WHITEPAPER
SERVIZI SAAS

SGSI UNI CEI ISO/IEC 27001

Rev. 00 del 11/11/2021

horizons unlimited h.u. s.p.a. via c. cignani, 66, 40128 bologna tel. +39.051.370887 fax +39.051.4157636 p.i. e c.f. 04164060370 registro imprese bologna n.04164060370 r.e.a. n.347816 capitale sociale euro 50.000,00

Indice

horizons unlimited h.u. s.p.a. via c. cignani, 66, 40128 bologna tel. +39.051.370887 fax +39.051.4157636 p.i. e c.f. 04164060370 registro imprese bologna n.04164060370 r.e.a. n.347816 capitale sociale euro 50.000,00

Certificazioni

I servizi SaaS Cloud offerti da **Horizons Unlimited H.U. S.p.A.** (di seguito "Horizons") sono progettati e gestiti in accordo ai principali standard internazionali e *best practices* tra le quali:

- **ISO/IEC 9001** - Gestione della Qualità
- **ISO/IEC 27001** - Gestione della Sicurezza delle Informazioni
- **ISO/IEC 27017** - Controlli di sicurezza sul servizio cloud
- **ISO/IEC 27018** - Protezione dei dati personali nel cloud pubblico

Horizons si sottopone volontariamente a verifiche da parte di **Organismi di Certificazione terzi** ed **indipendenti** sulla propria organizzazione del servizio, al fine di fornire garanzie specifiche ed indipendenti.

Infrastruttura

I servizi di Horizons sono erogati in due **Data Center** di Aruba S.p.A., il principale (IT3) si trova a Ponte San Pietro (BG) ed il secondario è situato ad Arezzo (IT1). A questi Data Center si aggiungono le strutture di *Hetzner Online GmbH (Germania)* e *Amazon Web Services Inc. (Irlanda e Germania),* che erogano servizi di elaborazione dati integrati con i servizi di Horizons.

I Data Center utilizzati da Horizons, sono scelti secondo i più moderni standard in termini di affidabilità, prestazioni e sicurezza, garantendo una capacità trasmissiva molto superiore rispetto al fabbisogno effettivo, per assicurare continuità e qualità dei servizi.

Continuità e sicurezza dei Data Center

I Data Center utilizzati da Horizons rispettano i **massimi standard di resilienza previsti**, Tier 4*/Rating 4, la classificazione più alta per i data center.

Il Data Center primario IT3 è dotato della certificazione di qualità ISO 9001, di sicurezza ISO 27001, di gestione ambientale ISO 14001 e per il sistema di gestione

dell'energia ISO 50001. Assicurano **altissimi livelli di affidabilità** delle infrastrutture anche in presenza di gravi guasti grazie a livelli di ridondanza degli impianti che consentono di eseguire operazioni di manutenzione ordinaria senza la necessità di interrompere il servizio erogato.

I Data Center sono attrezzati per sopportare guasti in un qualsiasi punto dell'impianto senza causare downtime dell'infrastruttura oltre a garantire alti livelli di protezione nei confronti degli eventi fisici.

Log-on sicuro

Preme ricordare che il processo di "log-on" degli applicativi Cloud è soggetto a diverse misure di sicurezza (lunghezza, complessità della password, etc.).

Controlli crittografici

Nei servizi SaaS Cloud, i flussi di dati da/verso i sistemi ed i server esposti su Internet, sono protetti utilizzando un canale sicuro **SSL/HTTPS**, mediante opportuna configurazione sui server, tale da assicurare:

- **Autenticazione del server** (con chiave RSA da 2048 bit);
- **Cifratura della sessione** con un algoritmo di cifratura simmetrica considerato sufficientemente sicuro alla data, e con una chiave di sessione di almeno 256 bit.

Questo vale sia per i flussi originati in modo interattivo (Web browsing) sia per quelli generati in modo automatico (per esempio Web services). Come algoritmo di cifratura simmetrica, si utilizza AES 256 bit.

Responsabilità condivisa e proprietà degli asset

Horizons ha identificato le attribuzioni di proprietà per quanto riguarda infrastruttura, licenze, indirizzi IP, software forniti, dati e contenuti immessi dal cliente, suddividendole per servizio/finalità secondo la seguente tabella:

Software Cloud SaaS MediaLibraryOnLine (MLOL, MLOLScuola, MLOLPlus e applicativi correlati)	▪ L'infrastruttura Cloud e fisica è di proprietà dei provider che erogano il servizio (Aruba S.p.A., Hetzner Online GmbH e Amazon Web Services Inc). ▪ I software Cloud sono di proprietà di Horizons che concede in licenza d'uso il servizio al cliente per tutta la durata della sua permanenza sulla piattaforma Horizons, come meglio descritto nelle Condizioni Generali di Contratto sottoscritte dal cliente in fase di acquisto. ▪ Gli indirizzi IP dei servizi SaaS forniti sono di proprietà di Aruba S.p.A. e concessi in uso esclusivo ad Horizons. ▪ Tutto il contenuto a livello di dati, informazioni e documenti forniti e/o condivisi dal cliente mediante i software SaaS rimangono di proprietà e sotto la responsabilità del cliente.
Assistenza Tecnica Help Desk	▪ L'attività di assistenza e supporto al cliente viene erogata tramite le seguenti modalità: (i) assistenza tramite servizio di ticketing Freshdesk diretto per la segnalazione, (ii) FAQ, (iii) Video-tutorial, (iv) webinar. ▪ Gli indirizzi IP dei servizi SaaS forniti sono di proprietà di Aruba S.p.A. e concessi in uso esclusivo ad Horizons. Le modalità di erogazione informatiche dell'assistenza sono di proprietà di Horizons.
Cloud Backup	▪ L'infrastruttura Cloud e fisica è di proprietà dei provider che erogano il servizio (Aruba S.p.A., Hetzner Online GmbH e Amazon Web Services Inc). ▪ La licenza del software di backup, compresi gli agenti installati sui server utilizzati, è di proprietà Aruba S.p.A. ed è concessa in uso ad Horizons. ▪ Anche i dati, le informazioni e i documenti forniti e/o condivisi dal cliente mediante i software SaaS sono sottoposti

	a backup da parte di Horizons, sono quindi sotto la sua responsabilità e viene garantito al cliente per tutta la durata della sua permanenza sulla piattaforma Horizons fino alla scadenza del Contratto sottoscritto.
Cloud Monitoring	▪ Gli asset eroganti il servizio di monitoraggio sono di proprietà di Aruba S.p.A. e di Horizons. ▪ Le licenze dei software di monitoraggio dell'infrastruttura sono di proprietà di Aruba S.p.A. e di Horizons. ▪ Il software Cloud che fornisce i dati di monitoraggio/statistiche ai clienti è di proprietà di Horizons. ▪ I dati, le informazioni e le statistiche forniti e/o condivisi, memorizzati e visualizzati mediante i software SaaS, possono essere monitorati, esaminati, verificati e sono di proprietà e sotto la responsabilità del cliente.
IAAS e CSP	▪ L'infrastruttura utilizzata per erogare il servizio è di proprietà dei provider. ▪ I provider sono qualificati dall'Agenzia per l'Italia Digitale AgID come fornitori di servizi IaaS e CSP assicurando livelli di affidabilità e compliance prevista dalla normativa di riferimento. ▪ I dati, le informazioni e i documenti forniti e/o condivisi o introdotti nella piattaforma SaaS da parte del cliente sono di proprietà e sotto la responsabilità del cliente. ▪ L'utilizzo dell'infrastruttura IaaS e del relativo CSP è implicito nella licenza d'uso del servizio SaaS di Horizons concessa al cliente per tutta la durata della sua permanenza sulla piattaforma Horizons fino alla scadenza del Contratto sottoscritto.
Domain	▪ I domini dei servizi SaaS medialibrary.it, mlolplus.it, openmlol.it, sono di proprietà di Horizons.

Smaltimento sicuro dell'hardware

Horizons attua una specifica procedura di smaltimento per garantire che ogni dato presente negli storage che abbiano raggiunto il loro fine vita e che devono essere sostituiti e smaltiti sia completamente e definitivamente rimosso così come previsto dagli standard internazionali di riferimento ISO/IEC 27001 e Provvedimento del Garante Privacy del 13 ottobre 2008 "*Smaltimento e cancellazione sicura dei dati*".

Reversibilità e Cancellazione sicura dati e files

Le tempistiche di salvaguardia dei dati memorizzati nel sistema informativo aziendale sono di massimo 60 (sessanta) giorni.

La tempistica è da intendersi come tempo tecnico necessario per il completamento delle verifiche sui dati da restituire e cancellare, da compiersi in coordinamento con il Cliente.

Fermo restando quanto previsto, è fatto salvo il diritto di Horizons di trattare i dati anche successivamente alla data di cessazione del contratto al fine di ottemperare a specifici obblighi disposti dal diritto nazionale o dell'Unione, applicabile al Fornitore, nonché di conservare i dati, previa l'adozione di opportune misure di minimizzazione, **per finalità difensive e nei limiti dei termini stabiliti nel Registro dei Trattamenti** e di prescrizione previsti dal diritto nazionale in relazione alle controversie, potenziali o in essere, connesse all'erogazione dei servizi SaaS.

Horizons si assicura che i dati dei clienti vengano eliminati al termine del tempo di salvaguardia concordato secondo le modalità descritte nella tabella che segue.

Dati presenti nei Software Cloud SaaS	Alla cessazione del contratto con il cliente, si interrompe ogni trattamento effettuato per mezzo del servizio SaaS utilizzato dal cliente.
MediaLibraryOnLine (MLOL, MLOLScuola, MLOLPlus e applicativi correlati)	L'estrazione dei dati è indicativamente disponibile entro 48 (quarantotto) ore lavorative, mentre la disattivazione completa del servizio avviene orientativamente in 5 (cinque) giorni lavorativi. I dati sono cancellati entro 60 (sessanta) giorni dalla data di cessazione del contratto siglato tra le parti

horizons unlimited h.u. s.p.a. via c. cignani, 66, 40128 bologna tel. +39.051.370887 fax +39.051.4157636 p.i. e c.f. 04164060370 registro imprese bologna n.04164060370 r.e.a. n.347816 capitale sociale euro 50.000,00

	e tale tempistica è da intendersi come tempo tecnico necessario per il completamento delle verifiche sui dati da restituire e da cancellare in coordinamento con il Cliente. Dopo i 60 giorni indicati, i dati presenti nel database sono anonimizzati con una cancellazione logica per tutelare la struttura della base dati considerata asset aziendale, gli stessi, in base a quanto definito nel Registro dei Trattamenti Dati, vengono successivamente cancellati definitivamente e non possono più essere recuperati.
Cloud Backup	Tutti i dati salvati vengono sottoposti a backup quotidianamente. La cancellazione dei backup memorizzati nell'infrastruttura viene effettuata al massimo dopo 90 giorni, al termine di tale periodo le informazioni contenute nei backup non potranno più essere recuperate. La cancellazione avviene attraverso tool del sistema operativo dei server dedicati a tale processo.
Log di accesso	Nell'infrastruttura dei servizi SaaS sono presenti dei server che registrano ogni genere di attività (accesso, modifica, eliminazione, ricerca) e log di accesso di tutti gli utenti che usufruiscono dei servizi Cloud SaaS. I log degli utenti dei servizi Cloud SaaS sono cancellati dopo 1 anno.

Sviluppo Sicuro e testing

Gli ambienti di sviluppo di Horizons **sono chiusi e non accessibili** ad esclusione del personale Horizons formalmente autorizzato (ADS e Sviluppo Software). I deploy vengono effettuati attraverso **procedure di progettazione e sviluppo degli applicativi web** e **rigorose linee guida di sviluppo sicuro**, atte ad assicurare il rispetto dei principi di *Privacy by Design* e *Privacy by Default*.

Ogni modifica/aggiornamento viene testato secondo fasi di test (di funzionalità, di sicurezza e di non regressione) predefinite e rigorose, il sistema di rilascio in produzione, oltre a richiedere la supervisione di figure di comprovata esperienza,

prevede il versioning.

Infine, per le attività di sviluppo e test è garantito un **ambiente sicuro e separato da quello di produzione**, le cui richieste di accesso vengono sottoposte a verifica e validazione.

Backup

Le componenti funzionali all'erogazione dei servizi SaaS di Horizons, la gestione degli utenti e le altre componenti architetturali del servizio seguono le logiche di ridondanza e di backup che vengono periodicamente verificate e testate. I backup automatizzati dei servizi SaaS di Horizons prevedono proprie politiche in termini di cifratura, periodicità, tipologia (completi o incrementali) in base alle tipologie ed alle specificità dei singoli asset.

Tutti i dati salvati vengono sottoposti a backup quotidianamente.

In dettaglio: le immagini server vengono sottoposte a backup quotidiani con durata settimanale; i Data Base vengono sottoposti a backup quotidiani con durata trimestrale; I file vengono sottoposti a backup quotidiani con durata mensile.

Logging

Horizons raccoglie e conserva i **log dei server per assicurare** ai propri clienti **alti livelli di sicurezza** dei servizi SaaS erogati oltre che la **conformità normativa**. Tali log vengono periodicamente verificati dagli ADS di Horizons.

Horizons registra e conserva per le tempistiche definite nel precedente paragrafo "*Reversibilità e Cancellazione sicura dei dati e dei files*" i log applicativi nell'utilizzo dei servizi SaaS.

Log degli Accessi ai Software Cloud SaaS	Il cliente può consultare dal proprio user-panel disponibile nel software SasS le attività di logging dei propri utenti sotto forma di elaborazioni statistiche anonime.
MediaLibraryOnLine (MLOL, MLOLScuola,	I log degli accessi alle piattaforme online sono conservati nel database per finalità difensive e nei limiti dei termini stabiliti nel Registro dei Trattamenti.

MLOLPlus e applicativi correlati)	
Log delle Attività	I Log delle operazioni svolte dagli utenti (sia interni - *dipendenti* - che esterni - *clienti* - a Horizons) sono registrate nell'infrastruttura per un periodo di 3 mesi. Al termine di tale tempistica i Log vengono cancellati da una procedura automatica e non sono più accessibili. Oltre alle operazioni svolte, i Log delle Attività registrano anche l'utenza personale di colui che le ha compiute.

Comunicazione cifrata

Tutti i servizi SaaS di Horizons rivolti all'esterno utilizzano dei **canali di comunicazione cifrati** (ad esempio canale HTTPS, che è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti http e che viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti ed evitare diffusioni e modifiche non autorizzate).

Il seguente elenco descrive il dettaglio dei protocolli utilizzati su rete pubblica dei servizi SaaS Cloud:

Software Cloud SaaS MediaLibraryOnLine (MLOL, MLOLScuola, MLOLPlus e applicativi correlati)	Tutti i software SaaS Cloud di Horizons sono accessibili solo previa autenticazione dell'utente e sono raggiungibili online tramite certificato cifrato SSL/HTTPS.
Assistenza Tecnica Help Desk	Tutte le attività di assistenza erogate nei confronti dei clienti consentono l'accesso a dati solo previa autenticazione da parte dell'operatore, registrazione delle operazioni svolte, autorizzazione formale da parte del cliente.

horizons unlimited h.u. s.p.a. via c. cignani, 66, 40128 bologna tel. +39.051.370887 fax +39.051.4157636 p.i. e c.f. 04164060370 registro imprese bologna n.04164060370 r.e.a. n.347816 capitale sociale euro 50.000,00

Cloud Backup	I processi di backup sono protetti da password e l'accesso a tali dati è disponibile solo tramite connessioni crittografate con cifratura asimmetrica a 2048 bit nominale per ogni autorizzato.
Cloud Monitoring	I sistemi di monitoraggio utilizzano il protocollo HTTPS e l'accesso ai pannelli di controllo è possibile solo agli ADS
IAAS e CSP	L'accesso all'infrastruttura è possibile solo tramite connessione nominale VPN 2FA con autenticazione SHA-1 e cifratura a 256 bit. Ogni accesso viene registrato ed è possibile solo agli ADS.

Sincronizzazione

Così come previsto dallo standard internazionale ISO/IEC 27001, tutti i sistemi Cloud Horizons utilizzano il sistema NTP per sincronizzare i propri orologi e mantenere coerenza degli eventi. La fonte autoritativa per la sincronizzazione dell'orologio è **INRiM** (https://www.inrim.it).

Il fuso orario su tutti i sistemi utilizzato è CEST su cui viene utilizzato GMT+1. Tutte le macchine virtuali dell'infrastruttura hanno fuso orario basato su CEST e utilizzano come fonte di sincronizzazione clock quella dell'host su cui risiedono.

Sicurezza Organizzativa

In accordo alla propria **Politica SGSI**, Horizons assicura che tutti coloro che operano per l'erogazione dei servizi siano **adeguatamente formati e consapevoli dell'importanza del patrimonio informativo gestito**.

Questa misura applica in particolar modo per le nuove figure aziendali con i quali viene condivisa la politica adottata ed il rispetto dei termini previsti nello specifico accordo di riservatezza (*Non Disclosure Agreements*) per coloro svolgono funzioni di sviluppo e manutenzione dell'area IT. Per ciascuna area aziendale sono stati sviluppati programmi di formazione specifici, che vengono ripetuti e testati con cadenza periodica.

Per garantire la sicurezza dei propri servizi, Horizons controlla gli accessi ai dati ed ai sistemi e limita e monitora gli accessi ad essi.

Tra i principi adottati per la gestione della sicurezza organizzativa ci sono:

- "**need to know**" (Allegato B del D.Lgs. 196/2003) secondo il quale i soggetti che devono compiere attività di trattamento di informazioni sono autorizzati a trattare i soli dati essenziali allo svolgimento dell'attività attribuita;
- "**least privilege**" secondo il quale ad ogni operatore è concesso il privilegio minimo necessario per poter svolgere i propri compiti in modo da ridurre per quanto possibile il rischio di accesso/modifica/cancellazione degli asset e dei dati gestiti;
- "**privacy by design**" per il quale l'obiettivo già in fase di sviluppo dei servizi SaaS Cloud il tema del trattamento dei dati sia prioritario per garantire sicurezza e trasparenza oltre al fine ultimo di prevenire un problema;
- "**privacy by default**" secondo cui si debbano trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste (art. 5 p. 1 lett. b) e per il periodo strettamente necessario a tali fini (art. 5 p. 1 lett. c).

Nello specifico caso in cui si renda necessario l'intervento di Amministratori di sistema Horizons sui sistemi Cloud, **è garantito che i privilegi di accesso siano forniti solo sulla base di specifiche procedure definite** e che tutte le attività siano eseguite secondo iter ed istruzioni predeterminate per le quali sia possibile mantenere traccia.

Gestione delle vulnerabilità

Horizons riconosce che la gestione delle vulnerabilità tecniche dei sistemi informatici rappresenti una delle attività cruciali per poter garantire la sicurezza dei propri servizi: per questo motivo sono predisposte delle misure per ricercare, governare e risolvere le vulnerabilità tecniche individuate per evitare che possano comportare impatti negativi sul servizio e sui dati gestiti.

Gli ADS e gli sviluppatori software compongono il gruppo deputato a eseguire **periodiche e regolari scansioni di vulnerabilità** sia sui servizi offerti alla clientela, sia sull'infrastruttura IT.

horizons unlimited h.u. s.p.a. via c. cignani, 66, 40128 bologna tel. +39.051.370887 fax +39.051.4157636 p.i. e c.f. 04164060370 registro imprese bologna n.04164060370 r.e.a. n.347816 capitale sociale euro 50.000,00

Gestione degli incidenti

Horizons ha definito **controlli e procedure** per poter permettere un approccio organizzato e regolato alla **gestione degli incidenti** come parte della propria strategia di sicurezza delle informazioni.

Horizons ha individuato nello standard ISO/IEC 27001 i propri principi di riferimento per le attività di pianificazione e predisposizione ad una corretta e tempestiva risposta a eventuali eventi di sicurezza, anche con il supporto di una specifica squadra incaricata in base alla peculiarità della problematica riscontrata.

Gestione delle capacità e del cambiamento

Al fine di garantire la corretta consegna/erogazione del servizio Horizons ritiene fondamentale monitorare le risorse a disposizione e adottare gli opportuni accorgimenti per lo sfruttamento ottimale delle stesse.

A tal fine sono state individuate alcune risorse cui applicare un costante monitoraggio ed analisi delle capacità per poter permettere di assicurare la normale fruizione dei servizi.

I livelli di connettività, i livelli di occupazione delle risorse, lo spazio su disco ed il dimensionamento dell'infrastruttura sono monitorati con specifici strumenti di monitoraggio.

Gli strumenti di monitoraggio permettono l'impostazione di controlli specifici per ciascun servizio, rilevando le anomalie e permettendo di anticipare le necessità di cambiamento.

I cambiamenti resi necessari dalle attività di monitoraggio e di gestione delle capacità vengono gestiti in modo controllato per permettere di verificarne i risultati e di mantenere traccia delle attività svolte.

Policy di Sicurezza Logica e Fisica

Per conoscere in dettaglio **le politiche di sicurezza logica e fisica** adottate dai provider nelle proprie infrastrutture presenti nei Data Center, si rimanda ai documenti disponibili nei rispettivi siti internet.

horizons unlimited h.u. s.p.a. via c. cignani, 66, 40128 bologna tel. +39.051.370887 fax +39.051.4157636 p.i. e c.f. 04164060370 registro imprese bologna n.04164060370 r.e.a. n.347816 capitale sociale euro 50.000,00