

POLITICA PER LA PRIVACY E PER LA SICUREZZA DELLE INFORMAZIONI

La Direzione di **ReeVo SpA** ha deciso di progettare e rendere operante un **Sistema di Gestione della Privacy e della Sicurezza delle Informazioni** conforme ai requisiti della norma internazionale ISO/IEC 27701 e ISO/IEC 27001, per meglio strutturare i propri processi ed ottimizzare la sua organizzazione al fine di rendere coerenti gli obiettivi di Privacy e di Sicurezza delle Informazioni con le proprie linee strategiche, divenute essenziali e determinanti nel mercato molto particolare e in continua evoluzione in cui ReeVo S.p.A. opera.

Al fine di perseguire i nostri obiettivi di compliance ai requisiti del GDPR abbiamo adottato un sistema di gestione per la privacy conforme allo standard ISO 27701.

Il nostro Sistema di gestione per la Privacy è stato integrato nel più generale sistema di gestione aziendale ed è stato pianificato in modo da considerare aspetti di Governance e di Sistema di Controllo Interno, aspetti di Risk Management (con riferimento alle linee guida dello standard ISO 31000) e aspetti di Compliance (con riferimento alle linee guida dello standard ISO 19600).

Ci impegniamo ad adeguare e a migliorare continuamente il nostro Sistema di Gestione per la Privacy e a sensibilizzare e formare i nostri stakeholders in merito alla sua corretta applicazione.

Tutti coloro che trattano dati per nostro conto sono da noi formati e sensibilizzati in conformità all'articolo 29 del GDPR sulla corretta applicazione della presente politica e delle politiche operative da questa richiamate. Tutti i fornitori che trattano dati personali per nostro conto sono nominati responsabili del trattamento in conformità all'articolo 28 del GDPR.

Per ReeVo S.p.A. la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati personali e non, e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione. Proteggere i dati personali di tutti i nostri interessati al trattamento è per noi fondamentale. Lo stesso impegno lo chiediamo quindi a tutti i nostri stakeholders (fornitori, collaboratori, business partner, consorziati, aziende partecipate e collegate). Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'ISMS, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate, assicurando la resilienza dei trattamenti e il disaster recovery;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta.
4. **Privacy**: in ottemperanza dell'art.24 del "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" ("GDPR").

Per perseguire questi obiettivi di primo livello in obiettivi pianifichiamo obiettivi di secondo livello correlati alla corretta adozione di controlli operativi ("misure tecnico organizzative") applicabili per il trattamento dei rischi. La presente politica può quindi richiamare politiche più operative che indirizzano specifici aspetti di protezione dei dati personali.

Il nostro contesto

1. La nostra mission consiste nell'erogazione di servizi Cloud & Cyber Security alle aziende italiane e pubblica amministrazione, attraverso la rete di Partner qualificati e selezionati sul territorio.

2. Le principali finalità di trattamento consistono nella gestione dei rapporti contrattuali finalizzati all'approvvigionamento di beni e servizi verso fornitori o all'erogazione di servizi verso partner e clienti finali.

3. Trattiamo tipicamente, nell'erogazione del servizio, i dati personali delle seguenti categorie di soggetti interessati:

- Clienti;
- Fornitori e Collaboratori;
- Partecipanti ad eventi;
- Navigatori del sito internet aziendale;
- Aziende consorziate e Business Partners.

I dati sono trattati in modalità cartacea e informatica. I dati personali trattati sono prevalentemente dati anagrafici, dati di contatto, dati professionali, dati organizzativi e dati amministrativi. In alcuni casi possono essere trattati dati inerenti riprese foto e video, soprattutto in occasione di eventi.

4. La base giuridica del trattamento è prevalentemente di natura precontrattuale, contrattuale o cogente.

5. I dati sono trattati nell'ambito dell'Unione Europea.

6. I criteri di conservazione dei dati sono prevalentemente riferiti a requisiti di natura contrattuale o cogente. I dati possono essere inoltre conservati per ragioni storiche o per ragioni tecniche (nel caso in cui l'eliminazione dei dati potrebbe compromettere l'integrità e la fruibilità degli archivi). In tal caso i dati archiviati non sono oggetto di ulteriore trattamento.

7. Per ogni categoria di soggetti interessati al trattamento predisponiamo informative in conformità all'articolo 13 del GDPR. Dove necessario provvediamo a rilevare il consenso al trattamento in conformità dell'articolo 7 del GDPR.

La nostra accountability ai principi del GDPR e la valutazione dei rischi

Adottiamo un modello di gestione per assicurare la conformità ("compliance") ai requisiti del GDPR. Tale modello si basa sullo standard ISO 27701 Personal Information Management System (PIMS).

Il modello di gestione per la protezione dei dati personali include il framework per la gestione dei rischi per la protezione dei dati personali basato sulle linee guida dello standard ISO 31000.

Le sanzioni

Le violazioni della presente politica e del sistema di gestione per la privacy da questa richiamato implicano l'applicazione di provvedimenti disciplinari, inclusa la risoluzione di rapporti contrattuali in essere ed il decadimento della qualifica di consorziato.

I nostri canali di comunicazione

La versione aggiornata di questo documento così come l'informativa agli interessati sono disponibili sul sito internet www.reevo.it.

Per ogni richiesta di informazione, di esercizio dei diritti di cui all'art.13 del GDPR, di segnalazione di vulnerabilità, di violazioni dei principi per il trattamento dei dati, di incidenti puoi contattare il nostro privacy manager all'indirizzo di posta elettronica simone.brun@sole-consulting.com.

I nostri principi

La politica della sicurezza delle informazioni di ReeVo S.p.A. si ispira ai seguenti principi:

a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.

b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.

c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.

d. Garantire la sicurezza fisica e logica degli information asset e degli asset operativi.

e. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.

f. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.

g. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

I nostri obiettivi

Nell'ambito della gestione dei servizi offerti ReeVo S.p.A. assicura:

- assicurare ai nostri clienti e a tutti i nostri stakeholders la massima protezione dei loro beni, inclusi i loro dati personali.
- il miglioramento continuo della sicurezza delle informazioni, reale e percepita, dei propri prodotti/servizi, attraverso il miglioramento tecnologico dell'esistente e con un metodo di lavoro predisposto alla ricerca ed innovazione continua
- la soddisfazione dei requisiti impliciti ed espliciti del cliente
- la completa osservanza delle Service Level Agreement stabilite con i clienti
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza
- la garanzia di affidare a partner affidabili e qualificati il trattamento del proprio patrimonio informativo
- l'impegno a trattare i dati personali degli interessati in conformità ai principi richiamati dall'Articolo 5 del GDPR e di seguito riportati:

- liceità, correttezza e trasparenza dei trattamenti;
- finalità determinate, esplicite, legittime;
- dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- dati esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- dati conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi esclusivamente a fini di archiviazione e previa l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- dati trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

La politica della privacy e sicurezza delle informazioni è formalizzata nell'ISMS, viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema intranet e specifici canali di comunicazione.

Brugherio, 01 03 2021

La Direzione ReeVo S.p.A.

Indice delle revisioni

<i>Data</i>	<i>Rev.</i>	<i>Descrizione delle revisioni</i>	<i>Categoria</i>
01 03 21	00	Prima emissione	Usò Pubblico