Data Protection & Retention Policy

Criteri e tempi di conservazione dei dati personali

IMS_MPO_001-1.0 Data Protection & Retetion Policy

SOMMARIO

1 Obiettivo

Sorint.Sec necessita di raccogliere dati personali per svolgere in modo efficace le proprie funzioni e attività quotidiane e per fornire i prodotti e i servizi definiti dal proprio tipo di attività. Tali dati vengono trattati da dipendenti e includono, nella maggior parte dei casi e facendo riferimento al Servizio di Security Operation Center, dati di contatto (nome, indirizzo, indirizzo e-mail, , indirizzo IP, geolocalizzazione)
Inoltre, potremmo essere tenuti a raccogliere e utilizzare determinati tipi di dati personali per ottemperare ai requisiti di legge e/o normativi, tuttavia ci impegniamo a trattare tutti i dati personali in conformità con il Regolamento generale sulla protezione dei dati (GDPR) e qualsiasi altra legge e codice di condotta in materia di protezione dei dati (di seguito collettivamente denominati “le leggi sulla protezione dei dati”).
Sorint.Sec ha sviluppato politiche, procedure, controlli e misure per garantire la massima e continua conformità alle leggi e ai principi sulla protezione dei dati, tra cui la formazione del personale, i documenti procedurali, le misure di audit e le valutazioni.
Garantire e mantenere la sicurezza e la riservatezza dei dati personali è una delle nostre priorità principali e siamo orgogliosi di adottare un approccio “Privacy by Design”, valutando i cambiamenti e il loro impatto fin dall'inizio e progettando sistemi e processi per proteggere le informazioni personali al centro del nostro lavoro.

2 Scopo

Lo scopo della presente politica è garantire che Sorint.Sec soddisfi i requisiti legali, statutari e normativi previsti dalle leggi sulla protezione dei dati e assicurare che tutte le informazioni personali e di categoria speciale siano trattate in modo conforme e nel migliore interesse degli individui.
Le leggi sulla protezione dei dati includono disposizioni che promuovono la responsabilità e la governance e, pertanto, Sorint.Sec ha messo in atto misure di governance complete ed efficaci per soddisfare tali disposizioni.
Lo scopo di tali misure è quello di ridurre al minimo il rischio di violazioni e garantire la protezione dei dati personali. La presente politica funge anche da documento di riferimento per i dipendenti e le terze parti in merito alle responsabilità relative al trattamento e all'accesso dei dati personali e alle richieste degli interessati.

3 Riferimenti Normativi

3.1.1 Documenti Applicativi

Per la consultazione dei documenti applicativi, fare riferimento al Registro di prescrizioni legali e prendere visione della documentazione di supporto relativa alla norma ISO/IEC 27001:2022.

3.1.2 Documenti di riferimento

Per la consultazione dei documenti di riferimento, fare riferimento al Registro di prescrizioni legali e prendere visione della documentazione correlata alla norma ISO/IEC 27001:2022.

4 Campo di applicazione

La presente politica si applica a tutto il personale di Sorint.Sec e riguarda il trattamento dei dati personali. Il rispetto della presente politica è obbligatorio e la sua violazione può comportare provvedimenti disciplinari.

5 General data protection regulation - GDPR

Il regolamento UE 2016-679 sulla protezione dei dati personali, noto con l'acronimo “GDPR – Regolamento generale sulla protezione dei dati”, ha introdotto alcuni aspetti innovativi rispetto alla normativa precedente (Direttiva 95/46 CE, Decreto Legislativo n. 196/2003) che ha richiesto a Sorint.Sec di attivare specifiche azioni di revisione delle proprie politiche e procedure interne per affrontare il tema della “compliance” in materia di protezione dei dati, in una prospettiva nazionale e internazionale, al fine di tutelare i diritti degli interessati, consolidare le basi giuridiche per la liceità del trattamento dei dati personali effettuato nell'ambito delle proprie attività e ridurre e mitigare entro livelli accettabili l'esposizione al rischio di violazioni e relative sanzioni.
Attraverso il sistema di procedure e politiche esistenti, Sorint.Sec intende garantire la conformità al GDPR e alle altre normative correlate.

6 Termini e definizioni

Data Breach	Una violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso accidentale o illecito a dati personali trasmessi, conservati o trattati in altro modo.
Titolare del trattamento	Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il responsabile del trattamento o i criteri specifici per la sua nomina possono essere previsti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento	Persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che tratta dati personali per conto del titolare del trattamento.
Dati personali	Qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più fattori specifici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Terza parte	Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un organismo diverso dall'interessato, sotto la nostra diretta autorità.
Consenso	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con cui l'interessato, mediante una dichiarazione o un'azione positiva inequivocabile, manifesta il proprio assenso al trattamento dei dati personali che lo riguardano; Inoltre, il "consenso" dovrebbe essere espresso mediante un atto affermativo chiaro che costituisca un'indicazione libera, specifica, informata e inequivocabile dell'accordo dell'interessato al trattamento dei dati personali che lo riguardano, ad esempio mediante una dichiarazione scritta, anche con mezzi elettronici, o una dichiarazione orale.

7 Dati trattati da Sorint.Sec

Nell'ambito dell'erogazione dei nostri servizi di cybersecurity, principalmente nel Servizio SOC (Security Operation Center), Sorint.Sec tratta dati di contatto e informazioni di geolocalizzazione.
Facendo sempre riferimento al Servizio sopra indicato, Sorint.Sec tratta i dati personali per i seguenti scopi:

- Raccolta dei dati sul Siem, sul tool di Ticketing e sulla Share Aziendale (con accesso secondo i principi "Need To Know" e "Least Privilege")
- Conservazione sul tool di Ticketing e sulla share aziendale (con accesso secondo i principi "Need To Know" e "Least Privilege")
- Utilizzo e consultazione,
- Cancellazione.

Tali dati vengono raccolti e utilizzati esclusivamente per finalità legate alla fornitura dei servizi richiesti, nel rispetto dei principi di liceità, correttezza e trasparenza. La conservazione è disciplinata dal paragrafo di *data retention* conforme allo standard ISO/IEC 27001 e alle normative vigenti, che stabilisce tempi e modalità di archiviazione e cancellazione sicura. L'accesso ai dati è limitato al personale autorizzato e protetto da misure tecniche e organizzative adeguate, al fine di garantire riservatezza, integrità e disponibilità delle informazioni.

8 Privacy by design

Sorint.Sec adotta il principio di *Privacy by Design*, integrando la protezione dei dati personali in ogni fase di progettazione e sviluppo di tecnologie, processi e servizi. Ci impegniamo a garantire che le impostazioni predefinite siano orientate alla tutela della riservatezza, che vengano raccolti solo i dati strettamente necessari e che siano implementate misure tecniche e organizzative adeguate per prevenire rischi e garantire sicurezza. Ogni nuovo progetto è sottoposto a valutazioni d'impatto sulla protezione dei dati, e la policy viene periodicamente aggiornata per assicurare conformità alle normative vigenti e trasparenza verso gli interessati.

Considerando lo stato dell'arte delle tecnologie, i costi e l'impatto dell'implementazione, l'ambito, il contesto e la finalità del trattamento in atto, l'impatto e la probabilità di un determinato rischio, Sorint.Sec deve valutare l'adozione di tecniche quali la minimizzazione dei dati e la crittografia, ove opportuno, in conformità con le disposizioni dell'art. 32 del GDPR.

9 Data Retention

I dati personali gestiti da Sorint.Sec saranno disponibili per il tempo strettamente necessario alle finalità del trattamento.
A titolo esemplificativo e senza pretese di esaustività, si riporta di seguito una tabella riassuntiva delle categorie dei soggetti più significativi trattati dalla società e della relativa durata dei trattamenti, con l'aggiunta dei principali riferimenti normativi.

Categoria di dato	Finalità del trattamento	Periodo di conservazione	Note/Normative di riferimento
Dati anagrafici cliente e contrattuali	Gestione contrattuale e fatturazione	10 anni	Obblighi fiscali
Candidati e curriculum vitae	Selezione del personale	24 mesi	Informativa candidati interna
Ticket	Erogazione del servizio	1 anno	Policy
Dati dipendenti	Gestione rapporto lavorativo	5 anni dalla cessazione	Normativa lavoro
Dati di contatto	Assistenza clienti	Tempo strettamente necessario (Massimo 24 mesi dopo la cessazione)	GDPR
Dati di geolocalizzazione	Sicurezza e protezione	Tempo strettamente necessario all'erogazione del servizio	GDPR
Log di accesso amministrativo (cliente)	Sicurezza informatica	6 - 12 mesi max	Best practice di sicurezza
Log di accesso dipendenti (IT,VPN)	Sicurezza informatica	6-12 mesi max	GDPR
Log di sicurezza (firewall/IPS)	Sicurezza informatica	6 – 12 mesi max	Best practice di sicurezza
Metadati della Mail	Sicurezza informatica	30 giorni	GDPR

10 Sicurezza delle informazioni e integrità dei dati

Sorint.Sec ha adottato misure tecniche e organizzative idonee a proteggere i dati personali da fatti accidentali o illeciti che ne provochino la distruzione, perdita, alterazione, e da uso, rivelazione o accesso non autorizzati, in special modo dove il trattamento prevede la trasmissione di dati tramite una rete e contro qualsiasi altra forma di trattamento illecito e abuso.

11 Notifica della violazione dei dati

È politica dell'azienda agire in modo equo e proporzionato nel valutare le misure da adottare per informare gli stakeholder in merito alla violazione dei dati personali. In linea con il GDPR, in caso di violazione che potrebbe comportare un rischio per i diritti e le libertà delle persone, l'autorità responsabile della protezione dei dati sarà informata entro 72 ore.
Le procedure operative e i dettagli per la gestione della violazione dei dati sono documentati in una procedura operativa specifica.

12 Trasferimento Dati Personali

Qualsiasi trasferimento di dati personali al di fuori dell'Unione Europea deve essere attentamente esaminato prima della sua autorizzazione e attuazione, al fine di garantire che l'azienda operi entro i limiti imposti dal GDPR. Ciò dipende anche dalla valutazione della Commissione Europea sull'adeguatezza delle garanzie per i dati personali applicabili nel paese ospitante, una valutazione soggetta ad aggiornamenti e per la quale è necessario consultare la pagina istituzionale.
Nel caso in cui sia necessario per scopi legittimi o per il legittimo interesse dell'azienda trasferire i dati, devono essere messe in atto misure di salvaguardia adeguate a seguito dell'analisi, in conformità con le disposizioni del capitolo V, art. 44-50 del GDPR.

13 Ruoli e responsabilità per la protezione dei dati

In ambito di protezione e conservazione dei dati personali, Sorint.Sec definisce ruoli e responsabilità chiari e distinti.

1. Titolare del trattamento (Cliente):

    - Garantire la conformità al GDPR,
    - Raccogliere consensi se necessari,
    - Adottare misure di sicurezza.

2. Responsabile del trattamento (Sorint.Sec):

    - Tratta i dati per conto del titolare, seguendo istruzioni documentate.
    - Deve garantire sicurezza, supportare nelle notifiche di violazioni e rispettare i tempi di retention stabiliti nei contratti

3. Data Protection Officer – DPO (Sorint.Lab – Rossella Piazzalunga):

    - Figura indipendente prevista dall’art. 37 GDPR.
    - Sorveglia l’applicazione della normativa, fornisce consulenza, funge da punto di contatto con il Garante.
    - Ha compiti di monitoraggio, formazione e audit interni

14 GDPR COMPLIANCE

Sorint.Sec, al fine di garantire la conformità al GDPR, ha implementato le seguenti azioni:

- La base giuridica per il trattamento dei dati personali è chiara e inequivocabile ed è tracciata nel registro dei trattamenti ex art. 30 GDPR tenuto dall'azienda su base volontaria;
- Tutto il personale coinvolto nella gestione dei dati personali comprende le proprie responsabilità in materia di buone pratiche di protezione dei dati;
- Tutto il personale è adeguatamente informato in merito alla protezione dei dati personali adottata da Sorint.Sec;
- Sono definiti e accessibili specifici processi aziendali che consentono agli interessati di esercitare in piena trasparenza i propri diritti in materia di dati personali;
- L'approccio “Privacy by Design” è adottato per ogni implementazione di servizi, sistemi e processi nuovi o modificati ed è documentato nel contesto delle licenze d'uso delle applicazioni utilizzate dall'azienda e/o dai suoi fornitori e outsourcer;
- La documentazione delle attività di trattamento è registrata nel registro dei trattamenti.

Tali azioni sono svolte da Sorint.Sec con il supporto e sotto il coordinamento del CISO, che a sua volta si avvale del supporto della funzione IT.
Nell'ambito dei controlli relativi all'adeguatezza e all'affidabilità delle misure di sicurezza dei sistemi informativi prescritte dalla normativa di settore, la funzione di internal audit verifica a intervalli regolari i principi di protezione dell'accesso ai dati dei Clienti e l'effettiva attivazione delle procedure di Data Breach in caso di violazioni della sicurezza rilevanti.

15 INFORMATION DELETION

Per le tempistiche e le modalità previste per la cancellazione sicura dei dati archiviati, si rinvia alla Disposal of Asset Procedure.

DOCUMENT INFORMATION

COPYRIGHT

Sorint.SEC S.r.l. Società 51% Controllata da Sorint.Lab S.p.A.
Sede Legale: Via Zanica, 17 – 24050 Grassobbio (Bg), Italy
Sede Operativa: Via Dell'Artigianato – Osio Sotto, 24046 (Bergamo), Italy
COD. FISC., N. REG. IMPR. BG 04010360164, PI 04010360164
CAP. SOC. € 10.000,00 i.v. REA BG 427668

Legale Rappresentante e Amministratore Unico: Luca Pedrazzini
Società Soggetta a Direzione e Coordinamento di Sorint.Lab S.P.A.
Phone: +39 035 0510401
https://sorintsec.ai