

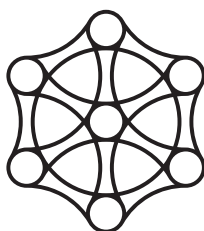


Dichiarazione di trasparenza per i servizi cloud

**Ripartizione delle responsabilità
e protezione dei dati personali
nei servizi SaaS di Plug-in S.r.l.**

Informativa per i Clienti predisposta
in conformità alle Linee Guida ISO/IEC 27017:2026
e ISO/IEC 27018:2025, a integrazione
del Sistema di Gestione per la
Sicurezza delle Informazioni certificato
ISO/IEC 27001.

Rev. 00 del 31/08/2026 - Documento pubblico



plug-in

INCREASE, INTEGRATE, INNOVATE BUSINESS



Perché questo documento

Plug-in S.r.l. (“Plug-in”) mette a disposizione dei propri Clienti servizi in modalità SaaS (Software as a Service), assumendo il ruolo di Cloud Service Provider (CSP). La sicurezza delle informazioni e la protezione dei dati personali trattati nei servizi cloud sono il risultato di un impegno condiviso tra Plug-in e i propri Clienti (Cloud Service Customer - CSC): alcune attività sono di competenza di Plug-in, altre restano necessariamente in capo al Cliente, in funzione di come il servizio viene utilizzato e configurato.

Questo documento descrive tale ripartizione con il livello di dettaglio richiesto dai principi di trasparenza delle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, illustrando le garanzie offerte da Plug-in, gli impegni richiesti al Cliente e le misure tecniche e organizzative adottate a tutela dei dati trattati nei servizi cloud.

La nostra infrastruttura Cloud, in sintesi

I servizi SaaS sono erogati su un'infrastruttura di proprietà di Plug-in, ospitata (in modalità housing) presso il data center di un primario operatore di telecomunicazioni, situato in Italia (UE). Il fornitore del data center mette a disposizione esclusivamente lo spazio fisico e la connettività di rete: non ha alcun accesso logico ai sistemi né ai dati dei Clienti, che restano sotto il controllo esclusivo di Plug-in.

Come ci ripartiamo le responsabilità: la matrice in sintesi

L'immagine e la tabella seguenti riepilogano, per le principali aree di sicurezza, le responsabilità di Plug-in in qualità di CSP e quelle che restano in capo al Cliente in qualità di CSC. Nei paragrafi successivi ciascuna area viene descritta con maggiore dettaglio.



Ambito	Plug-in (Cloud Service Provider)	Cliente (Cloud Service Customer)
Infrastruttura fisica e data center	Gestione completa dell'infrastruttura server, ospitata in data center situato in Italia (UE)	-
Piattaforma cloud, virtualizzazione e sistemi operativi	Hardening, aggiornamenti e patch di sicurezza	-
Segregazione dei dati tra Clienti (multitenancy)	Garantita a livello di piattaforma e di infrastruttura	-
Cifratura dei dati	Cifratura dei dati in transito	Corretto utilizzo delle eventuali funzioni di cifratura previste dall'applicativo
Backup e continuità operativa (BCP/DR)	Piani di backup e di disaster recovery dell'infrastruttura e dei dati ospitati	Segnalazione tempestiva di esigenze specifiche di ripristino
Gestione delle credenziali e degli account	Di norma a cura di Plugin, su richiesta del Cliente, per la creazione, modifica e disattivazione delle utenze	In alternativa, a cura del Cliente stesso qualora richieda un account amministrativo dedicato per la gestione autonoma dei propri utenti
Custodia delle credenziali e utilizzo delle utenze	Adozione di policy di password robuste e di un sistema di log management	Custodia riservata delle proprie credenziali; utilizzo delle utenze esclusivamente da parte dei soggetti a cui sono assegnate
Configurazione e uso dell'applicativo	Manutenzione, aggiornamento e sicurezza della piattaforma software	Corretta configurazione dei parametri applicativi e dei permessi in base alle proprie esigenze
Contenuti e dati trattati tramite il servizio	Protezione infrastrutturale e logica dei dati ospitati	Correttezza, liceità e pertinenza dei dati inseriti nel servizio
Backup dei dati	Esecuzione di backup periodici secondo policy definite; informativa al Cliente sulle proprie politiche di backup	Segnalazione di esigenze specifiche di conservazione o ripristino
Gestione delle vulnerabilità tecniche	Analisi periodiche delle vulnerabilità e, ove necessario, penetration test; rilascio su richiesta di un'attestazione sull'avvenuta esecuzione delle attività e presa in carico delle eventuali vulnerabilità rilevate. Il report tecnico è consultabile esclusivamente presso la sede di Plugin.	Valutazione delle informazioni ricevute nell'ambito della propria gestione del rischio
Comunicazione di modifiche al servizio	Gestione delle modifiche tramite procedura interna di change management; comunicazione al Cliente delle modifiche applicative solo in caso di major release.	-
Notifica di data breach	Notifica al Cliente entro 72 ore dalla rilevazione dell'incidente	Notifica al Garante e agli interessati, ove applicabile, in qualità di Titolare del trattamento
Richieste di terzi e degli interessati	Inoltro tempestivo al Cliente di richieste ricevute da interessati o da autorità pubbliche relative ai suoi dati	Gestione della richiesta in qualità di Titolare del trattamento
Conformità normativa in materia di dati personali	Adempimenti quale Responsabile del trattamento (art. 28 GDPR)	Adempimenti quale Titolare del trattamento



Responsabilità di Plug-in in qualità di Cloud Service Provider

- **Garanzie generali del servizio**

Plug-in eroga i servizi SaaS con la diligenza e la professionalità richieste dalla prassi di settore, nel rispetto degli SLA concordati contrattualmente con ciascun Cliente e della normativa applicabile ai servizi cloud.

- **Sicurezza delle informazioni e gestione degli incidenti**

Plug-in assicura la segregazione logica tra il proprio ambiente di amministrazione e gli ambienti cloud dei singoli Clienti, e mantiene un presidio costante sulla sicurezza dell'infrastruttura tramite attività periodiche di analisi dei rischi, vulnerability assessment e penetration test.

Plug-in comunica inoltre al Cliente eventuali incidenti rilevanti che possano compromettere la riservatezza, l'integrità o la disponibilità delle informazioni trattate nell'ambito dei servizi erogati. In caso di incidente di sicurezza che comporti una violazione di dati personali (data breach), Plug-in notifica il Cliente entro 72 ore dalla rilevazione, fornendo le informazioni utili affinché il Cliente possa assolvere ai propri obblighi verso l'Autorità Garante e gli interessati.

- **Manutenzione, aggiornamenti e supporto**

Plug-in monitora regolarmente le prestazioni del servizio e pianifica le finestre di manutenzione ordinaria dandone preventiva comunicazione ai Clienti; per gli interventi di manutenzione straordinaria o urgente, la comunicazione avviene non appena possibile, adottando ogni misura utile a minimizzare l'impatto sul servizio erogato.

- **Utilizzo di subfornitori**

Ove Plug-in si avvalga di subfornitori per l'erogazione, anche parziale, dei servizi cloud (ad esempio per l'housing dell'infrastruttura), tali soggetti sono selezionati privilegiando la presenza di misure di sicurezza tecniche e organizzative equivalenti a quelle adottate da Plug-in, e sono vincolati contrattualmente al rispetto della riservatezza e della sicurezza dei dati. Eventuali incidenti di sicurezza rilevati presso un subfornitore sono notificati al Cliente con le medesime modalità e tempistiche previste per gli incidenti diretti.

- **Ubicazione e gestione degli asset**

Plug-in colloca i dati dei Clienti esclusivamente su infrastruttura situata in Italia, all'interno dell'Unione Europea, senza trasferimenti verso paesi terzi. Ogni asset informativo è identificato e classificato secondo le procedure interne del Sistema di Gestione per la Sicurezza delle Informazioni.

- **Dismissione sicura degli ambienti cloud**

Alla cessazione del servizio, Plug-in provvede alla dismissione sicura degli ambienti cloud dedicati al Cliente, secondo procedure coerenti con i principi della ISO/IEC 27001 e delle Linee Guida ISO/IEC 27017.

- **Conservazione, restituzione e cancellazione dei dati del Cliente**

I dati del Cliente sono conservati per l'intera durata contrattuale secondo le migliori pratiche di sicurezza. Su richiesta del Cliente, e comunque alla cessazione del contratto, Plug-in mette a disposizione una copia dei dati nei formati concordati; una volta completata la restituzione, ovvero decorso il periodo contrattuale, i dati vengono cancellati in modo sicuro, fatti salvi eventuali obblighi di conservazione previsti da normative vigenti.



Responsabilità del Cliente in qualità di Cloud Service Customer

- **Gestione delle proprie utenze e dei propri dati**

Il Cliente è responsabile delle attività svolte attraverso le utenze e le chiavi di accesso a esso assegnate, dell'utilizzo operativo del servizio da parte dei propri Utenti e delle operazioni di caricamento e gestione dei propri dati all'interno del servizio.

- **Sicurezza delle credenziali di accesso**

Il Cliente gestisce con diligenza le proprie credenziali (identificativi, password, altri strumenti di autenticazione), adottando le misure necessarie ad assicurarne la riservatezza ed evitando che soggetti non autorizzati ne vengano in possesso. Il Cliente si impegna a informare tempestivamente Plug-in in caso di uso non autorizzato di un'utenza o di altre violazioni di sicurezza di cui venga a conoscenza.

- **Configurazione e utilizzo corretto del servizio**

Il Cliente è tenuto a mantenere correttamente configurati e aggiornati i propri sistemi utilizzati per accedere al servizio, a impiegare strumenti aggiornati di protezione da malware, e a configurare i parametri e i permessi applicativi in coerenza con le proprie esigenze e con la propria politica di controllo degli accessi.

- **Formazione e consapevolezza dei propri utenti**

Il Cliente è invitato a includere nei propri programmi di formazione interna i temi relativi all'utilizzo sicuro dei servizi cloud, ai rischi per la sicurezza delle informazioni connessi a tale utilizzo e alle relative modalità di gestione.

Misure tecniche di sicurezza adottate

- **Gestione delle credenziali e degli account**

La gestione delle credenziali e degli account utente può seguire due modalità, in funzione delle esigenze del Cliente: nella modalità standard, Plug-in cura direttamente, su richiesta del Cliente, la creazione, la modifica e la disattivazione delle utenze dei suoi utilizzatori; in alternativa, qualora il Cliente richieda un account amministrativo dedicato, è il Cliente stesso ad assumere la gestione autonoma delle proprie utenze, restando in tal caso responsabile della corretta assegnazione dei profili e della tempestiva disattivazione delle utenze non più necessarie.

- **Policy delle password**

Le password di accesso al servizio sono soggette a requisiti minimi di sicurezza (obbligo di modifica al primo accesso, lunghezza minima, regole di complessità, scadenza periodica, storicizzazione, archiviazione in forma cifrata/hash) definiti da Plug-in in coerenza con le proprie policy di sicurezza.

- **Log Management e tracciamento degli accessi**

Plug-in mantiene un sistema di log management che consente il tracciamento degli accessi al servizio e, in particolare, delle attività svolte dagli amministratori di sistema, con conservazione dei relativi dati in modalità che ne garantiscono l'integrità ai fini di un successivo controllo.



- **Backup dei dati**

Plug-in esegue backup periodici dei dati e dei sistemi che compongono l'infrastruttura cloud, secondo policy interne di frequenza e conservazione definite in base alla criticità dei dati trattati. Su richiesta, Plug-in informa il Cliente circa le proprie politiche di backup.

- **Gestione delle vulnerabilità tecniche**

Plug-in effettua periodicamente attività di vulnerability assessment e, ove necessario, penetration test sull'infrastruttura e sugli applicativi erogati in modalità cloud, in coerenza con i controlli previsti dalla ISO/IEC 27001 per i servizi cloud. Su richiesta del Cliente, Plug-in può rilasciare un'attestazione relativa all'avvenuta esecuzione di tali attività e all'impegno a prendere in carico e gestire, secondo le proprie procedure interne, le eventuali vulnerabilità rilevate. Il report tecnico di dettaglio non viene trasmesso al Cliente ed è reso disponibile esclusivamente per consultazione presso la sede di Plug-in.

- **Disponibilità del servizio (SLA)**

La disponibilità del servizio è garantita da Plug-in secondo i livelli di servizio (SLA) concordati contrattualmente con ciascun Cliente.

- **Amministratori di sistema**

L'elenco degli amministratori di sistema che operano sull'infrastruttura cloud è mantenuto costantemente aggiornato, con funzioni definite in appositi atti di nomina; le relative attività sono tracciate attraverso il sistema di log management di cui al presente documento.

- **Segregazione e hardening degli ambienti virtuali**

Plug-in garantisce la segregazione logica dei dati e degli ambienti dei diversi Clienti all'interno della propria infrastruttura condivisa (multi-tenancy), nonché la segregazione tra la rete di amministrazione dell'infrastruttura e gli ambienti cloud dei Clienti. Le macchine virtuali su cui sono erogati i servizi SaaS sono configurate secondo pratiche di hardening finalizzate a ridurre la superficie di attacco, e sono mantenute costantemente aggiornate.

- **Change Management**

Plug-in ha adottato una procedura interna di change management per la gestione, valutazione, approvazione e tracciamento delle modifiche relative all'infrastruttura, ai sistemi e agli applicativi erogati in modalità cloud. Le modifiche ordinarie e manutentive sono gestite secondo tale procedura interna, con l'obiettivo di garantire continuità, sicurezza e controllo degli interventi. Eventuali modifiche all'applicativo vengono comunicate al Cliente solo qualora configurino una major release, ovvero comportino cambiamenti significativi nelle funzionalità, nelle modalità di utilizzo o nella fruizione del servizio.

- **Data center e localizzazione dei dati**

L'infrastruttura cloud di Plug-in è ospitata presso un data center situato in Italia, all'interno dell'Unione Europea. Il fornitore del data center mette a disposizione unicamente lo spazio fisico e la connettività di rete, senza alcun accesso logico ai sistemi né ai dati dei Clienti.

- **Sicurezza delle comunicazioni e crittografia**

I flussi di dati verso i sistemi cloud esposti su internet sono protetti tramite canale sicuro (TLS), con autenticazione del server e cifratura della sessione mediante algoritmi considerati ragionevolmente sicuri allo stato dell'arte.



- **Cancellazione sicura dei dati e dei file temporanei**

Al termine del servizio, o su richiesta del Cliente, Plug-in assicura la cancellazione sicura dello spazio cloud e dei file temporanei associati, secondo le procedure interne di dismissione descritte nel presente documento.

- **Sincronizzazione degli orologi di sistema**

Tutti i sistemi che compongono l'infrastruttura cloud di Plug-in sono sincronizzati su una fonte oraria comune e affidabile, tramite protocollo sicuro di sincronizzazione (NTP). Questo garantisce che i log di sistema e le registrazioni degli accessi, di cui al par. 3.3, riportino marcature temporali coerenti e affidabili, elemento essenziale per la corretta ricostruzione cronologica in caso di analisi di sicurezza o di incidente. La fonte di sincronizzazione è la seguente: 0.pool.ntp.org / 1.pool.ntp.org / 2.pool.ntp.org

Misure organizzative di sicurezza

- **Policy e regolamenti per gli utenti**

Plug-in applica regolamenti interni, vincolanti per tutto il personale con accesso ai sistemi informativi, finalizzati a garantire comportamenti idonei alla protezione dei dati nell'utilizzo delle risorse informatiche, inclusi quelli erogati in modalità cloud.

- **Autorizzazione degli accessi logici**

I profili di accesso del personale Plug-in sono definiti in funzione delle mansioni assegnate, in modo da limitare l'accesso ai soli dati necessari allo svolgimento delle attività di competenza, e sono soggetti a controlli periodici.

- **Gestione degli interventi di assistenza**

Gli interventi di assistenza tecnica sono limitati alle sole attività necessarie a risolvere la richiesta del Cliente, in modo da evitare trattamenti di dati personali non pertinenti o eccedenti rispetto a quanto richiesto.

- **Gestione degli incidenti e dei data breach**

Plug-in ha adottato una procedura strutturata di gestione degli incidenti informatici, articolata in contenimento, eliminazione, ripristino e analisi post-incidente, finalizzata a ripristinare la normale operatività nel minor tempo possibile e a garantire, in caso di data breach, la tempestiva informativa al Cliente secondo quanto indicato nel presente documento.

- **Formazione del personale**

Il personale Plug-in coinvolto nella gestione dei servizi cloud partecipa periodicamente a percorsi di formazione sulla sicurezza delle informazioni e sulla corretta gestione dei dati personali, inclusi gli aspetti specifici dei servizi cloud.

- **Change management**

Le modifiche all'infrastruttura, ai sistemi e agli applicativi erogati in modalità cloud sono gestite attraverso una procedura interna strutturata di change management, che prevede la valutazione, l'approvazione, la pianificazione e il tracciamento degli interventi. Le modifiche ordinarie, manutentive o correttive sono gestite internamente secondo tale procedura.



Le modifiche applicative vengono comunicate al Cliente solo qualora configurino una major release, ovvero comportino cambiamenti significativi nelle funzionalità, nelle modalità di utilizzo o nella fruizione del servizio; per eventuali modifiche urgenti o non pianificate, la comunicazione avviene non appena possibile, ove rilevante per il Cliente.

- **Audit interni e verifiche indipendenti**

il Sistema di Gestione Integrato di Plug-in è sottoposto ad audit interni periodici e a verifiche di sorveglianza da parte di un Ente di Certificazione accreditato indipendente. I Clienti possono richiedere evidenze della conformità agli standard adottati; ove non sia possibile concordare un audit diretto, Plug-in mette a disposizione la documentazione relativa alle certificazioni ottenute.

- **Sviluppo sicuro del software**

Gli ambienti di sviluppo, test e produzione sono logicamente separati e accessibili al solo personale autorizzato. Lo sviluppo del software erogato in modalità SaaS segue principi di security by design, con test dedicati alla verifica dell'assenza di vulnerabilità significative prima del rilascio in produzione.

Trattamento dei dati personali (PII)

- **Ruolo di Plug-in quale Responsabile del trattamento**

Nell'ambito dei servizi cloud, Plug-in agisce quale Responsabile del trattamento (PII Processor ai sensi della ISO/IEC 27018) per conto del Cliente, che riveste il ruolo di Titolare del trattamento.

Plug-in tratta i dati personali esclusivamente sulla base delle istruzioni del Cliente e per le sole finalità funzionali all'erogazione del servizio, e non li utilizza per finalità proprie (marketing, profilazione, pubblicità), salvo diversa ed esplicita autorizzazione contrattuale.

- **Obblighi del Cliente quale Titolare del trattamento**

Il Cliente garantisce la liceità dei dati personali conferiti a Plug-in, fornisce istruzioni conformi alla normativa applicabile e adotta le misure tecniche e organizzative necessarie affinché siano trattati, per impostazione predefinita, solo i dati personali necessari a ciascuna finalità.

- **Sub-responsabili del trattamento**

Ove Plug-in si avvalga di soggetti terzi che comportino il trattamento di dati personali per suo conto, tali soggetti sono individuati nell'atto di nomina a Responsabile del trattamento sottoscritto con il Cliente, e sono vincolati a garanzie di sicurezza equivalenti a quelle di Plug-in.

- **Diritti del Cliente sui propri dati**

il Cliente può in qualsiasi momento richiedere l'esportazione, la restituzione o la cancellazione dei propri dati, e comunque ottiene tale possibilità alla cessazione del contratto, secondo le modalità indicate nel presente documento.



- **Richieste di terzi e degli interessati**

Qualora un interessato (ad esempio un utente finale del Cliente) rivolga direttamente a Plug-in una richiesta relativa ai propri dati personali, Plug-in la inoltra tempestivamente al Cliente, in qualità di Titolare del trattamento, senza darvi seguito autonomamente. Allo stesso modo, in caso di richiesta di divulgazione di dati personali proveniente da autorità pubbliche o forze dell'ordine, Plug-in ne informa il Cliente prima di darvi riscontro, salvo che ciò sia espressamente vietato dalla legge, e comunque rifiuta ogni divulgazione che non sia giuridicamente vincolante.

Le nostre certificazioni

Il Sistema di Gestione Integrato di Plug-in è certificato da un Ente di Certificazione accreditato secondo i seguenti standard, ed è sottoposto a verifiche periodiche di sorveglianza:

- **UNI EN ISO 9001:2015**
Sistemi di gestione per la qualità
- **UNI ISO 45001:2018**
Sistemi di gestione per la salute e sicurezza sui luoghi di lavoro
- **ISO/IEC 27001:2022**
Sistemi di gestione per la sicurezza delle informazioni.



Contatti

Per qualsiasi richiesta relativa alla sicurezza delle informazioni o al trattamento dei dati personali nell'ambito dei servizi cloud, i Clienti possono contattare il Responsabile della Sicurezza delle Informazioni di Plug-in all'indirizzo

info@plug-in.it