SIGEMI

GCP - EasyCloud per Zucchetti HR Infinity /AGO Zucchetti - compliance GDPR

Area Adempimento GDPR	Componenti	EasyCloud HR/AGO Zucchetti	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 • Ambiente DR	• Tutte le componenti hardware e infrastrutturali sono ridondate • Garantisce la disponibilità dei servizi per ospitare le applicazioni con SLA del 98,00%.[12] • Ogni comunicazione è cifrata con certificati SSL SHA 256 with RSA • I servizi sono oggetto di un piano di Disaster Recovery gestito e verificato periodicamente • Verifica continua delle prestazioni applicative, capacity planning settimanale. • Tutti i dati sono salvati in più copie criptate in archivi differenti. • 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 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 (*Accountability*)		• 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. • Fornisce report automatizzati sullo stato dell'applicazione consentendovi di dimostrare il pieno controllo sul dato.	La rispondenza alla norma è determinata anche dalla configurazione dell'applicativo definita in fase di avviamento.
Data Breach		• 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.	
Collocazione dei dati in Europa o in nazioni/fornitori previsti dal GDPR		• Dati in Europa: i dati sono collocati nel territorio europeo (Italia, Belgio, Germania e Francia).	Produzione mensile di report GDPR; personalizzati opzionali per requisiti di compliance specifici
Privacy By Design/Default		• Gli accessi amministrativi sono basati su ruoli limitati e specificatamente assegnati. • Le credenziali di accesso sono salvate e scambiate attraverso tecniche di hashing. • L'autenticazione degli utenti amministrativi prevede l'utilizzo di autenticazione a 2 fattori. • Tutte le attività amministrative sull'infrastruttura sono registrate (Audit / Log), consentendo di sapere l'origine dell'accesso ai dati (chi, quando e da dove).	
Security By Design		• Ogni strato dell'infrastruttura e del servizio è pensato per isolare i dati dei clienti. • Ogni sei mese viene eseguito una verifica della vulnerabilità (Vuknerability Asessment) svolto da società esterne. • Google esegue penetration test periodici sui servizi infrastrutturali condovisi. (Es. La connessione, il firewall, il bilanciamento delle sessioni http/https, …)	
Mantenimento Compliance	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. Detto questo, è importante considerare che la conformità alla norma è determinata sia da come l'infrastruttura è implementata e gestita, sia dal software e la relativa configurazione.		

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 Zucchetti - Strategie tecniche GDPR

<table>
<tr><th>Adempimento GDPR</th><th>Stategia / 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 trattare tutti i dati come “Dati Particolari”.</td></tr>
<tr><td>Collocazione Dati</td><td>I dati gestiti sulle piattaforme sono situati in Europa (Italia, Belgio, Germania). I backup dei dati sono collocati in Europa (Italia, Belgio, Germania, Francia).</td></tr>
<tr><td>Analisi del rischio e degli impatti</td><td>Sigemi esegue una analisi annuale dei rischi e degli impatti coinvolgendo il responsabile del trattamento dei dati.
Vulnerability assessment delle infrastrutture, eseguito ogni 6 mesi da società terza.</td></tr>
<tr><td>Privacy By Design</td><td>Le impostazioni di base previste dalle procedure in essere in Sigemi prevedono la privacy by design.
Il personale Sigemi è formato continuamenti sui temi della sicurezza e privacy secondo quanto indicato nel GDPR.
<table>
<tr><td>Certificazioni Infrastrutturali</td><td>ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018</td><td>SOC 1
SSAE16 / ISAE 3402 (SOC 2/3)</td></tr>
</table></td></tr>
<tr><td>Integrità</td><td>Tutti i dati sono salvati con frequenza minima giornaliera in locale e off-site. 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</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></td><td></td></tr>
<tr><td>• Data Base Server</td><td>4h</td><td>24h</td><td></td><td>>= 99.5%</td></tr>
<tr><td>• File Share (NFS)</td><td></td><td>24h</td><td>FS aa a service (replicato e bilanciato)</td><td>>= 99.9%</td></tr>
<tr><td>• Back-end Networking</td><td>4h</td><td>n.a</td><td></td><td>>= 99.99%</td></tr>
<tr><td>• Altri Server</td><td>8h</td><td>24h</td><td></td><td>>= 99.5%</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 con l’aggiunta della retention dei salvataggi definita nel contratto</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.</td></tr>
<tr><td>Riferimenti / link</td><td>https://cloud.google.com/terms/sla | https://cloud.google.com/network-tiers | https://cloud.google.com/files/gcp-mpaa-compliancemapping.pdf | https://cloud.google.com/files/GCP_Client_Facing_Responsibility_Matrix_PCI_2018.pdf</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

SIGEMI

GCP - EasyCloud per Zucchetti HR Infinity /AGO Zucchetti - 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	90	Local-SystemLog + Bucket	180			
• 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	90	WinEvt + log collection	90			
Network Operative System	WinEvt + log collection	90	Local-SystemLog + Bucket GCP Log	180 400	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