ALLEGATO TECNICO DI SICUREZZA (ATS) E CONDIZIONI GENERALI

Specifiche operative autoportanti per la fornitura delle «Piattaforme ERP SaaS della Pluservice S.r.l.»

PREAMBOLO DI VALIDITÀ CONTRATTUALE

Il presente documento, redatto in conformità ai requisiti dettati dalle Linee Guida ISO/IEC 27017, costituisce l'esposizione formale, completa e autoportante delle specifiche tecniche e di sicurezza applicate da Pluservice S.r.l. L'accettazione delle Condizioni Generali di fornitura del servizio SaaS implica l'accettazione integrale e incondizionata delle presenti specifiche da parte del Cliente. Nessun ulteriore accordo o matrice esterna è necessario per definire gli obblighi di sicurezza qui riportati.

Art. 1 Ripartizione delle Responsabilità per la Sicurezza delle Informazioni

Riferimento ISO/IEC 27017: Paragrafo 6.1.1.

Applicazione: Il modello operativo condiviso prevede che Pluservice S.r.l. abbia la responsabilità esclusiva dell'hardening dell'infrastruttura cloud che ospita i moduli applicativi e della sicurezza delle comunicazioni. L'Azienda Cliente detiene la responsabilità esclusiva della profilazione RBAC (Role-Based Access Control) dei propri utenti nonché della liceità dei dati anagrafici immessi.

Tale ripartizione è tecnicamente segregata (tramite l'isolamento logico degli ambienti applicativi in Virtual Private Cloud - VPC dedicati per ogni Azienda Cliente, garantendo che i domini di amministrazione operino in perimetri di rete stagni) e documentata contrattualmente mediante l'accettazione diretta e inequivocabile del presente documento in fase di attivazione del servizio.

Ai sensi dell'art. 4 del Reg. UE 2016/679, l'Azienda Cliente agisce in veste di Titolare del Trattamento, mentre Pluservice S.r.l. si configura formalmente come Responsabile esterno del trattamento (ai sensi dell'art. 28 del Regolamento UE 2016/679 - GDPR) per tutte le operazioni di conservazione, elaborazione e protezione dei dati necessarie all'erogazione del servizio SaaS. A tal fine, a formale completamento e disciplina di tale specifico ruolo sul trattamento di dati personali, deve essere obbligatoriamente stipulato tra le parti un apposito Data Processing Agreement (DPA).

Figura di riferimento: Responsabile Sicurezza IT (CISO) di Pluservice S.r.l. per la supervisione della segregazione logica.

Art. 2 Ubicazione Geografica e Giurisdizione dei Dati

Riferimento ISO/IEC 27017: Paragrafi 6.1.3, 18.1.1.

Applicazione: I dati primari e derivati del Cliente sono archiviati fisicamente in Data Center localizzati nel territorio dell'Unione Europea. Qualsiasi controversia legata alla protezione dei dati e all'erogazione del servizio regolata da questo documento è soggetta alla giurisdizione della Repubblica Italiana.

Figura di riferimento: Resp. IT / Ufficio Legale di Pluservice / Data Protection Officer (DPO).

PluService Srl
S.S. Adriatica Sud 228/D 60019 Senigallia (AN) Italy | C.F. e Registro Imprese AN n. 01140590421
REA AN n. 111202 | Capitale sociale € 450.000 i.v. | Dati per la fatturazione: Partita IVA del Gruppo IVA Mooney: 12564030968 - cod. SDI A4707H7 |
www.pluservice.net - pluservice@pluservice.net - pluservicesrl@legalmail.it - tel. +39 071799961

Art. 3 Classificazione, Etichettatura e Protezione dei Record

Riferimento ISO/IEC 27017: Paragrafi 8.2.2, 18.1.3.

Applicazione: L'azienda dichiara che tutti i dati all'interno dei DB gestisti dagli applicativi, essendo dati personali e transazioni, sono considerati confidenziali.

Figura di riferimento: Resp. IT

Art. 4 Gestione degli Accessi e delle Credenziali Utente

Riferimento ISO/IEC 27017: Paragrafi 9.2.1, 9.2.2, 9.2.4.

Applicazione: La registrazione e deregistrazione degli utenti della piattaforma di back-office avviene tramite i moduli di amministrazione forniti a portale. Il sistema impone autonomamente password di minimo 14 caratteri, alfanumerici e almeno un carattere speciale, scadenza password impostabile, almeno un carattere maiuscolo e un carattere minuscolo. Le procedure automatizzate di Pluservice S.r.l. gestiscono le informazioni segrete di autenticazione applicando algoritmi crittografici irreversibili (hash con salt) ai database delle credenziali.

Figura di riferimento: Amministratore di Sistema di Pluservice.

Art. 5 Controlli Crittografici

Riferimento ISO/IEC 27017: Paragrafo 10.1.1.

Applicazione: Al fine di garantire la protezione end-to-end delle informazioni in ambiente Microsoft Azure, l'architettura impone i seguenti controlli crittografici: la protezione dei dati in transito è assicurata dal Cloud Network Engineer tramite l'adozione esclusiva dei protocolli TLS 1.2 e 1.3; la confidenzialità dell'infrastruttura a riposo è garantita dal Cloud Infrastructure Administrator mediante l'applicazione di Azure Disk Encryption (AES-256) sui dischi delle Virtual Machine, utilizzando chiavi archiviate in Azure Key Vault; infine, la segregazione e cifratura dei documenti di identità e dei dati personali (PII) all'interno del database è implementata attraverso la funzionalità nativa Always Encrypted di Azure SQL Database, vincolando l'accesso in chiaro esclusivamente alle applicazioni client autorizzate tramite permessi granulari di accesso al certificato installato nei server che contiene la chiave principale.

Figura di riferimento: Resp. IT /Addetto IT

Art. 6 Gestione delle Modifiche al Servizio (Change Management)

Riferimento ISO/IEC 27017: Paragrafo 12.1.2.

Applicazione: Pluservice S.r.l. fornisce notifica telematica ai referenti di sistema del Cliente in caso di modifiche «Major» (es. aggiornamenti architetturali dell'ERP o dei moduli tariffari) con un preavviso minimo di 7 giorni. Le finestre di manutenzione ordinarie sono eseguite in fasce orarie notturne predefinite a basso impatto per l'operatività. L'obbligo informativo viene applicato anche in caso di variazioni critiche causate dai provider IaaS/PaaS sottostanti.

Dasa-Rägister
UNI EN ISO 9001:2015 IQ-0702-30
UNI EN ISO 14001:2015 IE-0521-01
UNI CEI EN ISO/IEC 27001:2024 IS-1025-05

PluService Srl
S.S. Adriatica Sud 228/D 60019 Senigallia (AN) Italy | C.F. e Registro Imprese AN n. 01140590421
REA AN n. 111202 | Capitale sociale € 450.000 i.v. | Dati per la fatturazione: Partita IVA del Gruppo IVA Mooney: 12564030968 - cod. SDI A4707H7 |
www.pluservice.net - pluservice@pluservice.net - pluservicesrl@legalmail.it - tel. +39 071799961

PLUSERVICE.NET
Società del Gruppo mooney

Figura di riferimento: Resp. IT.

Art. 7 Specifiche delle Funzionalità di Backup

Riferimento ISO/IEC 27017: Paragrafo 12.3.1.

Applicazione: Le specifiche di backup applicate in via standard e irrevocabile a tutti i tenant prevedono: snapshot incrementali orari e backup completi giornalieri. I backup sono conservati in un'infrastruttura di storage isolata con retention di 30 giorni. Pluservice S.r.l. esegue test di ripristino per garantire un Recovery Time Objective (RTO) massimo di 8 ore e un Recovery Point Objective (RPO) massimo di 24 ore, essenziali per la continuità dell'operatività.

Figura di riferimento: Resp. IT / Addetto IT

Art. 8 Funzionalità di Registrazione Eventi (Logging) e Sincronizzazione Orologi

Riferimento ISO/IEC 27017: Paragrafi 12.4.1, 12.4.4.

Applicazione: Pluservice S.r.l. rende disponibile su richiesta i tracciamenti *log* di accesso e di modifica. L'infrastruttura SaaS di Pluservice S.r.l. è rigorosamente sincronizzata con server NTP (Network Time Protocol) internazionali basati su UTC. Si prescrive al Cliente di sincronizzare la propria rete locale e i dispositivi hardware sui medesimi standard NTP per garantire la validità forense delle correlazioni temporali tra i sistemi.

Figura di riferimento: Resp. IT / Addetto IT

Art. 9 Sviluppo Sicuro e Sicurezza nella Catena di Fornitura

Riferimento ISO/IEC 27017: Paragrafi 14.1.1, 14.2.1, 15.1.2, 15.1.3.

Applicazione: L'infrastruttura applicativa è protetta nativamente da Web Application Firewall (WAF). Il ciclo di sviluppo software (SSDLC) di Pluservice S.r.l. include obbligatoriamente test di sicurezza (SAST) sul codice sorgente prima di ogni primo rilascio dell'ambiente di produzione. Contestualmente, Pluservice S.r.l. si avvale di sub-fornitori per l'infrastruttura cloud, dotati delle certificazioni ISO 27001 e ISO 27017, verificandone annualmente l'aderenza per assicurare che la catena del valore non comprometta i livelli di sicurezza.

Figura di riferimento: Resp. IT / Metodi e Tecnologie

Art. 10 Servizi di Assistenza, Ticketing e Gestione Incidenti (Data Breach)

Riferimento ISO/IEC 27017: Paragrafi 16.1.1, 16.1.2, 16.1.7.

Applicazione: Pluservice S.r.l. mette a disposizione del Cliente un portale di Suppot web dedicato (Help Desk B2B) per la segnalazione, il tracciamento e la gestione delle problematiche operative e degli eventi relativi alla sicurezza delle informazioni. Il portale è garantito come accessibile e disponibile per l'inserimento dei ticket H24, 7 giorni su 7. La presa in carico e la risoluzione tecnica sono governate dalle condizioni contrattuali: le anomalie standard

PluService Srl
S.S. Adriatica Sud 228/D 60019 Senigallia (AN) Italy | C.F. e Registro Imprese AN n. 01140590421
REA AN n. 111202 | Capitale sociale € 450.000 i.v. | Dati per la fatturazione: Partita IVA del Gruppo IVA Mooney: 12564030968 - cod. SDI A4707H7 |
www.pluservice.net - pluservice@pluservice.net - pluservicesrl@legalmail.it - tel. +39 071799961

vengono gestite negli orari operativi di ufficio, mentre le anomalie bloccanti e le criticità di sicurezza prevedono canali di intervento a priorità massima.

In caso di accertata violazione dei dati personali o incidenti di sicurezza (Data Breach) che coinvolgano i tenant del Cliente, Pluservice S.r.l. si impegna a informare tempestivamente i referenti designati. La comunicazione includerà un report dettagliato sull'impatto, le contromisure di mitigazione adottate e i log di sistema necessari per supportare il Cliente nelle proprie indagini forensi e nell'assolvimento degli obblighi di notifica all'Autorità Garante per la Protezione dei Dati Personali (ai sensi dell'art. 33 del GDPR).

Figura di riferimento: Resp. Business Unit / Incident Response Team e DPO di Pluservice per la comunicazione e gestione dei Data Breach.

PluService Srl
S.S. Adriatica Sud 228/D 60019 Senigallia (AN) Italy | C.F. e Registro Imprese AN n. 01140590421
REA AN n. 111202 | Capitale sociale € 450.000 i.v. | Dati per la fatturazione: Partita IVA del Gruppo IVA Mooney: 12564030968 - cod. SDI A4707H7 |
www.pluservice.net - pluservice@pluservice.net - pluservicesrl@legalmail.it - tel. +39 071799961