Sommario

1. INTRODUZIONE

Si riportano nel presente documento gli accordi relativi alla Sicurezza delle Informazioni per i servizi contrattualizzati in ambito Cloud e le informazioni dovute dal fornitore Lascaux srl (nel seguito indicato come "Fornitore").

2. CONDIVISIONE DI RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

Per quanto riguarda l'assunzione di responsabilità in merito ai ruoli che garantiscono la sicurezza delle informazioni, in particolare per le attività (ove applicabili) relative ad:

- Hardening di sistemi e apparati;
- Backup;
- Controlli crittografici;
- Gestione delle vulnerabilità tecniche;
- Gestione degli incidenti;
- Segregazione degli ambienti
- Monitoraggio del Servizio e Raccolta delle registrazioni (log);
- Protezione delle informazioni al termine del contratto;
- Autenticazione e controllo degli accessi

Si concorda che Cliente e Fornitore sono entrambi responsabili, ciascuno per le aree di propriacompetenza, che sono desumibili contrattualmente.
In linea generale vale la regola secondo cui l'onere di effettuare le attività che garantiscono la sicurezza delle informazioni spetta a chi detiene le password degli account con privilegi di amministrazione degli ambienti da mettere in sicurezza.

3. PROTEZIONE DELLE INFORMAZIONI DEL CLIENTE NELL'AMBITO DEI SERVIZI CLOUD

3.1. Garanzie

Il Fornitore garantisce ai propri Clienti, oltre all'applicazione delle idonee misure per la protezione dei dati personali e particolari previste dalla normativa vigente RE UE 679/2016, anche l'applicazione di una serie di misure idonee alla protezione di tutti i dati, tra cui l'adozione, l'applicazione e la certificazione di conformità della/alla norma di sicurezza volontaria ISO/IEC 27001:2013 "Information technology - Security techniques - Code of practice for information security management" ed il rispetto delle linee guida:

- **ISO/IEC 27017:2015** "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- **ISO/IEC 27018:2019** "Information technology - Security techniques - Code of practice forprotection of personally identifiable information (PII) in public clouds acting as PII processors";

Si forniscono maggiori informazioni con particolare riferimento ai seguenti controlli:

a) Autenticazione e controllo degli accessi

L'Accesso al Servizio erogato dal Provider è garantito attraverso credenziali personali degli Utilizzatori. Le credenziali scelte devono rispettare i criteri di sicurezza imposti dal sistema e vengono mantenute sulla base dati del Provider attraverso opportuni meccanismi di crittografia che ne garantiscono la riservatezza.
All'utenza associata a tali credenziali vengono garantiti i permessi strettamente necessari alla visualizzazione e alla modifica dei dati di competenza dell'Utilizzatore.

b) Controlli Crittografici

Il transito dei dati dal browser dell'utilizzatore al server del Provider che eroga il Servizio, è protetto tramite protocollo HTTPS.
Se nell'erogazione del servizio vengono individuati in modo esplicito campi che contengono dati sensibili o particolari, potranno essere definiti opportuni meccanismi di crittografia at-rest.
Tutti i criteri qui menzionati sono validi per gli ambienti di Produzione su cui è installato il servizio. Di conseguenza, gli ambienti di test non devono essere utilizzati per memorizzare dati personali reali.

c) Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche vengono gestite ciclicamente tramite un processo di individuazione strumentale delle vulnerabilità sugli asset (la frequenza è proporzionale al livello di esposizione degli asset stessi), gli input dei vendor e dei gruppi di interesse in contatto con i competence center tecnici oltre che da possibili inneschi provenienti da strumenti di monitoring o da segnalazioni utente.
La comunicazione ed il fixing delle vulnerabilità tecniche segue sempre un iter concordato tra le parti e da definire in fase di transition (change management) ed è comunque in funzione della gravità delle vulnerabilità stesse.

d) Hardening delle macchine virtuali

Le attività di hardening delle macchine virtuali saranno effettuate dal fornitore dei servizi Cloud (Provider) secondo le proprie Policy interne.

e) Condivisione di ruoli e responsabilità

I ruoli e le responsabilità in merito all'erogazione dei servizi offerti dal Provider vengono descritti sul documento "Condizioni Generali di Vendita", che costituiscono parte integrante della Modulistica Contrattuale.

f) Segregazione degli ambienti

La segregazione dei dati tra i diversi tenant gestiti dal Servizio e gli accessi consentiti agli utilizzatori del Servizio è garantita attraverso opportune logiche di controllo, definite secondo le Policy di sviluppo del Provider.

g) Monitoraggio del Servizio

Per garantire il corretto funzionamento del servizio l'applicativo e tutte le risorse ad esso allocate sono costantemente tenute sono monitoraggio al fine di verificare il rispetto degli SLA concordati e di poter intervenire repentinamente qualora si verificassero interruzioni del Servizio.

h) Sicurezza delle reti fisiche e virtuali

La sicurezza delle reti fisiche e virtuali utilizzate per l'erogazione del Servizio è garantita dal possesso delle certificazioni ISO 27001 del Cloud Provider Pubblico.
Il Provider rafforza tale livello di sicurezza garantendo l'utilizzo di una rete virtuale dedicata per ogni tipologia di Servizio SaaS.

i) Conservazione dei dati

Il Provider garantisce la conservazione sicura dei dati degli utilizzatori e, come disciplinato da GDPR, provvede alla loro cancellazione **quando** sono esaurite le finalità per le quali tali **dati** sono stati raccolti.
Ove non diversamente concordato con il cliente del Servizio, il Provider procede alla cancellazione dei dati personali e particolari degli utilizzatori del servizio dopo quattro anni di inattività.

3.2. Trattamento delle informazioni

Le informazioni affidate al Fornitore vengono trattate dal Fornitore stesso per conto del Cliente secondo quanto previsto dalla giurisdizione di riferimento che è quella **europea ed italiana**. Solo ed esclusivamente per le finalità contrattualizzate, a meno di specifici ed espliciti accordi con il Cliente stesso. In particolare, il Fornitore si impegna a non utilizzare le informazioni per finalità commerciali diverse da quelle previste sul Documento di Informativa Privacy senza autorizzazione esplicita del Cliente e dichiara che tale autorizzazione non è mai precondizione necessaria all'erogazione dei propri servizi.
Le informazioni risiedono in Italia in uno o più dei Datacenter Aruba (a meno di differenti specifici ed espliciti accordi con il Cliente).
I trattamenti vengono effettuati esclusivamente da personale qualificato, formalmente incaricato ai sensi delle normative Privacy ed istruito in tal senso.

3.3. Diffusione delle informazioni

In caso di richiesta di consegna da parte di Autorità Giudiziarie o Amministrative (es. Polizia, Carabinieri, Guardia di Finanza, Magistratura), delle informazioni affidate al Fornitore dal Cliente, il Fornitore fornirà al Cliente tempestiva notifica di tale richiesta, tranne nei casi di divieto da parte dell'Autorità stessa.

3.4. Notifica degli incidenti

Il Fornitore si impegna a notificare tempestivamente al Cliente gli incidenti di sicurezza informatica (data-breach) che implichino o consistano di:

- Accessi non autorizzati
- Perdita di dati

- Alterazione di dati
- Diffusione indebita di dati

e che possono venire rilevati tramite strumenti di monitoraggio e controllo o da segnalazioni.
La notifica avverrà via posta elettronica (al riferimento indicato dal Cliente), di norma entro il giorno successivo alla rilevazione dell'incidente. Successivamente alla sua chiusura sarà inviato al Cliente l'Incident Report descrittivo dell'accaduto e delle azioni intraprese.
Il Cliente può segnalare tramite il Portale customer.lascaux.it eventuali anomalie riscontrate nei servizi acquistati. Il Fornitore sarà tenuto a risolvere le problematiche segnalate in base alle SLA riportate nel documento apposito, scaricabile dal portale customer.lascaux.it

3.5. Trasferimento o restituzione delle informazioni o rimozione a fine contratto

Il trasferimento delle informazioni ad altro cloud provider, oppure la ri-consegna delle stesse al Cliente,sono garantite dal Fornitore che indirizzerà su base progettuale qualsiasi richiesta del Cliente in tal senso, stimando tempi e costi delle operazioni e sottoponendone proposta al Cliente. L'esecuzione delle attività è subordinata all'accettazione della proposta, e in tutti i casi è seguita dalla cancellazione sicura.
A fine contratto ed in assenza di richieste di trasferimento delle informazioni oppure di riconsegna come sopra descritte, il Fornitore provvede puntualmente alla cancellazione sicura dei dati cliente, con l'eccezione delle registrazioni che vengono ancora conservate secondo i termini di legge.

3.6. Utilizzo di sub-fornitori

Il Fornitore non prevede il ricorso a sub-fornitori nell'erogazione dei servizi in Cloud.
L'eventuale utilizzo di sub-fornitori nell'erogazione dei servizi contrattualizzati è vincolato al consenso esplicito del Cliente (lettera firmata), al quale devono essere resi noti:
il nome del sub-fornitore
la/e nazione/i nella quale vengono operati i trattamenti delle informazioni
Nel richiedere tale consenso Il Fornitore garantisce di aver esteso al sub-fornitore (o al "peer" serviceprovider), le informazioni necessarie al rispetto delle norme per la sicurezza delle informazioni e che il sub-fornitore si sia impegnato a rispettarle.

3.7. Backup e restore

Il backup dei dati Cliente è finalizzato a consentire il ripristino in caso di eventi avversi.
Il servizio di backup/restore è sempre dovuto dal Fornitore al Cliente tranne nei casi in cui, per naturadel servizio o per esplicitazione contrattuale, è il Cliente stesso a provvedere autonomamente.
Il backup dei dati Cliente, qualora dovuto, viene garantito in duplice copia per tutti i dati, viene eseguito in modalità incrementale dal lunedì al venerdì e in modalità full il sabato e la domenica. Eventuali deroghe richieste dal Cliente possono riguardare ambienti o dati "non di produzione". Originali e copie dei backup vengono conservati in locazioni differenti e il trasferimento dei dati in sede diversa avvienesolo sotto protezione crittografica, in caso di trasporto su supporti magnetici.
A meno di differenti accordi contrattuali, l'inizio dell'attività di restore dei dati in caso di incidente è sempre garantita, nel caso peggiore, nell'arco del giorno lavorativo successivo all'evento che rende necessario il ripristino. La durata complessiva dell'attività di restore è funzione del volume di dati da ripristinare.

3.8. Logging

I servizi di collezione e conservazione dei log a norma di legge sono sempre dovuti dal Fornitore al Cliente tranne nei casi in cui, per esplicitazione contrattuale, è il Cliente stesso a provvedere autonomamente.
I log vengono resi disponibili al Cliente in forma di report "spot", effettuato su richiesta estemporanea del Cliente oppure, se concordato tra i servizi contrattualizzati, in forma di report periodico, o garantendo l'accesso in visione ai dati via rete. In tutti i casi viene garantita la riservatezza delle informazioni nel senso che ogni Cliente ha visibilità esclusivamente dei log relativi a sistemi/servizi disua pertinenza.

3.9. Proprietà intellettuali

I software come qualsiasi altro diritto di autore o altro diritto di proprietà intellettuale sono di proprietà esclusiva di Lascaux e/o dei suoi danti causa; pertanto, Il Cliente non acquista nessun diritto o titolo al riguardo ed è tenuto all'utilizzo degli stessi soltanto nel periodo di vigenza contrattuale.
Nel caso di Licenze e Servizi forniti da terzi fornitori per il tramite di Lascaux, il Cliente, per sé e/o per i terzi cui ha consentito di utilizzare il Servizio e la Licenza, da atto di aver preso visione dei termini e si impegna ad utilizzarli secondo le modalità indicate sui rispettivi siti esclusivamente per proprio uso personale. Il Cliente si impegna ad accettare e rispettare i diritti di proprietà intellettuale e/o industriale secondo quanto indicato in merito nella Policy di utilizzo dei servizi.
Il Cliente dichiara, inoltre, di essere a conoscenza del fatto che le Licenze ed i Servizi intercorrono fra il Cliente ed il titolare dei diritti di copyright sulle stesse con esclusione di qualsiasi responsabilità di Lascaux.
È fatto espresso divieto al Cliente di commercializzare il Software, il Servizio e/o la Licenza quale agente o rivenditore o concessionario o distributore o licenziatario Lascaux o in qualsiasi altra veste e, comunque, di commercializzarli ovvero utilizzarli quali servizi Lascaux. è fatto, inoltre, divieto di utilizzare i marchi e/o le immagini e/o il materiale promo pubblicitario di Lascaux e comunque più in generale qualsiasi diritto di proprietà intellettuale e/o industriale da essa di fatto utilizzato o di cui la stessa è titolare.