MISURE
DI SICUREZZA
GLE HOLDING S.R.L

(EX ART. 32 G.D.P.R.)

golee

INDICE DEGLI ARGOMENTI

INFORMAZIONI DOCUMENTO

DOCUMENTO	VERSIONE	ULTIMO AGGIORNAMENTO
Misure di Sicurezza 32 GDPR - GLE Holding S.r.l.	2.0	12/03/2024

REDAZIONE E VERIFICA	Avv. Andrea Baldrati
APPROVAZIONE	Marco Morri (Amministratore di Sistema)

ULTIME REVISIONI	
DATA	**DESCRIZIONE**
23.02.2021	Prima versione approvata
20.03.2022	Aggiornamento alla prima versione
24.03.2024	Seconda versione approvata

SCOPO E AMBITO DI APPLICAZIONE

Il presente documento è suddiviso in 7 aree di controllo Cybersecurity e Data Protection allo scopo di ridurre il numero di vulnerabilità presenti nei sistemi e nei processi organizzativi dell'azienda titolare. All'interno di ogni area sono elencati una serie di misure di sicurezza adottate per la specifica realtà aziendale.

FONTI

- *Guidelines for SMEs on the security of personal data processing* - Dicembre 2016 - ENISA
- *2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity* - Marzo 2017 - CIS SAPIENZA Università di Roma;
- *Framework Nazionale per la Cybersecurity e la Data Protection* - Febbraio 2019 - CIS SAPIENZA Università di Roma;
- *Digital Identity Guidelines: Authentication and Lifecycle Management* - Febbraio 2020 - NIST 800-63B
- *Guidelines for Managing the Security of Mobile Devices in the Enterprise* - Marzo 2020 - NIST 800-124

-

1. INVENTARIO DISPOSITIVI, SOFTWARE E DATI

1.1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software in uso all'interno del perimetro aziendale. A questo LINK è possibile consultare un inventario dei dispositivi aziendali.

1.2. I servizi web I servizi web offerti da terze parti (a cui si è registrati) sono quelli strettamente necessari. **Si precisa che, per i servizi con data center in USA, si è verificata la loro presenza all'interno della lista del Data Privacy Framework USA-UE, che certifica la loro conformità per il trasferimento dati extra UE**. Nello specifico la società si serve dei seguenti tool digitali:

Nome Prodotto	Funzione	Data Center
Calendly	Sales - Prenotazioni Call	USA (DPF)
Make / Integromat	Sales - Integrazione tra prodotto e commerciali	Germania
Zapier	Sales - Integrazione tra prodotto e commerciali	USA (DPF)
Hubspot	Sales - CRM commerciale	USA (DPF)
Google Cloud Server	Prodotto - Server in cloud	USA (DPF)
BROWSERLESS	Prodotto - Realizzazione file pdf export e moduli Golee Manager	USA (DPF)
Frill	Prodotto - Raccolta idee clienti e pubblicazione sviluppi	Australia con hosting AWS (DPF)
Stripe	Prodotto - Pagamenti Golee Membership e Golee Pay	USA (DPF)
Twilio	Prodotto - Invio Mail di sistema	USA (DPF)
Brevo	Prodotto - Invio Mail di sistema	Francia con hosting Kinsta Inc. - USA (DPF)
MongoDB	Prodotto - Database	USA (DPF)
Auth0 Prod	Prodotto - Autenticazione Utenti	USA (DPF)
Mixpanel	Prodotto - Analytics	USA (DPF)
Gsuite	Business - suite di Google per mail, storage e operatività interna	USA (DPF)

1.3. L'azienda, anche per mezzo della compilazione di un registro del trattamento (art. 30 GDPR), ha individuato i dati e le informazioni più rilevanti in relazione al proprio business. In tal senso, i trattamenti di dati personali sono identificati e catalogati.

1.4. A seguito di un Risk Assessment effettuato sulla base delle Linee Guida emesse dal WP29 (ora EDPB – European Data Protection Board), e in costante aggiornamento in relazione a nuovi servizi e sviluppi aziendali, la società ha individuato i trattamenti più rischiosi, mettendo in atto adeguate misure tecniche e organizzative.

2. PROTEZIONE DA MALWARE

2.1. Tutti i dispositivi aziendali sono dotati di software di protezione regolarmente aggiornati e disposti su più livelli.

2.2. È pianificata la dismissione dei software che viene gestita direttamente dal Team tecnico di Golee.

2.3. La posta elettronica aziendale è dotata di strumenti antispam/antivirus di adeguata efficacia.

3. FORMAZIONE

3.1. L'azienda ha dato mandato al DPO di organizzare incontri formativi rivolti al personale perché venga adeguatamente sensibilizzato sul corretto trattamento dei dati personali e sulle procedure da adottare per un loro impiego sicuro.

4. PROTEZIONE DEI DATI

4.1. Sulla configurazione iniziale di tutti i dispositivi IT è svolta dai referenti interni di competenza.

4.2. Sono eseguiti back-up giornalieri e incrementali e back-up in cloud.

4.3. I backup del database sono di tipo snapshot e conservati da Mongodb Atlas. Si tratta di uno storage snapshot che non consuma spazio al momento della creazione. È solo una copia dei metadati che contengono informazioni sui dati acquisiti. L'elemento di diversificazione tra uno storage snapshot e un backup è che lo snapshot risiede nella stessa posizione in cui si trovano i dati originali. Pertanto, dipende interamente dall'affidabilità della fonte. Nel caso specifico la fonte è rappresentata da Google Cloud, il quale garantisce - a sua volta - back-up cifrati.

5. PROTEZIONE DELLE RETI

5.1. Le reti e i sistemi sono protetti da accessi esterni non autorizzati attraverso strumenti specifici: firewall (hardware e software); intrusion detection-prevention system.

5.2. Le reti wireless all'interno degli spazi di co-working in cui operano i dipendenti e collaboratori di Golee sono adeguatamente protette e configurate con algoritmo di protezione WPA2 e password complesse.

5.3. L'accesso che viene eseguito tramite Internet è crittografato tramite protocolli crittografici (TLS/SSL)

6. PREVENZIONE E MITIGAZIONE

6.1. In caso di data breach è stato predisposto un apposito registro per annotare violazioni di dati personali trattati. Inoltre, vengono informati l'amministratore di sistema e il DPO per la gestione degli adempimenti necessari in caso di violazioni (messa in sicurezza dei sistemi, annotazione dell'evento su registro data breach, eventuale notifica all'Autorità Garante e/o agli interessati).

6.2. Tutti i software in uso per l'operatività aziendale sono in modalità SaaS e, come tale sono aggiornati dal fornitore con regolarità. Lo stesso vale per l'eventuale dismissione di software obsoleti.

6.3. L'autenticazione ai servizi SaaS avviene tramite misure di protezione Single Sign-on e accesso alle risorse necessarie rispetto alle mansioni del collaboratore e/o dipendente.

7. PRIVACY BY DESIGN SVILUPPO SOFTWARE

7.1. Sono previsti incontri periodici bisettimanali tra il DPO e l'Amministratore di Sistema per analizzare gli sviluppi del software e definire i processi in termini di privacy by design e by default.

7.2. Ogni incontro viene verbalizzato e sono previste le azioni di conformità necessarie ai fini di accountability.