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.	1.1	23/02/2021

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

ULTIME REVISIONI	
DATA	**DESCRIZIONE**
23.02.2021	Prima 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. Nello specifico la società si serve di:

- GSUITE: la suite di Google che contiene SaaS e applicazioni fra cui:
  - Gmail: provider mail; Google Drive e altri servizi utilizzati per la operatività interna
  - Google cloud: intero database piattaforma Golee. Contiene dati e contenuti multimediali relativi a tutti i servizi di Golee.
- AWS: il servizio di cloud hosting di Amazon
- SendGrid: provider mail, i dati sono conservati in UE. Consente la pianificazione di mail automatizzate;
- Bugsnag e Sentry: gestiscono notifiche di errore; contengono indirizzo IP, indirizzi e-mail, nomi utente, identificatori del browser, del sistema operativo e altri dati del terminale);
- Zapier: piattaforma che permette di collegare e integrare fra loro diverse applicazioni e servizi web;
- CloudAMQP: broker di messaggi che funge da intermediario gestendo la comunicazione con un messaggio di protocollo, mentre Google Cloud fa da storage. L'azienda consente di modellare la DPA (Data Protetection Agreement) sulla base delle proprie esigenze, scegliendo solo data center in UE - si veda: https://www.cloudamqp.com/dpa.html;
- CloudMQTT (tools che gestisce la comunicazione - si appoggia su data center di Amazon AWS);
- Cloudfare: Cloudflare, Inc. è una società americana che si occupa di content delivery network, servizi di sicurezza internet e servizi di DNS distribuiti, che si pongono tra i visitatori di un sito e gli hosting provider degli utenti Cloudflare
- SolarWinds - i log (dati del dispositivi e indirizzi IP e dati utente);
- Signrequest: Saas per la sottoscrizione di documenti
- Atlas MongoDb: un database distribuito, document-based che si affianca a quello di Google Cloud;
- Mailchimp è una piattaforma di automazione del marketing e un servizio di email marketing.
- Netfly è una società di cloud computing che offre servizi di hosting e server senza back-end per applicazioni Web e siti Web statitici
- Algolia: motore di ricerca utilizzato all'interno dei servizi Golee.
- Social network (Facebook e Instagram) per la promozione dei propri servizi;
- Sendinblue: Soluzione per il marketing relazionale utilizzato per inviare newsletter
- Hubspot: Software commerciale per il monitoraggio delle trattative e dei clienti già paganti.

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 di LVenture Group S.p.a presso Milano LUISS-HUB 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.