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 periodicamente • Verifica continua delle prestazioni applicative, capacity planning settimanale. • Gestione continua degli aggiornamenti di sicurezza sulle componenti infrastrutturali	• (min ogni 12mesi)
		• 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		• 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	Rif. Controlli ISO27001	Frequenza minima				
		DAILY	WEEKLY	MONTLY	ANNUAL	OTHERS FREQ.
Failed Backup check	8.13	Daily (Alert)				
Vulnerability Assessment	8.1; 8.25		Internally			Made from third part Every six moth
Penetration Test	8.1; 8.25					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, …)	8.1; 8.25		Analysis			Based on software vendor certification
Capacity Planning	8.6; 8.14;8.27; 5.30			KPI Analysis and average usage		After receiving alert
Performance Monitor	8.5; 8.15;8.16		Analysis			After receiving alert
Log Analysis (Errors / Warning)	8.5; 8.15;8.16					After receiving alert
Change Management	8.9; 8.19; 8.26; 8.29, 8.31; 8.33; 8.34		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)	5.15; 5.17; 5.18; 8.1; 8.6				Review	On organization changes (Role, Responsibility)
Risk Analysis (GDPR)					Review & Update	On significant changes
Security Awareness Training	6.3			Analysis		Continuous simulations
Cyber Security training	6.3		Weekly Sec. meeting			
Security Risk Analysis (attack surface)	8.1; 8.25, 8.16					Continuous verifications
Supplier Security Posture Evaluation	5.19-5.22					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 [Rif. ISO27001]</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>>= 99.5%</td></tr>
<tr><td>• File Share (NFS)</td><td>2h</td><td>24h</td><td></td><td>>= 99.5%</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. (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 [Rif. ISO27001 8.5; 8.15;8.16, 8.13]	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

EasyCloud per Zucchetti HR Infinity & AGO – Compliance Strategies [ENG version]

GDPR – NIS2 -DORA compliance topics	Componenti	EasyCloud for Zucchetti HR & AGO	Note / Riferimenti
Data Availability – Integrity	• Internet Connection and HTTPS Load Balancer • Presentation Layer (Web Server - Apache) • Application Layer (JVM - Apache Tomcat) • Data Layer (DB SQL e DMS) • Infrastructure layer (local area network , hardware, power supply) • Backup dati • Data Encryption • DR Environment	• All hardware and infrastructure components are redundant and, where possible, balanced. • Ensures service availability to host applications with minimum SLA of 98%[1]. • All communications are encrypted with SSL SHA 256 with RSA certificates. • Services are subject to a managed and periodically simulated Disaster Recovery plan. • Continuous monitoring of application performance and weekly capacity planning are conducted. • Ongoing management of security updates for infrastructure components is performed.	
		• Increasing standard service levels to further reduce risks, it's possible as optional . Optionally: geographical replication (always within Europe), SLAs equal to or greater than 99%, customized DR and BC Plans, additional data encryption systems.	Optional Services
Data Controller and/or Data Processor Reliability Data Breach		• All components are monitored to ensure service performance, availability, and data integrity. • Every event and activity is tracked in a ticketing system. • The audit functionalities for access and usage of its resources make it possible to identify any incorrect data access and respond quickly to intrusion.	Conformity is also determined by the application configuration applied in the start-up phase by the application partner.
Data Location(SEE)		• Data in Europe: data are located in Europe (Belgium, Holland, Germany and France). • Production environment in Belgium, Disaster Recovery Netherlands, data backups on a different cloud infrastructures respect production enviroment; France and Germany) • All data is encrypted AT REST and in transit. [Advanced Encryption Standard (AES) algorithm, AES-256] • All backups are encrypted. • Comprehensive Annual Disaster Recovery simulation involving partners and customers.	Monthly GDPR reports; Optional addon customizations for specific compliance requirements
Privacy By Design/ Privacy By Default		• Administrative access is based on limited and specifically assigned roles. All technicians involved in the management of the infrastructure have personal administrative credentials with two-factor authentication to access it and to access their own computer. • All administrative activities on the infrastructure, system logs of all servers are recorded (Audit / Log), allowing the origin of data access (what, when, who and how) to be known. • Each layer of the infrastructure and service is designed to isolate customers' data. • Local and backend networks are segmented to isolate access and communication.	
Governance / Compliance Maintenance	• Compliance achievement is a continuous process that cyclically unfolds in the phases of analysis - implementation - control. This continuous process and the security measures is proportional to the risks require investments that only economies of scale can ensure. It is emphasized that compliance with the standard is determined both by how the infrastructure is implemented and managed, and by the software and its configuration. • Below are the internal procedures that contribute to Service compliance:: Availability and Continuity ; Backup & Restore ; Change Management ; Vulnerability &Update ; Incident Mgmt ; Disaster Recovery		

[1] Value don't include planed infrastructure maintenance ; [2] FLASH Subscription have a availability SLA off 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 – Compliance Strategies [ENG version]

OPERATION ACTIVITIES	ISO27001 checks	Minimum frquency				
		DAILY	WEEKLY	MONTLY	ANNUAL	OTHERS FREQ.
Failed Backup check	8.13	Daily (Alert)				
Vulnerability Assessment	8.1; 8.25		Internally			Made from third part Every six moth
Penetration Test	8.1; 8.25					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, …)	8.1; 8.25		Analysis			Based on software vendor certification
Capacity Planning	8.6; 8.14;8.27; 5.30			KPI Analysis and average usage		After receiving alert
Performance Monitor	8.5; 8.15;8.16		Analysis			After receiving alert
Log Analysis (Errors / Warning)	8.5; 8.15;8.16					After receiving alert
Change Management	8.9; 8.19; 8.26; 8.29, 8.31; 8.33; 8.34		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)	5.15; 5.17; 5.18; 8.1; 8.6				Review	On organization changes (Role, Responsibility)
Risk Analysis (GDPR)					Review & Update	On significant changes
Security Awareness Training	6.3			Analysis		Continuous simulations
Cyber Security training	6.3		Weekly Sec. meeting			
Security Risk Analysis (attack surface)	8.1; 8.25, 8.16					Continuous verifications
Supplier Security Posture Evaluation	5.19-5.22					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 – Compliance Strategies [ENG version]

<table>
<tr><th>GDPR and ISO27001 ref.</th><th>Solutions and Strategies adopted</th></tr>
<tr><td>Governance</td><td>Sigemi has no certain information on the kind of data passing through the service platforms offered to customers; therefore, it has decided to consider all data as “Particular Data”.</td></tr>
<tr><td>Data Location</td><td>The data managed on the platforms are located in Europe (Belgium, the Netherlands). Data backups are located in Europe (the Netherlands, Germany and France).</td></tr>
<tr><td>Risk Analysis</td><td>Sigemi carries out an annual risk analysis involving the data controller. Sigemi, upon request, can provide information as well as support to the Data Controller in carrying out an impact assessment, should he be required to do so.
vulnerability Assessment, carried out every 7 days internally and every 6 months by an independent external company.</td></tr>
<tr><td rowspan="2">Privacy By Design</td><td>The default settings in Sigemi's existing procedures provide for privacy by design, by default and least privileged
Sigemi's staff is continuously trained on security and privacy issues according to the GDPR.</td></tr>
<tr><td>Certifications ISO/IEC 27001 ISO/IEC 27017 ISO/IEC 27018 SOC 1 SSAE16 / ISAE 3402 (SOC 2/3)</td></tr>
<tr><td>Integrity</td><td>All data are saved at least daily in the local and off-cloud. Data are encrypted. Backup retention is defined in the SLA of each individual service provided. The customer may express the need for different requirements from the standard that can be fulfilled by optional services.</td></tr>
<tr><td>[]</td><td>All critical components to ensure service availability are redundant. The Disaster Recovery plan is tested at least every 12 months. Recovery SLA:
<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 (Balanced)</td><td rowspan="3">>= 99.99%</td></tr>
<tr><td>• http/s Balancer and 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">Application Balancing to different data centers (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>>= 99.5%</td></tr>
<tr><td>• File Share (NFS)</td><td>2h</td><td>24h</td><td></td><td>>= 99.5%</td></tr>
<tr><td>• Back-end Networking</td><td>4h</td><td>n.a</td><td></td><td>>= 99.99%</td></tr>
<tr><td>• Other Servers</td><td>8h</td><td>24h</td><td></td><td>>= 99.5%</td></tr>
</table>
</td></tr>
<tr><td>Delete rights</td><td>Sigemi execute secure deletion of all customer data at the end of the contract. (complete delete of data after backup retention times)</td></tr>
<tr><td>Data Breach</td><td>Sigemi has adopted logging solution to collect administrative access events on server and database ; in order to promptly detect possible breaches of the integrity and confidentiality of its customers' data. Sigemi has a security incident management procedure that complies with the GDPR, NIS2 and DORA regulations.</td></tr>
<tr><td>Reference</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

EasyCloud per Zucchetti HR Infinity & AGO – Compliance Strategies [ENG version]

Log Retention

Log Type [Ref. ISO27001 8.5; 8.15;8.16, 8.13]	Windows Platform		Linux Platform		Nerwork Services		Note
	Collection Method	Retention	Collection Method	Retention	Collection Method	Retention	
Security							
• Authentications	WinEvt + log collection	365	Local-SystemLog + Bucket	365			
• Users and Groups creation/change			GCP Log	400	GCP Log	400	
Configuration Mgmt							
• vServer configurations changes	GCP Log	400	GCP Log	400			
• Infr, settings changes (setup, …)	WinEvt + log collection	365	WinEvt + log collection	365			
Network Operative System Application (SQL, Scheduler, FTP Serv,…| Catalina, Apache, Postifix,…)	WinEvt + log collection	365	Local-SystemLog + Bucket GCP Log	365 400	GCP Log	400	
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