Politica del Cloud

Controllo delle revisioni

Versione	Redazione	Data	Approvazione	Data	Motivo
01	RSGI	10/02/2020	MD	10/02/2020	Prima emissione – Estensioni ISO 27017:2015 e ISO 27018:2019 alla precedente certificazione ISO 27001
02	RSGI	22/03/2022	MD	22/03/2022	Aggiunta servizi di Service Desk; Modifica Carta Intestata; Adeguamento Lista di distribuzione; Controllo Semantico e Ortogrammatico.

Lista di distribuzione

Questo documento è accessibile a chiunque all'interno e all'esterno di **S.M.I. Technologies and Consulting S.R.L.**.

Politica del Cloud

S.M.I. Technologies and Consulting S.r.l. offre una serie di servizi Core IT che riguardano:

- Servizi di Assistenza e Manutenzione (Application and Technical Management);
- Servizi di Building Management System e Facilities Management;
- Servizi di Fleet Management;
- Servizi di Service Integration;
- Servizi di Progettazione di infrastrutture IT;
- Servizi di Project Management;
- Servizi di Progettazione di infrastrutture IoT;
- Servizi di Cyber Security;
- Servizi di fornitura hardware e software;
- Servizi di Service Desk.

S.M.I. Technologies and Consulting S.r.l. si rivolge ad imprese, enti pubblici e privati e aziende di ogni dimensione per governarne processi di implementazione, Tuning, gestione e cut-off.

I principi fondamentali su cui ***S.M.I. Technologies and Consulting S.r.l.*** basa il proprio operato sono:

La **Sicurezza,** il **rispetto delle regole e del cliente**, la **gestione per processi** e per progetti, la **trasparenza** nelle relazioni e il **miglioramento continuo**, soprattutto nell'utilizzo e nella prestazione dei servizi Cloud. Per garantire una continua rispondenza ai bisogni espressi dai propri Clienti in fatto di Qualità, Servizi, Sicurezza delle Informazioni e Tutela dell'Ambiente, ***S.M.I. Technologies and Consulting S.r.l.*** al fine di proteggere ulteriormente le informazioni dei Clienti archiviate e gestite in Cloud, si è posta come obiettivo le certificazioni agli standard ISO 27017:2015 e ISO 27018:2019 e mantenimento delle stesse nel triennio successivo; in quest'ambito assicura la sicurezza per i seguenti aspetti:

- le informazioni archiviate nell'ambiente del Cloud cui il Cliente può avere accesso e che sono gestite dal Provider del Cloud;
- gli asset mantenuti sul Cloud, come le applicazioni;
- i processi in multi-tenant che si possono svolgere nel Cloud virtuale;
- gli utenti del Cloud ed il contesto in cui essi utilizzano il servizio;
- gli amministratori del servizio Cloud dei Clienti che hanno un accesso privilegiato;
- la localizzazione geografica del Provider del Cloud ed i Paesi in cui quest'ultimo può archiviare i dati relativi al Cloud (anche temporaneamente);
- i requisiti base di sicurezza delle informazioni applicabili alla progettazione ed alla implementazione del servizio Cloud;
- i rischi derivanti da addetti ai lavori autorizzati;
- accesso agli asset del Cliente da parte del Provider;
- procedure per il controllo accessi, come la strong authentication per l'accesso amministrativo al Cloud;
- comunicazioni con il Cliente durante il change management;
- allineamento e sicurezza degli ambienti virtuale e Cloud;
- accesso ai dati del Cliente del servizio Cloud e loro protezione;
- comunicazione di Data Breach e linee guida per la condivisione delle informazioni, per aiutare le investigazioni;
- gestione del ciclo di vita dell'account del Cliente.

S.M.I. Technologies and Consulting S.r.l. mette in pratica una Privacy Policy descrivendo le modalità con cui tratta i dati personali nell'ambito della erogazione del servizio di Cloud Computing, anche alla luce degli obblighi imposti dal Regolamento UE 2016/679.

S.M.I. Technologies and Consulting S.r.l. in qualità di Service Cloud Provider (PaaS) assicura che vengano soddisfatte le seguenti condizioni:

- I dati archiviati sui server rimangono sempre di proprietà dell'azienda;
- Impone adeguati controlli di accesso e garantisce che i dati in transito e il caricamento o il trasferimento di file siano protetti con protocolli di crittografia;
- Concede la possibilità di scaricare una copia dei dati in qualsiasi momento ed in totale autonomia e dichiara con la massima trasparenza il luogo fisico dove risiedono i dati;
- Fornisce al Cliente di poter monitorare periodicamente la sua riposta alle prestazioni e al rispetto del contratto;
- Rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il rischio residuo a livelli accettabili;
- Attuazione, ove necessario, di idonee azioni correttive per ridurre a livelli ritenuti accettabili l'incidenza di condizioni anomale sul funzionamento complessivo del sistema;
- Definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (Business Continuity);
- Stabilizzazione e progressivo miglioramento del livello di sicurezza, anche attraverso l'attuazione di idonee azioni preventive, rispetto agli indicatori misurati negli anni precedenti.

Relativamente allo Standard ISO 27018:2019, ***S.M.I. Technologies and Consulting S.r.l.*** garantisce l'implementazione dei controlli richiesti per il trattamento di dati personali, implementando adeguate misure di protezione, nel rispetto dei seguenti requisiti:

- **Scelta e Consenso**: agevolazione dell'esercizio dei diritti di accesso, rettifica e/o cancellazione da parte dell'interessato, attraverso le informazioni rilevanti e le misure tecniche specificate nel contratto.
- **Finalità del trattamento**: le finalità del trattamento sono rese note nel contratto di servizio.
- **Minimizzazione dei dati**: file e documenti temporanei sono cancellati o distrutti entro un periodo specificato e documentato.
- **Limitazione all'uso, alla conservazione e alla divulgazione**: Non avviene la divulgazione di dati personali a Terze Parti. La richiesta di divulgazione di dati personali da parte di autorità amministrative o giudiziarie è notificata al Cliente in maniera tempestiva.
- **Trasparenza**: il ricorso a subappaltatori è reso noto al Cliente del servizio Cloud prima del loro utilizzo. Le disposizioni per l'utilizzo dei subappaltatori sono riportate in chiaro nel contratto tra il Provider e il Cliente. Viene informato il Cliente in modo tempestivo in caso di eventuali modifiche previste in questo senso, in modo tale da concedergli la possibilità di opporsi a tali modifiche o di risolvere il contratto.
- **Accountability**: In caso di violazioni che comportino perdite, diffusione o modifica dei dati personali (Data Breach), effettua la notifica tempestivamente al Cliente attraverso un processo interno di Incident Management.
- **Conformità alla Privacy**: vengono indicati i Paesi in cui sono conservati i dati, anche derivanti dall'utilizzo di subappaltatori e gli specifici accordi contrattuali applicati in merito al trasferimento internazionale di dati. Viene informato tempestivamente il Cliente in caso di eventuali modifiche previste a tale riguardo, in modo da concedergli la possibilità di opporsi o di recedere dal contratto.

Inoltre le seguenti azioni sono assicurate nel senso più esteso dei controlli Cloud:

- fornisce procedure di accesso sicuro per qualsiasi account richiesto dal Cliente del servizio Cloud per gli utenti sotto il suo controllo;
- fornisce le informazioni al Cliente del servizio Cloud in merito alle circostanze in cui utilizza la crittografia per proteggere le informazioni personali che elabora;
- effettua smaltimento sicuro o riutilizzo, delle apparecchiature contenenti supporti di memorizzazione;
- effettua la valutazione del rischio e attua misure tecniche e organizzative per ridurre al minimo i rischi identificati;
- stipula accordi di riservatezza o di non divulgazione tra il provider e i suoi dipendenti e collaboratori;
- implementa meccanismi per il backup off-site per la protezione dalla perdita di dati, garantendo continuità alle operazioni di trattamento dei dati e fornendo la possibilità di ripristinare le operazioni di trattamento dei dati dopo un evento dirompente;
- limita la creazione di materiale cartaceo (comprese le stampe che contengono dati personali);
- procedure di controllo e registrazione del ripristino dei dati;
- procedura di autorizzazione per i dati personali trasferiti su supporti magnetici al di fuori dei locali aziendali del provider e crittografia dei contenuti;
- divieto di utilizzo di supporti e dispositivi di memorizzazione portatili non crittografati a meno di eccezioni;
- crittografia dei dati che vengono trasmessi sulle reti pubbliche;
- smaltimento sicuro dei materiali cartacei;
- utilizzo di ID univoci per i Clienti Cloud;
- stesura e aggiornamento sistematico di un registro degli utenti che accedono al sistema e dei relativi profili di accesso;
- gestione degli ID utente e divieto di assegnazione ad altri di quelli non utilizzati o scaduti;
- evidenza dei controlli minimi di sicurezza nei contratti con clienti e subappaltatori;
- garanzia che ogni volta che lo spazio di archiviazione dei dati viene assegnato a un servizio Cloud, tutti i dati che precedentemente risiedevano su tale spazio di archiviazione siano stati resi intellegibili;
- raggiungere la conformità rispetto alle condizioni contrattuali concordate con il Provider del Cloud pubblico che tratta Informazioni Personali Identificabili e con i Clienti del servizio Cloud.

Il Sistema di Gestione identifica e tiene conto dei requisiti derivanti dall'evoluzione del contesto interno e del contesto esterno, in particolare dei requisiti delle terze parti interessate, e gli obiettivi di sicurezza da perseguire. L'Alta Direzione si impegna ad allocare le risorse necessarie alla realizzazione del predetto sistema e mantiene un "commitment" adeguato sulle tematiche della sicurezza, assicurando che gli obiettivi di sicurezza siano integrati nei processi aziendali e conseguiti.

In considerazione dell'importanza degli obiettivi da raggiungere e dell'impegno necessario per il loro ottenimento, si invita tutto lo Staff a prestare la propria disponibilità e collaborazione nell'attuazione ed aggiornamento del Sistema e ad attenersi scrupolosamente alle prescrizioni contenute nel Manuale del Sistema di Gestione Integrato, nelle Procedure Operative e nelle altre disposizioni in merito eventualmente fornite dal Management.

Roma, 22/03/2022

Presidente

Maria Stella Pizzuto