Misure di sicurezza

Versione 1.1, in vigore dal 21 ottobre 2026

OutLine Digital Agency (libero professionista), Via Dalmazia 36, 76125 Trani (BT), Italia — P.IVA 08978680729

Come proteggiamo i dati: separazione degli ambienti, cifratura, accessi, backup. Con dentro anche ciò che non facciamo.

Riferimenti normativi	Regolamento (UE) 2016/679, art. 32 (sicurezza del trattamento) · Regolamento (UE) 2016/679, art. 25 (protezione dei dati fin dalla progettazione e per impostazione predefinita)

1. Un database per ambiente

È la misura più importante e quella che quasi nessun gestionale cloud adotta, perché costa: **ogni ambiente di lavoro ha un proprio database**, non una colonna «cliente» dentro tabelle condivise.

La differenza si vede il giorno in cui qualcosa va storto. Con le tabelle condivise, una query a cui sfugge il filtro sul cliente mostra i dati di tutti; qui non esiste una query che possa farlo, perché i dati degli altri stanno in un altro database, con altre credenziali. Vale anche per i backup, che si ripristinano uno per volta senza toccare nessun altro.

L'unica eccezione, dichiarata: la bacheca della community, che è per definizione uno spazio comune, vive in un archivio separato da tutti i dati di lavoro e non tocca nessuna tabella di business.

2. Cifratura

Cosa	Come
Traffico verso il sito e il gestionale	HTTPS con certificati rinnovati automaticamente. Il traffico in chiaro viene reindirizzato.
Password degli utenti	Mai conservate in chiaro né cifrate in modo reversibile: solo l'impronta calcolata con **scrypt**, con sale casuale per ogni utente e confronto a tempo costante. Nemmeno noi possiamo leggerle o comunicartele.
Token di sessione	Nel database si conserva solo l'impronta del token, mai il valore che sta nel cookie.
Credenziali dei servizi collegati (negozi online, corrieri, pagamenti, caselle di posta)	Cifrate a riposo con **AES-256-GCM**, con chiave dedicata e separata dai dati. Chi ottenesse un dump del database non otterrebbe le tue chiavi API.

Il modello di minaccia, detto onestamente

La cifratura delle credenziali protegge dai dump e dai backup che finiscono dove non devono — l'incidente di gran lunga più probabile. Non protegge da una compromissione totale del server, dove la chiave è comunque leggibile: per quello servirebbe un servizio di gestione chiavi esterno, che oggi non usiamo. Preferiamo scriverlo che lasciarlo intendere.

3. Controllo degli accessi

- Accesso con email e password personale; le sessioni scadono e si possono chiudere.
- Il cookie di sessione è **HttpOnly** (non leggibile da script), **Secure** (solo su connessione cifrata) e **SameSite=Lax** (non viaggia con richieste da altri siti).
- **Permessi per modulo**: il titolare decide, sezione per sezione, chi vede e chi modifica. I dipendenti hanno un ruolo separato che non accede al gestionale ma alla sola area personale.

- Gli accessi dell’assistenza usano un **utente temporaneo con scadenza a 15 minuti**, sono segnalati da una fascia visibile a schermo e finiscono nel registro degli eventi.
- I dati di un ambiente sono raggiungibili solo dall’interno dell’ambiente: non esiste una schermata, nemmeno per noi, che mostri i dati di lavoro di più clienti insieme.

4. Infrastruttura

- Server presso IONOS SE, datacenter in Germania: i dati non escono dallo Spazio economico europeo, tranne i testi che mandi alle funzioni di intelligenza artificiale quando usano l’IA di Omega (accese di serie, si possono spegnere: vedi l’elenco dei sub-responsabili).
- Il database non è esposto su internet: ascolta solo in locale e vi si accede attraverso un canale cifrato.
- Le pagine private (gestionale, pannello di amministrazione, avvio guidato, portali, interfacce di programmazione) sono escluse dall’indicizzazione dei motori di ricerca.
- Le attività pianificate girano su un canale interno protetto da un segreto condiviso: senza quel segreto l’endpoint rifiuta ogni richiesta invece di restare aperto.
- Aggiornamenti del sistema operativo e delle dipendenze applicati periodicamente; il rilascio passa da una build verificata, non da modifiche manuali sul server.

5. Backup e ripristino

- Copia di sicurezza **giornaliera** di tutti i database, compresso e con verifica dell’esito.
- Conservazione **a rotazione: 7 copie giornaliere, 4 settimanali, 3 mensili**. Le copie più vecchie vengono eliminate automaticamente.
- Le copie stanno sulla stessa infrastruttura europea, con permessi ristretti al solo utente di sistema che le produce.
- Il ripristino è **per singolo ambiente**: si riporta indietro un cliente senza toccare gli altri.
- La procedura di ripristino viene verificata periodicamente: un backup mai riprovato non è un backup.

> **Cosa significa per te**
>
> Se cancelli per errore un archivio importante, la finestra utile per recuperarlo è di norma di sette giorni per il dettaglio giornaliero. Prima ci scrivi, più è probabile che si recuperi tutto: scrivi a amministrazione@outlinedigital.it indicando l’ambiente e, se lo sai, quando è successo.

6. Come è scritto il software

- I dati degli utenti sono validati prima di essere salvati; le interrogazioni al database sono parametrizzate, quindi non manipolabili dall’esterno.
- Le operazioni che scrivono passano da azioni lato server con controllo del ruolo: non ci si arriva chiamando un indirizzo a mano.
- Le pagine pubbliche raggiungibili da un collegamento usano **codici imprevedibili** e revocabili: un codice rigenerato invalida subito il precedente.
- I segreti non stanno nel codice ma nelle variabili d’ambiente del server.
- Prima di ogni rilascio girano controlli automatici che verificano il funzionamento dei moduli e la coerenza delle configurazioni.

7. Se succede qualcosa

Le violazioni di dati personali sono comunicate al cliente **entro 48 ore** da quando ne veniamo a conoscenza, con le informazioni necessarie a valutare la notifica al Garante nelle 72 ore previste dall’art. 33 GDPR. Il dettaglio della procedura è all’art. 6 dell’Accordo sul trattamento dei dati (https://work.omegasuite.it/legale/dpa).

Se individui una vulnerabilità, scrivi a **amministrazione@outlinedigital.it**. Ci impegniamo a rispondere entro 5 giorni lavorativi e a non intraprendere azioni verso chi segnala in buona fede, senza accedere a dati altrui, senza degradare

il servizio e senza divulgare il problema prima che sia risolto.

8. Quello che non facciamo (ancora)

Un elenco di misure senza i suoi limiti è pubblicità. Queste sono le cose che oggi **non** ci sono, così le sai prima e non dopo:

- **Autenticazione a due fattori**: non disponibile. Usa una password lunga e diversa da quelle di altri servizi, e un gestore di password.
- **Cifratura dell'intero database a riposo**: non attiva. Sono cifrate le credenziali dei servizi collegati e le password; il resto dei dati è protetto dai controlli di accesso e dall'isolamento del sistema, non dalla crittografia.
- **Certificazioni** (ISO/IEC 27001, SOC 2): non ne abbiamo. Non ci attribuiamo standard che non abbiamo superato.
- **Restrizione degli accessi per indirizzo IP** e **registro degli accessi consultabile dal cliente per ogni utente**: non disponibili.

Quando una di queste voci verrà implementata si sposterà nelle sezioni precedenti e la versione di questo documento si alzerà.

9. Quello che tocca a te

La sicurezza di un gestionale si gioca almeno per metà fuori dal software:

- usa password robuste e non riusate quelle di altri servizi;
- crea un utente per ogni persona: gli accessi condivisi rendono impossibile sapere chi ha fatto cosa;
- assegna i permessi minimi necessari e **disattiva subito** chi lascia l'azienda;
- rigenera i codici delle pagine pubbliche se sospetti che siano circolati;
- tieni aggiornati i dispositivi da cui accedi, soprattutto il tablet della cassa;
- esporta periodicamente i dati che non potresti permetterti di perdere.

Testo integrale sempre aggiornato su https://work.omegasuite.it/legale/sicurezza. Per ogni domanda: amministrazione@outlinedigital.it.