TERMINI DI SERVIZIO CARE STUDIO

Il presente documento descrive alcuni aspetti, caratteristiche e precisazioni relative al servizio cloud erogato da ISED, in conformità allo standard internazionale ISO/IEC 27001:2022 e alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019, per i quali ISED è in possesso di certificazione.

1. Ruoli e responsabilità

ISED detiene la responsabilità di erogazione dei servizi di outsourcing della piattaforma oggetto del contratto e di tutte le attività annesse necessarie per garantirne il corretto funzionamento secondo i previsti livelli di servizio; il Cliente, fruitore dei suddetti servizi, è responsabile dei dati che inserisce e, se previsto, ha la possibilità, attraverso utenze applicative privilegiate, di accedere a specifiche funzioni di configurazione e amministrazione applicativa della piattaforma.

2. Comunicazioni e Contatti

Tipologia richiesta	E-mail
Servizio clienti	assistenza@carestudio.it
Legale (PEC)	ised@pec.ised.it
Contatto privacy	privacy@ised.it
Comunicazione al DPO	dpo@ised.it

3. Localizzazione e giurisdizione dei dati

I dati in formato elettronico sono conservati presso il Data Center ISED sito in via Coponia 8 – 00131 Roma.

Una copia dei dati è presente anche in cloud presso AWS nella *region* di Milano.

4. Asset

Gli unici asset del servizio di proprietà del Cliente sono costituiti dai dati. Alla scadenza contrattuale i dati di proprietà del Cliente saranno restituiti al Cliente stesso.

5. Gestione degli utenti e degli accessi

La richiesta di creazione, modifica o disabilitazione di utenze, laddove non gestita direttamente dal Cliente mediante utenze di amministrazione applicativa, può essere effettuata mediante l'invio di e-mail al referente del servizio (vedere paragrafo "2. Comunicazioni e Contatti").

In caso di creazione di nuova utenza sarà comunicata al nuovo utente la password di primo accesso, che il sistema richiederà di cambiare.

Il sistema prevede l'utilizzo di password "forti" con le seguenti caratteristiche:

- *lunghezza compresa tra 8 e 20 caratteri;*
- *non deve contenere il carattere spazio;*
- *deve contenere almeno una lettera minuscola;*
- *deve contenere almeno una lettera maiuscola;*
- *deve contenere almeno un numero;*
- *non deve contenere il nome;*
- *non deve contenere il cognome.*

6. Cifratura

Tutte le trasmissioni dei dati su reti pubbliche vengono effettuate mediante l'utilizzo di protocolli di trasmissione cifrati (es. HTTPS).

7. Gestione delle modifiche

ISED si impegna a comunicare tempestivamente via e-mail al Cliente le modifiche funzionali o infrastrutturali e le interruzioni di servizio programmate che possano avere impatto sulle attività operative del Cliente.

8. Backup e ripristino dei dati

Le procedure di Backup sono necessarie per salvaguardare la base informativa di ISED e dei relativi Clienti, e vengono programmate ed eseguite in funzione della criticità dei dati.

Il Processo di Backup dei dati e degli applicativi rispetta i seguenti principi:

- garantire l'integrità e la disponibilità di dati e di applicativi necessari per la continuità delle attività di business;
- proteggere i dati di Backup con i medesimi meccanismi di protezione dei dati trattati nelle attività di business;
- conservare almeno una copia dei dati di Backup in un luogo tale per cui i dati originali e quelli di Backup non possano essere danneggiati dal medesimo incidente;
- conservare più di una generazione di dati di Backup;
- verificare regolarmente le procedure di Backup e di ripristino.

A seconda dell'importanza dei dati e delle perdite anche finanziarie che possono scaturire dalla loro corruzione o perdita, vengono fissati i seguenti parametri di backup.

- Intervalli (giornalieri, settimanali, mensili);
- Orari nei quali effettuarli (ad esempio alle 18 di ogni giorno lavorativo);
- Periodo di ritenzione delle copie di Backup;
- Quantità dei dati da salvare;

Di tutti i dati esiste una doppia copia, una presso lo stesso CED di ISED, l'altra in cloud presso AWS. Le operazioni di allineamento della doppia copia dei dati avvengono in maniera giornaliera: una copia risiede su file system della macchina dove è operativo il servizio, una seconda copia viene portata all'esterno presso il cloud di AWS.

Per il servizio in oggetto si applicano le seguenti politiche di backup:

Oggetto	Periodicità	Tipologia	Retention	Sistema di archiviazione	Localizzazione
DB	Giornaliero	Logico full	2 giorni	Server DB	CED ISED Roma

Oggetto	Periodicità	Tipologia	Retention	Sistema di archiviazione	Localizzazione
DB	Giornaliero	Logico full	2 settimane	Storage S3	Cloud AWS (*region* Milano)
Application Server	Giornaliero	Logico / Configuration	2 giorni	Server DB	CED ISED Roma
Application Server	Giornaliero	Server virtuale	2 settimane	Storage AWS	Cloud AWS (*region* Milano)
DB	Giornaliero	Fisico incrementale	2 copie (2 settimane)	Server DB	CED ISED Roma
DB	Giornaliero	Fisico incrementale	2 settimane	Storage S3	Cloud AWS (*region* Milano)

9. Gestione dei log

Per quanto riguarda gli Amministratori di Sistema, per tutte le sorgenti di log (Sistemi, Applicazioni e Dispositivi) attinenti al trattamento dei dati personali secondo i criteri espressi dal Garante per la Protezione dei Dati Personali nel documento “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008“, la conservazione dei dati avviene per un periodo temporale non inferiore ai 6 mesi, al termine del quale i dati meno recenti vengono sostituiti con quelli più aggiornati.

Per quanto riguarda gli accessi degli utenti, viene mantenuto un log sui sistemi aziendali.

10. Sincronizzazione degli orologi

Inerentemente agli orari di sistema, il clock utilizzato all'interno dell’infrastruttura di ISED sita in Via Coponia, 8 – Roma, è sincronizzato con i server NTP dell'INRiM (Istituto Nazionale di Ricerca Metrologica).

11. Misure di sicurezza di rete

Dal punto di vista architetturale l’infrastruttura di rete di ISED si basa su un insieme di reti incentrate su una coppia di firewall configurati in alta affidabilità. Questo per garantire non solo la ridondanza fisica degli apparati ma anche il bilanciamento dei carichi di lavoro.

Questa tipologia di firewall permette inoltre di estendere le funzionalità dei comuni firewall con le più evolute funzionalità per affrontare con maggiore completezza le diverse tematiche di sicurezza, tra cui:

- Antivirus: La funzionalità permette l’ispezione del traffico su base signature e su base euristica, permettendo l’identificazione delle minacce più avanzate (Advanced Threat Persistent), l’identificazione di botnet e la possibilità di analizzare i file sospetti;
- Web Content Filtering: La funzionalità di Web Content Filtering dinamico, basato sulla categorizzazione dei siti, viene implementato per garantire maggiore sicurezza nella navigazione Internet e limitare i rischi legati alla responsabilità del traffico proveniente dagli IP pubblici assegnati alla navigazione. Tale categorizzazione è costantemente aggiornata e manutenuta direttamente dal vendor analizzando il testo e le componenti eseguite nei siti web.

- Application Control: La funzionalità permette l'individuazione, la registrazione nei log e l'esecuzione di azioni nei confronti del traffico di rete, sulla base del riconoscimento diretto delle singole applicazioni utilizzate dall'utenza.
- Intrusion Prevention: La funzionalità permette di effettuare l'inspection del traffico di rete e di identificare tipologie di attacco.

La rete aziendale, inoltre, è stata suddivisa internamente in diverse sottoreti (per tipologia di servizio, per cliente) che permettono di sezionare la struttura del Data Center per livelli di sicurezza e affinità di servizi.

I server facenti parte dell'infrastruttura sono collegati con connessioni ridondate in fibra ottica verso lo storage. Questa architettura denominata SAN (Storage Area Network) permette di garantire delle performance elevate, un ottimo livello di affidabilità ed una conveniente flessibilità.

12. Subfornitori

Il Cliente autorizza ISED a nominare eventuali subfornitori. La lista dei subfornitori è consultabile su richiesta formale a ISED. Qualunque modifica di subfornitore verrà comunicata al Cliente tempestivamente. Il Cliente potrà presentare domanda scritta di opposizione all'utilizzo del subfornitore motivandone le ragioni. ISED valuterà la richiesta ed entro 30 giorni fornirà una risposta scritta in modo che il Cliente possa eventualmente rescindere il contratto.

Tutti i fornitori di ISED vengono sottoposti annualmente ad un processo di selezione e qualifica finalizzato a verificare anche il loro livello di sicurezza. Inoltre, laddove trattino dati personali, vengono nominati Responsabili del trattamento ai sensi dell'art. 28 del GDPR.

I servizi forniti da terze parti vengono regolarmente monitorati, riesaminati e registrati; laddove necessario, eventualmente anche mediante degli audit periodici.

I contratti prevedono espressamente degli adeguati livelli di servizio (SLA – Service Level Agreement).

13. Gestione degli incidenti e Personal Data Breach

ISED ha implementato una procedura finalizzata alla gestione degli eventi e degli incidenti di sicurezza definendo ruoli e responsabilità, il processo di rilevazione, l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione, nonché le modalità attraverso le quali effettuare le comunicazioni al Cliente.

Nel caso di violazioni di dati personali per cui è Responsabile del Trattamento, ISED comunicherà tempestivamente, a mezzo PEC, l'eventuale violazione al Cliente (Titolare del Trattamento).

Qualora il Cliente dovesse venire a conoscenza di un possibile incidente di sicurezza può notificarlo a ISED agli indirizzi e-mail indicati nel paragrafo "2. Comunicazioni e Contatti". ISED manterrà aggiornato il Cliente sullo stato di gestione dell'incidente.

ISED si impegna, in seguito a richiesta scritta da parte del Cliente, a fornire tutto il supporto necessario per l'accesso a informazioni/prove digitali inerenti al servizio (ad esempio, in seguito a specifica richiesta da pane delle Autorità).

14. Protezione dei dati e delle registrazioni

I dati e le registrazioni sono protetti utilizzando le seguenti misure di sicurezza:

- Backup
- Controllo degli accessi logici
- Controllo degli accessi fisici

- Cifratura

ISED garantisce una rigorosa segregazione logica dei dati dei clienti e ogni Cliente ha accesso esclusivamente ai dati di propria pertinenza.

15. Operazioni critiche degli Amministratori di sistema

ISED ha definito delle procedure per le operazioni critiche degli amministratori di sistema (es. backup e restore). Qualora il cliente ne faccia richiesta, ISED può fornire estratti di tali procedure.

16. Monitoraggio del sistema

ISED monitora costantemente le prestazioni del sistema attraverso tool specifici di misurazione in conformità con le certificazioni di cui è in possesso.

Se richiesto, ISED fornisce con cadenza periodica ai clienti gli indicatori di monitoraggio, basati sugli SLA contrattualizzati.

Inoltre, in seguito a richiesta scritta da parte del Cliente, sarà possibile per scopi di monitoraggio, concordare le eventuali modalità di accesso da parte del Cliente a specifici aspetti e/o strumenti correlati al servizio.

17. Trattamento dei dati personali

ISED garantisce al Cliente la possibilità di dare seguito alle richieste di esercizio dei diritti degli Interessati che impattino sui dati gestiti da ISED per conto del Cliente.

Tutte le richieste di esercizio dei Diritti vengono gestite secondo la procedura interna di gestione dei diritti degli interessati.

ISED, in qualità di Responsabile del Trattamento, in applicazione del principio di “privacy by default”, tratta i Dati Personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

Relativamente alla portabilità dei dati personali gestiti nel perimetro del servizio, ISED si rende disponibile a concordare con il Cliente le modalità ed i formati di scambio impiegabili, sia per trasferire i suddetti dati ad altro responsabile, sia in caso di richiesta da parte dell'interessato.

Per quanto attiene al tracciamento di eventuali azioni di divulgazione di dati personali non attinenti ai normali scopi del servizio (vedi, ad esempio, richieste da parte delle Autorità), esse saranno notificate al Cliente, a meno di esplicito divieto da parte delle Autorità e saranno opportunamente registrate da ISED.

18. Restituzione e smaltimento dei dati al termine del contratto

Per quanto riguarda la restituzione dei dati trattati del Cliente a valle del termine del servizio, ISED agirà secondo le indicazioni concordate con il Cliente. Per quanto riguarda la cosiddetta "retention" (periodo di conservazione dei dati) prima del loro smaltimento definitivo, ISED li manterrà per 30 giorni dalla loro consegna al Cliente, se non diversamente specificato nel contratto; i dati conservati all'interno dei supporti di backup, previsti secondo quanto indicato nel par. “8. Backup e rispristino dei dati”, si esauriranno secondo il ciclo di vita previsto dalle procedure ivi descritte.

19. Richiesta di informazioni di audit indipendenti relativi alla sicurezza delle informazioni

In seguito a richiesta scritta da parte del Cliente, ISED si rende disponibile a fornire evidenza degli audit interni e di terza parte, condotti relativamente al proprio sistema di gestione della sicurezza

delle informazioni (ISO/IEC 27001:2022), concordando con il Cliente stesso il formato e le modalità di fruizione dei contenuti dei suddetti audit. In alternativa, è possibile concordare l'esecuzione di un audit da parte del Cliente relativamente alle misure di sicurezza implementate da ISED.

Data ultimo aggiornamento: 31/10/2024