

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E PER LA QUALITA'

Il Sistema di Gestione Integrato (SGI) per la Sicurezza delle Informazioni e per la Qualità, è lo strumento con il quale Il Dato Srl intende, tramite processi in Qualità, proteggere la riservatezza, l'integrità e la disponibilità del proprio patrimonio informativo ivi incluso le informazioni dei clienti gestite.

Il raggiungimento di adeguati livelli di qualità e di sicurezza nei processi aziendali, consente a Il Dato di mitigare e contrastare perdite e danneggiamenti che possano avere impatto sulle persone, sull'immagine e la reputazione aziendali, sugli aspetti di natura economica e finanziaria, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di protezione delle informazioni e dei dati personali. In tale ambito, Il Dato declina operativamente tali principi attraverso i seguenti obiettivi:

a) In merito alla sicurezza delle informazioni

- adottare ed implementare principi e best practice riconosciuti per garantire la Sicurezza delle Informazioni e promuovere l'acquisizione di certificazioni di conformità agli standard di riferimento;
- stabilire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in conformità alla norma ISO/IEC 27001:2022, per garantire e proteggere le informazioni proprie, dei propri clienti e di tutti i soggetti interessati di cui si gestiscono informazioni di diversa natura, da eventuali minacce, mediante un costante processo di valutazione del rischio;
- estendere il Sistema di Gestione per la Sicurezza delle Informazioni alle attività in Cloud in conformità con le norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019, avendo cura di garantire la loro costante ottemperanza;
- garantire il corretto accesso alle giuste informazioni quando necessario e prevenire l'accesso non autorizzato, sia da parte di chi opera in Il Dato Srl, sia di chi opera per suo conto;
- individuare ruoli e responsabilità, da assegnarsi al proprio organico, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave;
- assegnare le risorse necessarie al fine di assicurare l'impiego di misure idonee per gli aspetti riguardanti la sicurezza fisica, logica ed organizzativa;
- promuovere continuamente il Sistema di Gestione per la Sicurezza delle Informazioni, anche mediante un impegno costante degli Organi e dei Soggetti apicali;
- individuare, documentare ed applicare regole che disciplinano le modalità di utilizzo delle informazioni, dei beni e degli strumenti;
- supportare il personale e i collaboratori aziendali con un'adeguata istruzione e formazione per sensibilizzare in materia di sicurezza informatica al fine di minimizzare i rischi;
- predisporre adeguate misure di reazione e gestione a fronte del verificarsi di incidenti che possono compromettere la sicurezza delle informazioni e la normale operatività;
- garantire la continuità della sicurezza delle informazioni in caso di scenario sfavorevole o qualora si concretizzi una minaccia;
- ridurre quanto più possibile malfunzionamenti dei sistemi di sviluppo e produzione causati da diffusioni di malware, software o codice dannoso;

- tenere costantemente sotto controllo la gestione della capacity nell'ambiente di produzione per evitare che un suo eventuale sovraccarico causi il collasso dei sistemi, causando interruzioni lavorative e downtime non pianificati;
- assicurare che venga eseguito il corretto processo di gestione (riciclo o dismissione) di materiale informativo digitale, contenente dati aziendali, al fine di evitare la perdita di dati e informazioni sensibili;
- mantenere l'osservanza delle disposizioni contrattuali, legislative e regolamentari, in particolare sulla protezione delle informazioni;
- garantire la idonea custodia delle informazioni Personali di terzi e loro gestione secondo principi di liceità, proporzionalità e pertinenza;
- impegnarsi a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione per la Sicurezza delle Informazioni, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti al contrasto di potenziali eventi che possano compromettere il patrimonio informativo aziendale.

b) In merito alla Qualità

- Adottare ed implementare i principi e le buone pratiche riconosciute per garantire la Qualità dei processi aziendali, dei servizi erogati e promuovere l'acquisizione di certificazioni di conformità agli standard di riferimento.
- Stabilire un Sistema di Gestione Integrato garantendo la conformità ai requisiti ISO 9001:2015, per garantire il diritto dei clienti al miglior servizio possibile basato su processi di qualità.
- Individuare ruoli e responsabilità, da assegnarsi al proprio organico, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave.
- Assegnare le risorse necessarie al fine di assicurare l'impiego di misure idonee per gli aspetti riguardanti la qualità dei processi interni e dei servizi alla clientela.
- Promuovere continuamente il Sistema di Gestione Integrato, anche mediante un impegno costante degli Organi e dei Soggetti apicali.
- Individuare, documentare ed applicare regole che disciplinano le modalità di erogazione dei servizi secondo principi etici e di costante miglioramento.
- Sviluppare un programma di consapevolezza per il personale, mediante sessioni informative e formative periodiche.
- Predisporre adeguate misure di reazione e gestione a fronte del verificarsi di eventi che possono compromettere la qualità dei processi aziendali e della qualità dei servizi offerti alla clientela.
- Mantenere l'osservanza delle disposizioni contrattuali, legislative e regolamentari sia nei processi interni che nelle attività per i clienti.
- Selezionare e promuovere lo sviluppo dei fornitori secondo i principi di questa politica impegnandoli a mantenere comportamenti coerenti con essi.
- Impegnarsi a svolgere un processo continuo di miglioramento ed evoluzione del Sistema di Gestione Integrato, pianificando, eseguendo, verificando e attuando con continuità misure ed accorgimenti atti al contrasto di potenziali eventi che possano compromettere la Qualità nei processi e servizi alla clientela.

Cloud Service Provider

Il Dato S.r.l. si configura come Cloud Service Provider (CSP), dal momento che eroga i servizi per la *“Commercializzazione, Erogazione, Gestione, manutenzione e assistenza di servizi software, anche in modalità Cloud SaaS”* per i propri clienti. Il Dato non si qualifica come Cloud Service Customer (CSC) secondo la norma ISO/IEC 27017, in quanto utilizza esclusivamente un servizio di colocation standard offerto da un CSP globale, come Aruba. La colocation non rientra nel perimetro dei servizi cloud così come definiti dalla norma (IaaS, PaaS, SaaS), poiché si tratta di un semplice affitto di spazio fisico e connettività, senza la fornitura di risorse virtualizzate o scalabili on-demand. Pertanto, inquadrare l'organizzazione come CSC risulterebbe improprio e superfluo, poiché non usufruisce direttamente di servizi cloud gestiti, né personalizza o amministra infrastrutture cloud fornite dal CSP.

Nell'erogazione dei servizi SaaS, Il Dato Srl:

- ha valutato i requisiti di qualità e di sicurezza di base applicabile nella progettazione ed implementazione dei servizi cloud;
- Nell'erogazione dei servizi SaaS verso i propri clienti sono valutati tutti i rischi relativi alla sicurezza delle informazioni all'interno del ciclo annuale di valutazione dei rischi rientranti all'interno del sistema di gestione ISO/IEC 27001;
- ha valutato il rischio derivante dall'operato del suo personale interno nella gestione delle informazioni dei clienti elaborate in Cloud;
- ha garantito che il cliente possa accedere solo ai dati di appartenenza e non abbia nessuna possibilità di accedere fisicamente alle macchine ove sono trattati i dati; per eventuali richieste inerenti ai suoi dati può contattare l'Organizzazione attraverso le modalità di comunicazione formalizzate in sede contrattuale;
- ha garantito che il sistema di virtualizzazione sia sicuro, secondo quanto previsto dalle best practice di mercato;
- permette al cliente, secondo specifiche modalità di autenticazione, di accedere ai dati caricati all'interno del servizio erogato in SaaS garantendo la segregazione delle informazioni tra Clienti;
- garantisce un ciclo di vita delle credenziali degli utenti che usufruiscono del servizio SaaS prontamente eliminando eventuali accessi non più necessari (es. per mancata sottoscrizione del contratto).
- garantisce che eventuali data breach che possono verificarsi, coinvolgendo eventualmente dati personali, sono prontamente gestiti e che è definito un protocollo di segnalazione dell'evento all'autorità competenti;
- ha una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni. Il Cliente deve verificare se l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni è adeguata e deve assicurarsi che soddisfi i propri requisiti. In caso di incidente che coinvolga la perdita di una o più caratteristiche tra Riservatezza, Integrità, Disponibilità, Autenticità riguardanti informazioni personali (Data Protection), è compito della Parte che identifica l'incidente dare immediata informazione all'altra Parte.

PII Processor

- garantisce che eventuali data breach siano prontamente gestiti attraverso un'apposita procedura di segnalazione dell'evento all'autorità competenti;
- ha formalizzato una specifica procedura per la gestione degli incidenti di sicurezza delle informazioni. Il Cliente di Il Dato S.r.l. ha l'obbligo verificare che l'assegnazione delle responsabilità

per la gestione degli incidenti di sicurezza delle informazioni sia adeguata e, pertanto, soddisfi i propri requisiti;

- garantisce che il Management concentri tutti i suoi sforzi sulla protezione continua e sulla segregazione dei dati personali dei clienti, trattati attraverso i servizi cloud proprietari, nel pieno rispetto della normativa vigente;
- si assicura che in caso di incidente che comporti la perdita di una o più delle seguenti caratteristiche delle informazioni personali (PII): riservatezza, integrità, disponibilità e autenticità, l'evento venga prontamente notificato alla parte interessata.

Qualora necessario, e comunque entro un massimo di 48 ore, Il Dato S.r.l. intende decidere congiuntamente quale Parte debba essere responsabile della segnalazione del Data Breach. La comunicazione al Garante della Privacy, come previsto dal Regolamento UE 2016/679 – GDPR, dovrà essere inviata entro 72 ore dalla presa di consapevolezza dell'accaduto.

Per ulteriori approfondimenti circa le misure tecniche ed organizzative, adottate da Il Dato S.r.l., per garantire la sicurezza delle informazioni e dei dati personali all'interno dei servizi Cloud proprietari, prendere evidenza di "Allegato tecnico dei servizi Saas".

Sistema di Gestione Integrato per la Sicurezza delle Informazioni e per la Qualità - SGI

Il SGI comprende tutte le politiche e le procedure messe in atto per il raggiungimento degli obiettivi della sicurezza delle informazioni e della qualità.

L'ambito dell'SGI comprende tutte le attività e i processi riguardanti le attività operative erogate a beneficio dei clienti e quelle di supporto.

L'osservanza della presente politica sulla sicurezza delle informazioni e la qualità è obbligatoria per tutti i dipendenti, collaboratori, fornitori, appaltatori, partner e parti esterne che gestiscono informazioni di Il Dato o dei suoi clienti. La Direzione di Il Dato Srl è direttamente responsabile dell'attuazione della politica e dell'osservanza della stessa da parte di tutte le parti interessate.

La Direzione condivide i principi e gli obiettivi dell'SGI e ne sostiene pienamente la realizzazione e il mantenimento, fornendo le risorse necessarie a tale scopo.

Con l'obiettivo della massima trasparenza e collaborazione la presente politica per la sicurezza delle informazioni è comunicata a tutti i dipendenti e resa disponibile a tutte le parti interessate per quanto ritenuto necessario.

La presente politica è soggetta a revisioni su base periodica e/o in caso di cambiamenti significativi riguardanti la sicurezza delle informazioni, al fine di garantirne l'idoneità, l'adeguatezza e l'efficienza.

Bergamo, 25 luglio 2025

La Direzione
Il Dato S.r.l.
Via Mazzini, 200 - 24021 ARBINO (BG)
Tel. 035/0492869 - e-mail: info@ildato.it
C.F. / P. IVA 02339360162

