDPR relative ai dati della piattaforma, inclusa la verifica dell'identità, l'evasione e la documentazione dell'esito come prova di conformità.	Identità e dati di contatto del richiedente; dati di verifica; contenuto della richiesta; documentazione dell'esito e corrispondenza	Utenti acquirenti, personale del Cliente	1 anno dopo l'ultima attività

4. Tipi di dati personali. Dati identificativi e di contatto (nome, indirizzo email di lavoro e numero di telefono cellulare ove utilizzato per gli inviti agli acquirenti); dati di account e di accesso (credenziali in forma di hash, ruoli, permessi, dati di sessione); dati di ordini e transazioni; contenuto e metadati di messaggi ed email, inclusi allegati e messaggi vocali trattati tramite l'Inbox; dati tecnici (indirizzo IP, informazioni su dispositivo e browser, marcature temporali).

5. Categorie di interessati. Utenti acquirenti e loro personale, ossia dipendenti dei clienti commerciali propri del Cliente; il personale del Cliente che utilizza la piattaforma.

6. Categorie particolari di dati personali. Nessuna prevista, e nessuna funzione è progettata per raccoglierle. Poiché il contenuto dei messaggi trattati tramite l'Inbox è determinato dal mittente e non può essere filtrato in anticipo, tale contenuto può incidentalmente contenere dati personali che il mittente ha scelto di includere.

7. Frequenza del trattamento. Continuativa per la durata del Contratto.

Allegato 2 - Sub-responsabili del trattamento

Elenca solo i sub-responsabili del trattamento che trattano Dati personali del Cliente per conto di Orderlion. I fornitori utilizzati esclusivamente per le operazioni interne proprie di Orderlion non sono sub-responsabili del trattamento ai sensi del presente DPA e non sono elencati. Ove un middleware di integrazione o un fornitore EDI sia contrattualizzato dal Cliente anziché da Orderlion, tale fornitore è il responsabile del trattamento proprio del Cliente e non è elencato qui; ove sia Orderlion a contrattualizzarlo, esso è elencato e contrassegnato come applicabile solo agli account la cui integrazione lo utilizza.

I sub-responsabili del trattamento incaricati da Orderlion sono indicati nell'elenco dei sub-responsabili del trattamento pubblicato all'indirizzo www.orderlion.com/it/subprocessors. Tale elenco costituisce parte integrante del presente DPA e la versione pubblicata alla data di entrata in vigore del presente DPA è l'elenco autorizzato ai sensi della Sezione 6.1. L'elenco indica la data del suo ultimo aggiornamento e riporta la propria cronologia delle modifiche.

L'elenco è pubblicato separatamente anziché riprodotto qui affinché resti aggiornato. L'aggiunta o la sostituzione di un sub-responsabile del trattamento non costituisce una modifica del presente DPA: essa segue la Sezione 6, ai sensi della quale Orderlion fornisce un preavviso di almeno 30 giorni prima dell'incarico e il Cliente può opporsi entro tale termine per ragionevoli motivi attinenti alla protezione dei dati.

Su richiesta, Orderlion fornisce l'elenco nella versione vigente a una determinata data sotto forma di PDF datato, per i clienti che necessitano di una documentazione dei sub-responsabili del trattamento autorizzati al momento della sottoscrizione.

Allegato 3 - Misure tecniche e organizzative (Art 32 GDPR)

Contiene solo misure che sono in essere e che sono state esaminate e confermate. Le misure pianificate o in corso di rimedio non sono deliberatamente elencate qui; Orderlion le divulga separatamente nella propria Panoramica sulla sicurezza anziché presentarle come controlli operativi.

1. Pseudonimizzazione e cifratura (Art 32(1)(a))

Cifratura a riposo. Tutti i Dati personali del Cliente sono cifrati a riposo con AES-256. Il database applicativo su MongoDB Atlas e l'archiviazione AWS utilizzata dalla piattaforma applicano automaticamente la cifratura lato fornitore, coprendo dati attivi, istantanee e backup. La gestione delle chiavi è operata dai fornitori di infrastruttura nell'ambito dei loro programmi certificati; non è offerta alcuna opzione di chiavi gestite dal cliente.

Cifratura in transito. Tutto il traffico tra i client, ossia browser, applicazioni mobili e consumatori di API, e i server di Orderlion è cifrato mediante TLS. I protocolli SSL legacy sono disattivati. Lo scambio di file con i sistemi dei clienti utilizza FTPS o SFTP.

Protezione delle credenziali. Le password di accesso degli utenti sono conservate con salt e hash tramite bcrypt e mai in chiaro. Le credenziali dei servizi interni sono conservate cifrate con AES-256.

2. Riservatezza e controllo degli accessi (Art 32(1)(b))

Segregazione dei tenant. I dati dei clienti sono segregati logicamente per tenant, e la segregazione è applicata dal livello di autorizzazione della piattaforma a ogni richiesta.

Account individuali. Il personale e i collaboratori esterni utilizzano account individuali, personalmente attribuibili, su ogni sistema che contiene dati personali o fornisce un accesso rilevante per la sicurezza. Le credenziali condivise sono vietate per tali sistemi. Ove una credenziale debba effettivamente essere utilizzata da più persone, essa è distribuita tramite un gruppo di autorizzazioni nel gestore di password aziendale, così che sia controllato e verificabile chi può recuperarla. Tale credenziale è un login condiviso: le azioni compiute con essa non sono attribuibili a una singola persona ed essa è ruotata quando un membro del gruppo lascia l'azienda o cambia ruolo.

Politica delle password e gestore di password. Un gestore di password aziendale (NordPass Business, residenza dei dati nell'UE) è obbligatorio per tutto il personale e i collaboratori esterni ed è accessibile tramite il single sign-on di Google Workspace. Le credenziali memorizzate richiedono una robustezza minima di 20 caratteri con struttura complessa e sono modificate almeno annualmente. La disattivazione dell'account Workspace al momento dell'offboarding revoca automaticamente l'accesso a tutte le credenziali memorizzate.

Autenticazione a più fattori. L'MFA è obbligatoria sui sistemi business-critical, incluso il provider di identità Google Workspace attraverso il quale si accede al gestore di password. Il recupero dell'account è riservato al livello dirigenziale.

Privilegio minimo. L'accesso segue un modello basato sui ruoli limitato alla necessità operativa, nel quale le azioni distruttive sono riservate al livello di privilegio più elevato e i fornitori amministrano gli utenti solo all'interno del proprio account.

Controlli sull'impersonificazione. L'impersonificazione di un utente cliente è trattata come accesso sensibile. È riservata al partner management e al personale tecnico approvato, consentita solo ove operativamente necessaria per risoluzione di problemi, onboarding, migrazione o su richiesta del cliente, e vietata per qualsiasi finalità non aziendale.

Revisioni degli accessi. I diritti di accesso sono riesaminati trimestralmente per l'infrastruttura di produzione e cloud, gli account amministrativi, i repository di codice, i sistemi di assistenza e analisi, gli accessi dei collaboratori esterni e gli account inattivi. Ogni revisione è registrata.

Protezione della rete. I firewall degli host e i security group cloud sono configurati come chiusi per impostazione predefinita, con aperte solo le porte necessarie all'operatività. Le applicazioni sono eseguite in container su host stateless dietro load balancer.

Accesso ai server. L'accesso ai server è limitato a persone nominativamente individuate e avviene principalmente tramite AWS Systems Manager anziché tramite chiavi SSH distribuite. Ove siano utilizzate chiavi SSH, esse sono detenute esclusivamente dal CTO e dall'Head of Engineering.

Sicurezza dei dispositivi. I dispositivi gestiti dall'azienda sono lo standard per tutto il lavoro e richiedono un metodo di sblocco robusto, la cifratura del disco, il blocco automatico dello schermo, aggiornamenti del sistema operativo aggiornati e il blocco o la cancellazione da remoto ove tecnicamente possibile. I dispositivi personali possono essere utilizzati solo per strumenti di comunicazione e documentazione interna, e mai per dati dei clienti o della piattaforma, accesso a database, produzione o infrastruttura, sistemi HR o payroll, o esportazioni di dati.

Offboarding. Gli accessi sono revocati secondo una checklist di offboarding documentata: account del provider di identità disattivato, accessi SaaS, cloud, ai repository e alla comunicazione rimossi, dispositivi recuperati e credenziali ruotate ove necessario. Poiché il gestore di password aziendale si autentica tramite il single sign-on di Google Workspace, la disattivazione dell'account Workspace revoca automaticamente l'accesso a tutte le credenziali memorizzate anziché richiedere un passaggio manuale separato.

Autenticità delle email. I domini di invio sono protetti con SPF, DKIM e DMARC.

3. Integrità, disponibilità e resilienza (Art 32(1)(b))

Hosting. Tutti i sistemi di produzione e il database applicativo sono eseguiti su Amazon Web Services nella regione di Francoforte (eu-central-1), Germania. La sicurezza fisica del data centre, i controlli ambientali e le protezioni a livello di rete, inclusa la mitigazione degli attacchi distributed denial of service, sono forniti da AWS nell'ambito del proprio programma certificato.

Resilienza. I server applicativi sono stateless, con controlli automatizzati di integrità ogni 30 secondi e riavvio automatico delle istanze non integre. Le modifiche di capacità sono effettuate manualmente.

Disponibilità. L'obiettivo contrattuale di disponibilità è del 99% per mese di calendario, escluse le manutenzioni annunciate e le circostanze al di fuori del controllo di Orderlion. La disponibilità è monitorata continuativamente.

Backup. Due sistemi di backup operano in parallelo. Le collezioni critiche del database sono sottoposte a backup giornaliero su una posizione remota sicura e cifrata e conservate per 30 giorni, e i dati dei clienti e dei prezzi importati sono sottoposti a backup settimanale. Separatamente, il fornitore del database esegue proprie istantanee, conservate all'interno dell'UE per 7 giorni. Entrambi scadono automaticamente, cosicché i dati cancellati dai sistemi attivi scompaiono da tutti i backup entro 30 giorni al più tardi.

Obiettivi di ripristino. Un recovery time objective di 8 ore, ossia il tempo massimo per ripristinare il servizio dopo un incidente, e un recovery point objective di 24 ore, ossia la finestra massima tollerabile di perdita di dati, allineata al ciclo di backup giornaliero.

4. Registrazione e monitoraggio

Monitoraggio dell'infrastruttura e delle applicazioni. Il monitoraggio lato server copre integrità, prestazioni e allerta sulle anomalie, con tracciamento degli errori sia lato server sia lato client. Il senior team è allertato in caso di eventi non pianificati, anche al di fuori dell'orario lavorativo e nei fine settimana.

Audit trail della piattaforma. Un livello interno di controllo degli accessi registra le azioni degli utenti rilevanti per la sicurezza sulla piattaforma, in particolare le azioni distruttive o che modificano i permessi, quali la disattivazione di acquirenti o prodotti, affinché tali azioni restino tracciabili.

Protezione dagli attacchi a forza bruta. I tentativi di accesso SSH sono registrati e gli indirizzi di origine sospetti sono bloccati automaticamente.

Conservazione e accesso ai log. La conservazione varia in base allo strumento: i log dell'infrastruttura e delle applicazioni sono conservati per 14 giorni, gli eventi di errore da 30 a 90 giorni a seconda del tipo di dato, e i log del server per un massimo di 30 giorni. L'accesso è riservato al personale di ingegneria autorizzato, e i log non sono condivisi con terzi né con singoli clienti, poiché possono contenere dati relativi a più di un tenant.

5. Sviluppo sicuro

Principio dei quattro occhi. Ogni modifica destinata alla produzione è riesaminata e approvata da almeno un altro sviluppatore prima del rilascio.

Test automatizzati. Più di 2.000 test automatizzati unitari e di integrazione sono eseguiti a ogni deployment, i test end-to-end sono eseguiti settimanalmente e un controllo qualità manuale precede i rilasci principali.

Separazione degli ambienti. Gli ambienti di produzione, staging e sviluppo sono separati.

Scansione delle dipendenze e delle vulnerabilità. La scansione automatizzata delle dipendenze e delle vulnerabilità è eseguita sui repository di codice, così che le vulnerabilità note nei pacchetti di terze parti siano evidenziate per la relativa risoluzione.

6. Salvaguardie specifiche per il trattamento tramite IA

L'estrazione degli ordini utilizza modelli linguistici di grandi dimensioni accessibili tramite API dai fornitori indicati nell'Allegato 2, in base ad accordi sul trattamento dei dati. I messaggi vocali sono trascritti su infrastruttura UE prima dell'estrazione. Ai fornitori è contrattualmente vietato addestrare i propri modelli sui Dati personali del Cliente trasmessi tramite Orderlion. I dati della piattaforma sono archiviati nell'UE, e il trattamento tramite IA può essere limitato su richiesta a infrastruttura ospitata nell'UE. Le estrazioni incerte o anomale sono segnalate per la verifica umana, e il Cliente sceglie se ogni ordine estratto debba essere verificato prima del trasferimento al proprio sistema ERP.

7. Misure organizzative

Quadro delle politiche. Una politica interna scritta di compliance e sicurezza disciplina identità e autenticazione, sicurezza dei dispositivi, strumenti approvati, controllo degli accessi, gestione e classificazione dei dati dei clienti, utilizzo dell'IA, gestione dei fornitori, risposta agli incidenti e onboarding e offboarding. È riesaminata almeno annualmente e forma parte di ogni rapporto di lavoro e di collaborazione.

Risposta agli incidenti. Gli incidenti sono rilevati mediante il monitoraggio, classificati per gravità, escalati al CTO, all'Engineering Lead e al CEO, contenuti, analizzati per individuarne la causa radice e chiusi con un post-mortem. Le violazioni dei dati personali seguono un'ulteriore procedura GDPR documentata: ogni violazione è registrata in un registro delle violazioni e, ove Orderlion agisca come responsabile del trattamento, i clienti interessati sono notificati senza ingiustificato ritardo e al più tardi entro 72 ore dalla conoscenza, ovvero entro qualsiasi termine più breve concordato nel singolo contratto.

Formazione di sensibilizzazione sulla sicurezza. I nuovi assunti ricevono un onboarding su sicurezza e protezione dei dati entro le prime due settimane, che copre phishing, igiene delle password e gestore di password, gestione dei dati dei clienti, segnalazione degli incidenti e regole per gli strumenti di IA, sulla base di un curriculum documentato. Un corso di aggiornamento è obbligatorio per tutto il personale con cadenza annuale, con sessioni specifiche per ruolo per i team di ingegneria e commerciali. La partecipazione è registrata e la copertura è verificata trimestralmente rispetto all'elenco del personale aggiornato.

Gestione dei fornitori. Prima dell'adozione di un nuovo fornitore, una valutazione documentata copre i dati da condividere, il supporto per autenticazione e single sign-on, la disponibilità di un accordo sul trattamento dei dati, l'hosting nell'UE, la criticità per l'attività e il rischio di sicurezza. I fornitori che trattano dati personali sono registrati in un registro dei sub-responsabili del trattamento con il relativo meccanismo di trasferimento e lo stato dell'accordo.

Sicurezza fisica. L'accesso all'ufficio è protetto con chiavi fisiche soggette a un registro delle chiavi che documenta ogni chiave consegnata e restituita, così che i detentori delle chiavi restino tracciabili. L'ufficio è tenuto chiuso a chiave in ogni momento, e i documenti cartacei contenenti dati personali sono conservati in armadi chiusi a chiave.