EasyCloud per Zucchetti HR Infinity & AGO - Strategie tecniche adottate per la compliance

Area adempimento GDPR – NIS2 -DORA	Componenti	EasyCloud for Zucchetti HR & AGO	Note / Riferimenti
Disponibilità – Integrità – del dato	• Connessione Internet e Bilanciatore HTTPS • Presentation Layer Pubblicazione Internet (Web Server - Apache) • Application Layer (JVM - Apache Tomcat) • Data Layer (DB SQL e DMS) • Infrastruttura (rete locale, hardware, alimentazione elettrica) • Backup dati • Cifratura dei dati • Ambiente DR	• Tutte le componenti hardware e infrastrutturali sono ridondate e ove possibile bilanciate • Garantisce la disponibilità dei servizi per ospitare le applicazioni con SLA minimi del 98%[1] • Ogni comunicazione è cifrata con certificati SSL SHA 256 with RSA • I servizi sono oggetto di un piano di Disaster Recovery gestito e simulato periodica • Verifica continua delle prestazioni applicative, capacity planning settimanale. • Gestione continua degli aggiornamenti di sicurezza sulle componenti infrastrutturali	
		• Possibilità d'incrementare i livelli di servizio standard per consentire di ridurre ulteriormente i rischi. Opzionalmente: replica geografica (sempre in Europa), SLA uguali o superiori al 99%, Piani di DR e BC personalizzati, Sistemi di cifratura dei dati aggiuntivi.	Servizi Opzionali
Affidabilità del Titolare e/o del Responsabile del Trattamento Data Breach		• Tutte le componenti sono monitorate per controllare le prestazioni, la disponibilità e integrità dei servizi e dei dati. • Ogni evento e attività sono tracciati in un sistema di ticketing. • Le funzionalità di audit degli accessi e utilizzo delle sue risorse consentono di poter identificare eventuali accessi non corretti ai dati e rispondere velocemente all'intrusione.	La rispondenza alla norma è determinata anche dalla configurazione dell'applicativo applicata in fase di avviamento ad opera del partner applicativo.
Collocazione dei dati nello SEE o in nazioni/territori con livello di protezione adeguato		• Dati in Europa: i dati sono collocati nel territorio europeo (Belgio, Olanda, Germania e Francia). Ambiente di produzione in Belgio, Disaster Recovery Olanda, Salvataggio di sicurezza su infrastrutture indipendenti cloud su cui si appoggiano la produzione e il DR; Francia e Germania) • Tutti di dati sono cifrati AT REST e in transito. [Advanced Encryption Standard (AES) algorithm, AES-256] • Tutti i backup sono cifrati. • Simulazione completa di Disaster Recovery Annuale con coinvolgimento di partner e clienti.	Produzione mensile di report GDPR; personalizzati opzionali per requisiti di compliance specifici
Privacy By Design/ Privacy By Default		• Gli accessi amministrativi sono basati su ruoli limitati e specificatamente assegnati. Tutti i tecnici coinvolti nella gestione dell'infr. hanno credenziali ammnistrative nominali con autenticazione a due fattori per accedere alla stessa e per accedere al proprio computer • Tutte le attività amministrative sull'infrastruttura, i log di sistema di tutti i server sono registrate (Audit / Log), consentendo di sapere l'origine dell'accesso ai dati (cosa, quando chi, come) • Ogni strato dell'infrastruttura e del servizio è pensato per isolare i dati dei clienti. • Le reti locali e di backend sono segmentate per isolare accessi e comunicazioni	
Mantenimento Compliance / Governance	• Il raggiungimento della compliance è un processo continuo che si sviluppa ciclicamente nelle fasi di analisi – implementazione – controllo. Questo processo continuo e le misure di sicurezza proporzionali ai rischi richiedono investimenti che solo le economie di scala possono assicurarvi. Si sottolinea che la conformità alla norma è determinata sia da come l'infrastruttura è implementata e gestita, che dal software e la sua configurazione. • Di seguito le procedure interne che concorrono alla compliance del Servizio: *Availability and Continuity ; Backup & Restore ; Change Management ; Vunerability & Update ; Incident Mgmt ; Disaster Recovery*		

[1] Dato non tiene conto delle manutenzioni programmate dell'infrastruttura; [2] Con attiva l'opzione FLASH lo SLA è del 99%.

Sigemi Srl
Via Brembo, 23 – 20139 Milano MI - Tel. +39.02.98.28.93.50 Fax +39.02.39.19.55.22 | P.IVA e C.F. 08186590967 C.C.I.A.A. Milano – R.E.A. n. 2008542 Capitale Sociale €. 10.000,00 i.v

EasyCloud per Zucchetti HR Infinity & AGO - Strategie tecniche adottate per la compliance

OPERATION ACTIVITIES	Frequenza minima				
	DAILY	WEEKLY	MONTLY	ANNUAL	OTHERS FREQ.
Failed Backup check	Daily (Alert)				
Vulnerability Assessment		Internally			Made from third part Every six moth
Penetration Test					On demand with customer
Disaster Recovery Test				with Application support (Partner) and selected costumer	
Updates / Patches install (OS)		On Pres. Layer resources (Es. Web, App Srv)	For critical update (all remaining layers)		For not critical update Every three month
Updates / Patches install (Application) (Java, Tomcat, …)		Analysis			Based on software vendor certification
Capacity Planning			KPI Analysis and average usage		After receiving alert
Performance Monitor		Analysis			After receiving alert
Log Analysis (Errors / Warning)					After receiving alert
Change Management		Planning, Risk & Impact evaluation			
Problem Management		Open issues analysis (Incidents, Problems)			
Customer Satisfaction				Key and selected Customers	Feedback requested on tickets closing
User Rights review (Administrative)				Review	On organization changes (Role, Responsibility)
Risk Analysis (GDPR)				Review & Update	On significant changes
Security Awareness Training			Analysis		Continuous simulations
Cyber Security training		Weekly Sec. meeting			
Security Risk Analysis (attack surface)					Continuous verifications
Supplier Security Posture Evaluation					Continuous verifications

Sigemi Srl
Via Brembo, 23 – 20139 Milano MI - Tel. +39.02.98.28.93.50 Fax +39.02.39.19.55.22 | P.IVA e C.F. 08186590967 C.C.I.A.A. Milano – R.E.A. n. 2008542 Capitale Sociale €. 10.000,00 i.v

EasyCloud per Zucchetti HR Infinity & AGO - Strategie tecniche adottate per la compliance

<table>
<tr><th>Adempimento GDPR</th><th>Strategia / Implementazione adottata</th></tr>
<tr><td>Governance</td><td>Sigemi non ha informazioni certe sulla natura dei dati che transitano sulle piattaforme di servizi offerte ai clienti; pertanto, ha deciso di considerare tutti i dati come “Dati Particolari”.</td></tr>
<tr><td>Collocazione Dati</td><td>I dati gestiti sulle piattaforme sono situati in Europa (Belgio, Olanda). I backup dei dati sono collocati in Europa (Olanda, Germania e Francia).</td></tr>
<tr><td>Analisi del rischio e degli impatti</td><td>Sigemi esegue una analisi annuale dei rischi coinvolgendo il responsabile del trattamento dei dati. Sigemi, su richiesta, può fornire le informazioni, nonché il supporto al Titolare nello svolgimento di una valutazione d’impatto, qualora lo stesso fosse tenuto ad effettuarla.
vulnerability assessment, eseguito ogni 7gg internamente e ogni 6 mesi da società esterna indipendente.</td></tr>
<tr><td rowspan="2">Privacy By Design</td><td>Le impostazioni di base previste dalle procedure in essere in Sigemi prevedono la privacy by design, by default e least privileged
Il personale Sigemi è formato continuamenti sui temi della sicurezza e privacy secondo quanto indicato nel GDPR.</td></tr>
<tr><td>Certificazioni Infrastrutturali
ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
SOC 1
SSAE16 / ISAE 3402 (SOC 2/3)</td></tr>
<tr><td>Integrità</td><td>Tutti i dati sono salvati con frequenza minima giornaliera in locale e off-cloud. I dati sono cifrati. La retention dei backup è definita nello SLA di ogni singolo servizio erogato. Il cliente può esprimere la necessità di requisiti differenti dallo standard che possono essere soddisfatti da servizi opzionali.</td></tr>
<tr><td></td><td>Tutte le componenti critiche per garantire la disponibilità del servizio sono ridondate.
Il piano di Disaster Recovery viene testato almeno ogni 12 mesi. SLA di ripristino:
<table>
<tr><th rowspan="2">Componenti / Layer</th><th colspan="2">Google vDataCenter</th><th colspan="2">GCP vDataCenter</th></tr>
<tr><th>RTO</th><th>RPO</th><th>Business Continuity Strategy</th><th>Infrastr. SLA / Mese</th></tr>
<tr><td>• Internet connection</td><td>n.a</td><td>n.a</td><td rowspan="2">Premium Tier
(Bilanciamento)</td><td rowspan="3">>= 99.99%</td></tr>
<tr><td>• Bilanciatore HTTPS e WAF</td><td>n.a</td><td>n.a</td></tr>
<tr><td>• Web Servers</td><td>2h</td><td>24h</td><td rowspan="2">Bilanciamento Applicativo
in data center differenti (GCP Zone)</td></tr>
<tr><td>• Application Servers</td><td>2h</td><td>24h</td><td>>= 99.5%</td></tr>
<tr><td>• Data Base Server</td><td>4h</td><td>24h</td><td></td><td>>= 99.9%</td></tr>
<tr><td>• File Share (NFS)</td><td></td><td>24h</td><td>FS as a service (replicato e bilanciato)</td><td>>= 99.99%</td></tr>
<tr><td>• Back-end Networking</td><td>4h</td><td>n.a</td><td></td><td>>= 99.5%</td></tr>
<tr><td>• Altri Server</td><td>8h</td><td>24h</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Diritto cancellazione</td><td>Sigemi provvede alla cancellazione sicura di tutti i dati del cliente alla chiusura del contratto. (cancellazione effettiva dei dati dopo i tempi di retention dei backup)</td></tr>
<tr><td>Data Breach</td><td>Sigemi ha adottato sistemi di log collection degli eventi di accesso amministrativo ai server e al database per rilevare prontamente possibili violazioni dell’integrità e confidenzialità dei dati dei propri clienti. Sigemi si è dotata di una procedura di gestione degli incidenti di sicurezza conforme alle normative GDPR, NIS2 e DORA</td></tr>
<tr><td>Riferimenti</td><td>https://cloud.google.com/terms/sla | https://cloud.google.com/network-tiers |</td></tr>
</table>

Sigemi Srl
Via Brembo, 23 – 20139 Milano MI - Tel. +39.02.98.28.93.50 Fax +39.02.39.19.55.22 | P.IVA e C.F. 08186590967 C.C.I.A.A. Milano – R.E.A. n. 2008542 Capitale Sociale €. 10.000,00 i.v

GCP - EasyCloud per Zucchetti HR Infinity & Ago - Log Retention

Log Type	Windows Platform		Linux Platform		Nerwork Services		Note
	Collection Method	Retention	Collection Method	Retention	Collection Method	Retention	
Security							
• Autenticazione	WinEvt + log collection	365	Local-SystemLog + Bucket	365			
• Creazione / Modifica utenze e Gruppi			GCP Log	400	GCP Log	400	
Configuration Mgmt							
• Modifica configurazione hardware (Virtuale)	GCP Log	400	GCP Log	400			
• Parametri di sistema (installazione, …)	WinEvt + log collection	365	WinEvt + log collection	365			
Network Operative System	WinEvt + log collection	365	Local-SystemLog + Bucket GCP Log	365 400	GCP Log	400	
Application (SQL, Scheduler, FTP Serv,…| Catalina, Apache, Postifix,…)							
Backup	Log + GCP Log	400	Log + GCP Log	400	na	na	

Sigemi Srl
Via Brembo, 23 – 20139 Milano MI - Tel. +39.02.98.28.93.50 Fax +39.02.39.19.55.22 | P.IVA e C.F. 08186590967 C.C.I.A.A. Milano – R.E.A. n. 2008542 Capitale Sociale €. 10.000,00 i.v