Allegato B - Condizioni generali di offerta e requisiti per la sicurezza delle informazioni per l'uso del Software as a Service- Rev. 0

REQUISITI DI SICUREZZA E TRATTAMENTO DATI PERSONALI

1.Requisiti di Sicurezza e Segnalazioni

Requisiti da mantenere	Misure/Strumenti Adottati dall'Organizzazione	Evidenze Prodotte
Sistema di sicurezza delle informazioni del servizio cloud secondo standard ISO 27001 – 27017 – 27018.	Certificazione del sistema di gestione per la sicurezza delle informazioni. Procedura P2/05 "Gestione degli incidenti di sicurezza"	Procedura approvata dalla direzione e presente nella documentazione di sistema di gestione per la sicurezza delle informazioni.
Divulgazione degli incidenti e specifiche sulle azioni intraprese per il trattamento da parte di GeneGIS GI Srl	Report trimestrale riepilogativo degli incidenti occorsi e sul loro trattamento	M2/05/04 "Report situazione incidenti nel servizio cloud". Comunicazione formale ad eventuali Autorità Interessate.
Segnalazioni al cliente di incidenti di sicurezza, rilevati da GeneGIS GI Srl	Procedura per la notifica dell'incidente di sicurezza in cloud come descritto in P2/05 – "Gestione incidenti di sicurezza" al Referente indicato dal cliente per la gestione degli incidenti	Vedi M2/05/03 "Comunicazione incidente nel servizio cloud"; Eventuali comunicazioni ad Autorità Interessate.
Tempi di notifica al cliente della segnalazione di incidente con disservizio, rilevato da GeneGIS GI Srl	Classificazione e registrazione di incidente specifico per il cliente	Avviso al cliente, in caso di disservizio, entro 1 ora dalla avvenuta classificazione con mail al referente del cliente.
Segnalazioni di incidente di sicurezza da parte del **Cliente:** informazioni di contatto per la gestione delle segnalazioni di incidente e/o problematiche relative alla sicurezza	Piattaforma di ticketing; mail dedicata; recapiti telefonici dedicati; Procedura P2/05 "Gestione degli incidenti di sicurezza".	Disponibilità in orario di lavoro (lunedì – venerdì dalle 08:30 alle 13:00 e dalle 14:30 alle 18:00): • Ticket (o mail assistenza@pagis.it • assistenza@pangeacloud.com • assistenza@rootsgreenlogistics.com Presa in carico entro 1 ora, con avviso al cliente. Gestione incidente come da procedura P2/05 – "Gestione incidenti di sicurezza"
Rimedi applicabili a fronte di alcune tipologie di incidenti sulla sicurezza di informazioni da parte di GeneGIS GI Srl	Quelli descritti nel modulo di comunicazione dell'incidente e/o nel reporting trimestrale	Vedi M2/05/03 "Comunicazione incidente nel servizio cloud" con note a tal riguardo
Informazioni al cliente sullo stato di avanzamento del trattamento degli incidenti da parte di GeneGIS GI Srl	Aggiornamento del modulo di comunicazione al cliente con lo stato di implementazione delle azioni di trattamento dell'incidente	Vedi M2/05/03 "Comunicazione incidente nel servizio cloud" Trasmesso con mail o con applicazione di ticketing
Reporting periodico sugli incidenti da parte di GeneGIS GI Srl	Reporting trimestrale da pubblicare sulla piattaforma ProceduraComCloud accessibile ai soli referenti per la gestione degli	Vedi M2/05/04 "Report situazione incidenti nel servizio cloud"

Requisiti da mantenere	Misure/Strumenti Adottati dall'Organizzazione	Evidenze Prodotte
	incidenti nominati dai clienti	
Crittografia Dati	GeneGIS GI Srl , di default, non implementa sistemi di crittografia sui database contenenti dati del cliente. A richiesta del cliente è possibile definire delle policy di crittografia dei database.	Contratto personalizzato per gestione crittografia database.
Sviluppo sicuro	GeneGIS GI Srl si è dotata di una policy interna di sviluppo software che prevede l'adozione di requisiti di sicurezza conformi a standard riconosciuti. Lo sviluppo avviene in ambiente separato da quello di produzione e tiene conto dei requisiti di Privacy by Design e by Default.	Certificazione sistema di gestione per la sicurezza delle informazioni secondo gli standard ISO/IEC 27001 – ISO/IEC 27017 - ISO/IEC 27018
File Temporanei	I file temporanei generati nell'uso delle applicazioni vengono cancellati con la chiusura dell'applicazione.	

2. Trattamento dei dati personali

Le parti convengono che in merito al trattamento dei dati personali, ai sensi della normativa europea Reg. UE 2016/679 - GDPR, il Cliente assume il ruolo di Titolare del trattamento dei dati e GeneGIS GI Srl assume il ruolo di Responsabile del trattamento dati ai sensi del art.28 del GDPR per tutte le operazioni di trattamento necessarie e connesse all'esecuzione del presente Contratto e dei Servizi Attivati. Lo standard di nomina di GeneGIS GI Srl quale Responsabile del trattamento è pubblicato nel sito internet della Società al link "https://www.genegis.it/documenti-contrattuali/". Qualora il Titolare voglia avvalersi di uno proprio standard di nomina del Responsabile del trattamento, tale documento dovrà prevedere la possibilità, per GeneGIS GI Srl, di avvalersi di sub-responsabili, identificando in tale ruolo il partner coinvolto nella erogazione del servizio in cloud (AWS o altro CSP qualificato AGID-ACN) presso cui sono allocate le infrastrutture tecnologiche, le applicazioni software ed i dati di cui è Titolare il cliente. La lettera di nomina, a seguito di valutazione dei requisiti in essa riportati, verrà formalmente accettata da GeneGIS GI Srl srl ed inviata al cliente successivamente alla firma del contratto.

I dati personali potranno essere comunicati ad Autorità Giudiziarie o Autorità/Enti Ispettivi di controllo (Garante Privacy) ai fini dello svolgimento delle loro funzioni istituzionali e nell'esecuzione di un obbligo di legge in merito ad attività istruttorie o richieste specifiche, senza autorizzazione da parte del Cliente, a meno di formali accordi, facenti parte del presente contratto, che facciano riferimento a norme che vietano la fornitura degli stessi.

2.1 Informativa di cui all'art 13 del Regolamento U.E 679/2016

Così come previsto dal Reg. U.E. 679/2016 e dal D.Lgs. 196/2003 i dati personali di soggetti che saranno contattati per esecuzione del Contratto, che rappresentano a vario titolo il cliente, sono trattati in conformità alla normativa sopra citata. Apposta informativa, rinvenibile sul sito internet www.genegis.it,

specifica nel dettaglio le finalità e la base giuridica del trattamento, la tipologia dei dati trattati, i soggetti a cui i dati possono essere comunicati e/o resi disponibili, la durata del trattamento ed i riferimenti per l'esercizio dei diritti dell'interessato.

2.2 Esercizio dei diritti dell'interessato e Data Breach

GeneGIS GI Srl ha predisposto procedure operative per l'esercizio dei diritti dell'interessato e per il Data Breach. Le attività di controllo sulla sicurezza in materia di trattamento di dati personali rimangono in capo al Team funzioni Responsabili dei processi (Direzione Aziendale, Rappresentante della Direzione per il sistema di gestione integrato e del Resp. Sicurezza Informatica) che governano il sistema di gestione per la sicurezza delle informazioni secondo lo standard ISO IEC 27001 e le linee guida 27017 e 27018.

L'interessato può esercitare i suoi diritti attraverso l'apposito "Modulo di esercizio diritti in materia di protezione dati personali" pubblicato nella sezione "Privacy" del sito istituzionale www.genegis.it, da inoltrare al referente privacy aziendale tramite mail all'indirizzo privacy@genegis.net Alla richiesta dovrà essere allegata – pena l'irricevibilità della richiesta, copia del documento d'identità del richiedente (a meno che l'istanza non abbia firma digitale del richiedente). Sarà compito del referente privacy interessare il Team Privacy per le decisioni conseguenti.

La richiesta è sempre oggetto di protocollazione, al fine di attribuirvi la data di ricezione utile al calcolo dei termini previsti dalla normativa di cui al paragrafo successivo.

In caso di Data Breach, secondo i requisiti ed i tempi definiti nella lettera di nomina a Responsabile del trattamento, GeneGIS GI Srl provvederà ad informare immediatamente il Titolare del trattamento per le opportune azioni conseguenti.

GeneGIS GI Srl **non rientra nell'obbligo** della nomina di un responsabile a protezione dei dati (DPO – Data Protection Officer) ma le segnalazioni possono essere inviate al Team Privacy istituito contattabile all'indirizzo mail privacy@genegis.net

2.3 Sicurezza dei dati personali e crittografia

GeneGIS GI Srl garantisce l'applicazione di sistemi crittografici nei protocolli di trasmissione delle informazioni A fronte di specifiche esigenze, la società è in grado di fornire un servizio di crittografia dei dati, residenti sui database.