# SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

# DATA VISION S.R.L.

# Politica di Sicurezza dei Dati

*La presente politica costituisce una delle politiche di sicurezza informatica per l'ambito "I) Sicurezza dei dati", richiesto dalla Determinazione ACN n. 164179/2025, Allegato 1, in attuazione della misura GV.PO-01. Documento derivato dal documento 02DI – DOPOL rev. 1.3 (Ott 2025), scorporato in due politiche distinte (Qualità / Sicurezza delle Informazioni) in data Giugno 2026.*

| |
|---|
| **Codice DOC**: 02DI-SI_POL-012 |
| **Livello di riservatezza 0 - Pubblico**<br>Informazioni di pubblico accesso. |
| Dati pubblicati su internet o destinati alla pubblica diffusione. |

| Revisione | Data di revisione | Redatta da | Verificata da | Approvata |
|---|---|---|---|---|
| Rilascio 1.0<br>**Prima emissione** del documento autonomo POL-SD, a seguito dello scorporo del documento 02DI – DOPOL "Documento Politica per la Qualità e per la Sicurezza" (rev. 1.3, ottobre 2025) in due politiche distinte: la Politica per la Qualità (ISO 9001:2015, codice POL-Q) e la presente Politica di Sicurezza dei Dati (ISO/IEC 27001:2022 – NIS2). | Ottobre 2026 | CSM / Resp. Gestione Rischi Elena Amendola | Resp. SGSI Daniel Bizzarro | Direzione DV / PdC NIS2 / Referente CSIRT Valerio Bizzarro |

| |
|---|
| **Lista di distribuzione:** Pubblicazione su sito web aziendale |
| **A:** |
| Al personale Data Vision |

| **Cronologia delle revisioni** | | | | |
|---|---|---|---|---|
| **Revisione** | **Data di revisione** | **Redatta da** | **Verificata da** | **Approvata** |
| | | | | |

# SOMMARIO

1. Scopo e campo di applicazione ....4
2. Terminologia ed abbreviazioni ....5
3. Impegno della Direzione....6
4. Politica di Sicurezza dei Dati ....6
4.1. Dichiarazione di intenti....6
4.2. Protezione dei dati a riposo (data-at-rest) ....7
4.3. Protezione dei dati in transito (data-in-transit)....7
4.4. Backup dei dati ....7
4.5. Approccio basato sul rischio ....8
4.6. Diffusione, conformità e processo disciplinare ....8
4.7. Obiettivi per la Sicurezza dei Dati ....8
5. Ruoli e responsabilità ....9
5.1. Punto di Contatto NIS2 / Referente CSIRT (Valerio Bizzarro)....9
5.2. Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni – RSGSI (Daniel Bizzarro) ....9
5.3. CSM / Responsabile Gestione Rischi (Elena Amendola)....9
5.4. Amministratore Sistemi / Responsabile BC-DR (Luca Urbinati) .... 10
6. Riferimenti normativi .... 10
7. Revisione.... 10

## 1. SCOPO E CAMPO DI APPLICAZIONE

Data Vision S.r.l. ha adottato un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) con l'obiettivo di garantire i requisiti sulla sicurezza delle informazioni secondo la normativa UNI CEI ISO/IEC 27001:2022, per la quale Data Vision ha ottenuto la corrispondente certificazione.

Dal 12 aprile 2025, con Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, Data Vision S.r.l. è stata inserita nell'elenco dei soggetti NIS ai sensi dell'articolo 7, comma 3, lettera a) del Decreto legislativo 4 settembre 2024, n. 138, ed individuata quale soggetto Importante.

Ai sensi della misura GV.PO-01 ("La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata") dell'Allegato 1 – "Misure di sicurezza di base per i soggetti importanti" della Determinazione ACN n. 164179/2025, Data Vision adotta e documenta politiche di sicurezza informatica per i sedici ambiti ivi individuati. Il presente documento costituisce la politica relativa all'ambito l) "Sicurezza dei dati", ed è complementare e allineato alla più ampia Politica per la Sicurezza delle Informazioni e alla Politica per la gestione del rischio di cybersecurity di Data Vision.

Il presente documento viene redatto quale supporto agli indirizzi strategici della Direzione, riesaminato almeno annualmente nel riesame periodico della Direzione, ed è reso disponibile a tutto il personale di Data Vision, alle parti interessate e ai fornitori, via e-mail e tramite pubblicazione sul sito web aziendale.

Scopo del presente documento è descrivere la Politica di Sicurezza dei Dati in modo tale che essa:

- risulti appropriata alle finalità e al contesto dell'organizzazione e che supporti i suoi indirizzi strategici in materia di cybersecurity;
- costituisca un quadro di riferimento vincolante per la protezione dei dati gestiti dall'organizzazione, in tutte le loro forme;
- comprenda l'impegno a soddisfare i requisiti applicabili delle norme UNI CEI ISO/IEC 27001:2022 e della Determinazione ACN n. 164179/2025, in particolare le misure PR.DS-01, PR.DS-02 e PR.DS-11;
- comprenda l'impegno per il miglioramento continuo del SGSI-DV così come concepito ed adottato dalla Direzione;
- sia disponibile e mantenuta come informazione documentata, comunicata, compresa e applicata all'interno dell'organizzazione, e disponibile alle parti interessate per quanto appropriato.

La presente Politica di Sicurezza dei Dati si applica a tutti i dati digitali trattati da Data Vision nell'ambito dei propri sistemi informativi e di rete rilevanti, in qualunque stato essi si trovino, e in particolare:

- ai dati a riposo (data-at-rest), ovunque memorizzati, ivi inclusi dispositivi portatili (laptop, smartphone, tablet) e supporti rimovibili;

- ai dati in transito (data-in-transit), ivi incluse le comunicazioni vocali, video e testuali, scambiate da e verso l'esterno del perimetro di Data Vision;
- ai dati oggetto di backup, ivi incluse le configurazioni dei sistemi informativi e di rete rilevanti.

La presente politica si applica ai processi e alle attività di progettazione, implementazione e gestione di sistemi informativi, di sviluppo e fornitura di hardware e software, e alle attività di gestione delle infrastrutture correlate all'erogazione dei servizi e al trattamento delle informazioni. Ogni piano e procedura inerente il trattamento dei dati deve uniformarsi alla presente politica.

## 2. TERMINOLOGIA ED ABBREVIAZIONI

Nell'ambito delle attività e dei documenti inerenti il SGSI si applica la terminologia definita nella norma UNI CEI ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni, nonché la terminologia adottata nel Framework Nazionale per la Cybersecurity e la Data Protection (FNCS) richiamato dalla Determinazione ACN n. 164179/2025.

**DD:** Direzione Data Vision, la più alta funzione aziendale con potere decisionale; ai fini NIS2, è il soggetto cui è in ultima istanza riconducibile la responsabilità della sicurezza informatica, in assenza di una figura CISO dedicata.

**SGSI:** Sistema di Gestione per la Sicurezza delle Informazioni di Data Vision.

**PdC NIS2 / Referente CSIRT:** punto di contatto NIS2 e referente verso il CSIRT Italia (Valerio Bizzarro), responsabile della gestione degli incidenti e dei rapporti con l'Agenzia per la Cybersicurezza Nazionale.

**RSGSI:** Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (Daniel Bizzarro), responsabile della redazione, aggiornamento e diffusione delle politiche di sicurezza informatica, ivi inclusa la presente.

**CSM / Responsabile Gestione Rischi:** funzione aziendale (Elena Amendola) responsabile della valutazione e gestione dei rischi di cybersecurity, ivi inclusi quelli relativi alla sicurezza dei dati a riposo, in transito e di backup.

**Amministratore Sistemi / Responsabile BC-DR:** funzione aziendale (Luca Urbinati) responsabile dell'attuazione tecnica delle misure di cifratura, backup, ripristino e continuità operativa di cui alla presente politica.

**Dati a riposo (data-at-rest):** dati memorizzati su dispositivi, supporti o sistemi di archiviazione, non in fase di trasmissione o elaborazione attiva.

**Dati in transito (data-in-transit):** dati durante la trasmissione tra sistemi, reti o dispositivi, ivi incluse le comunicazioni vocali, video e testuali.

**Sistemi informativi e di rete rilevanti:** i sistemi individuati da Data Vision, ai sensi della misura GV.OC-04, quali rilevanti ai fini dell'erogazione dei servizi e oggetto prioritario delle misure di sicurezza di base.

## 3. IMPEGNO DELLA DIREZIONE

È obiettivo di assoluta priorità della Direzione salvaguardare la sicurezza del proprio sistema informativo e tutelare la riservatezza, l'integrità e la disponibilità dei dati prodotti, raccolti o comunque trattati, da ogni minaccia intenzionale o accidentale, interna o esterna, sia essa relativa a dati a riposo, in transito o oggetto di backup.

Affinché vengano eseguite le attività per la predisposizione, l'attuazione ed il continuo miglioramento della presente politica, la Direzione si assume l'impegno a:

1. stabilire la presente Politica di Sicurezza dei Dati in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità di Data Vision, variandola ogni qualvolta sia necessario;
2. assicurare l'integrazione dei requisiti di sicurezza dei dati nei processi dell'organizzazione, assumendosi la responsabilità della relativa efficacia;
3. assicurare la disponibilità delle risorse tecniche, organizzative ed economiche necessarie per l'adozione delle misure di cifratura, protezione e backup descritte nella presente politica;
4. comunicare l'importanza di una gestione efficace della sicurezza dei dati e dell'essere conformi ai requisiti del SGSI e della Determinazione ACN n. 164179/2025;
5. sensibilizzare alla partecipazione attiva, guidare e sostenere il personale affinché contribuisca alla protezione dei dati, attraverso informazione, formazione e consapevolezza;
6. effettuare periodici Riesami sullo stato di attuazione della presente politica, con cadenza almeno annuale o maggiore in caso di incidenti significativi, evoluzioni normative o mutamenti dell'esposizione alle minacce;
7. approvare la presente politica tramite gli organi di amministrazione e direttivi, come richiesto dal punto 3 della misura GV.PO-01.

## 4. POLITICA DI SICUREZZA DEI DATI

### 4.1. Dichiarazione di intenti

La Direzione Data Vision (DD) considera la sicurezza dei dati un valore aziendale imprescindibile e un requisito necessario per l'erogazione affidabile dei servizi ai propri Clienti, per il rispetto dei requisiti contrattuali, normativi e regolamentari applicabili, e per il continuo miglioramento dei processi aziendali.

La presente politica è stabilita ed attuata per proteggere la riservatezza, l'integrità e la disponibilità dei dati gestiti da Data Vision, in coerenza con la strategia di gestione del rischio dell'organizzazione, da eventi intesi come minacce o incidenti, esterni e/o interni, che possano comprometterne il trattamento.

I principi fondamentali e distintivi della presente Politica di Sicurezza dei Dati sono:

8. la protezione dei dati a riposo (data-at-rest);
9. la protezione dei dati in transito (data-in-transit);

10. la protezione, conservazione e verificabilità dei backup dei dati;
11. l'approccio basato sul rischio nell'applicazione delle misure tecniche, proporzionato alla rilevanza dei sistemi informativi e di rete interessati;
12. la conformità ai requisiti legislativi, tecnici e normativi in materia di sicurezza dei dati, ivi compresi quelli di cui alla Determinazione ACN n. 164179/2025;
13. l'esame periodico sullo stato di applicazione della presente politica e degli obiettivi correlati;
14. la diffusione a tutto il personale aziendale dei principi della politica e dei corrispondenti obiettivi.

### 4.2. Protezione dei dati a riposo (data-at-rest)

Per almeno i sistemi informativi e di rete rilevanti, e in accordo agli esiti della valutazione del rischio condotta ai sensi della misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, Data Vision si impegna a garantire che:

- i dati memorizzati sui dispositivi portatili, ivi inclusi laptop, smartphone e tablet, e sui supporti rimovibili, siano cifrati con protocolli e algoritmi crittografici allo stato dell'arte e considerati sicuri;
- l'auto esecuzione dei supporti rimovibili sia disabilitata e che gli stessi siano sottoposti a scansione per il rilevamento di codice malevolo prima dell'utilizzo nei sistemi informativi e di rete aziendali.

Le procedure operative di attuazione delle misure sopra descritte sono adottate e documentate dalla funzione Amministratore Sistemi / Responsabile BC-DR, nel rispetto della presente politica, e sono periodicamente verificate nell'ambito degli Audit Interni.

### 4.3. Protezione dei dati in transito (data-in-transit)

Per almeno i sistemi informativi e di rete rilevanti, ivi inclusi quelli di comunicazione vocale, video e testuale, e in accordo agli esiti della valutazione del rischio condotta ai sensi della misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, Data Vision si impegna a garantire che, per la trasmissione dei dati da e verso l'esterno dell'organizzazione, siano utilizzati protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri.

Le procedure operative di attuazione di tale misura sono adottate e documentate nel rispetto della presente politica e sottoposte a verifica periodica.

### 4.4. Backup dei dati

In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei relativi piani (misura ID.IM-04), Data Vision si impegna a garantire che:

- siano effettuati periodicamente i backup dei dati e delle configurazioni dei sistemi informativi e di rete;
- per almeno i sistemi informativi e di rete rilevanti, siano conservate anche copie di backup offline;

- sia assicurata la riservatezza e l'integrità delle informazioni contenute nei backup, mediante adeguata protezione fisica dei supporti ovvero mediante cifratura;
- sia verificata periodicamente l'utilizzabilità dei backup effettuati, mediante test di ripristino.

Le procedure operative relative all'esecuzione, protezione, conservazione e verifica dei backup sono adottate e documentate nel rispetto della presente politica, sotto la responsabilità della funzione Amministratore Sistemi / Responsabile BC-DR.

### 4.5. Approccio basato sul rischio

L'applicazione delle misure di cui ai paragrafi 4.2, 4.3 e 4.4 è condotta, ove previsto, in accordo agli esiti della valutazione del rischio per la sicurezza informatica (misura ID.RA-05) e con riferimento prioritario ai sistemi informativi e di rete rilevanti individuati da Data Vision. Eventuali deroghe motivate da ragioni normative o tecniche sono documentate dalla funzione competente e sottoposte a verifica nell'ambito del Riesame della Direzione.

### 4.6. Diffusione, conformità e processo disciplinare

Il presente documento è uno dei documenti di riferimento del SGSI-DV in materia di sicurezza dei dati e deve essere condiviso con qualunque dipendente e con le terze parti rilevanti coinvolte in attività che possano avere impatto sulla sicurezza dei dati trattati da Data Vision.

La conformità alla presente politica è obbligatoria. Tutti devono comprendere il proprio ruolo e le proprie responsabilità nell'ambito della tutela del patrimonio informativo aziendale. Qualsiasi violazione ai principi espressi nel presente documento deve essere valutata per mettere in atto le azioni necessarie a minimizzare il rischio e per definire misure adeguate di prevenzione, nell'ambito del processo disciplinare applicabile in tutti i casi di violazione dei processi esistenti, ivi compresi quelli relativi alla sicurezza delle informazioni, definito nella procedura operativa S002_Disciplinare tecnico.

I destinatari della presente Politica di Sicurezza dei Dati sono il personale, i fornitori e tutte le terze parti interessate. Il documento, rivisto almeno annualmente, è reso disponibile a tutti ed ogni nuova versione viene pubblicata sul sito web aziendale e ne viene comunicata l'emissione.

Il documento è redatto con il supporto della funzione CSM / Responsabile Gestione Rischi, verificato dal Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI), approvato dal Punto di Contatto NIS2 / Referente CSIRT. La distribuzione di questo documento è sotto la responsabilità del RSGSI.

*Il Presidente del C.D.A.*

### 4.7. Obiettivi per la Sicurezza dei Dati

Nell'ambito dei principi sui quali si fonda la presente politica, la Direzione, con il supporto delle funzioni aziendali, ha definito il quadro di riferimento per fissare obiettivi coerenti, raggiungibili e misurabili in materia di sicurezza dei dati, tra i quali:

- garantire la cifratura, con algoritmi e protocolli allo stato dell'arte, dei dati a riposo sui dispositivi portatili e sui supporti rimovibili relativi ai sistemi informativi e di rete rilevanti;
- garantire la cifratura delle comunicazioni dati da e verso l'esterno relative ai sistemi informativi e di rete rilevanti;
- garantire l'esecuzione, la protezione e la verifica periodica dei backup, ivi incluse le copie offline per i sistemi rilevanti;
- ridurre il numero di eccezioni e deroghe non motivate alle misure di cifratura previste;
- garantire al personale un adeguato livello di consapevolezza in materia di sicurezza dei dati, anche attraverso il piano di formazione di cui alla misura PR.AT-01.

Gli obiettivi di dettaglio, con i relativi indicatori di prestazione (KPI), sono individuati e fissati annualmente in sede di Riesame della Direzione e riportati nel Documento Operativo Sicurezza delle Informazioni (DOSI) e nelle procedure operative specifiche del SGSI.

## 5. RUOLI E RESPONSABILITÀ

Coerentemente con l'assetto organizzativo di Data Vision e in assenza di una figura CISO dedicata, la responsabilità ultima della sicurezza informatica, ivi inclusa la sicurezza dei dati, è in capo all'Amministratore Delegato, che si avvale delle seguenti funzioni:

### 5.1. Punto di Contatto NIS2 / Referente CSIRT (Valerio Bizzarro)

- approva la presente Politica di Sicurezza dei Dati e le sue revisioni;
- rappresenta Data Vision nei rapporti con il CSIRT Italia e con l'Agenzia per la Cybersicurezza Nazionale;
- presiede il Comitato per la sicurezza informatica e ne coordina le attività.

### 5.2. Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni – RSGSI (Daniel Bizzarro)

- apporta gli aggiornamenti necessari alla presente politica e li sottopone all'approvazione;
- gestisce la redazione e l'aggiornamento delle politiche di sicurezza informatica per gli ambiti di cui alla misura GV.PO-01;
- programma ed esegue gli Audit Interni anche in materia di sicurezza dei dati;
- prepara i rendiconti periodici per il Riesame da parte della Direzione;
- diffonde le nuove versioni della presente politica.

### 5.3. CSM / Responsabile Gestione Rischi (Elena Amendola)

- supporta la redazione e l'aggiornamento della presente politica;
- conduce e mantiene aggiornata la valutazione del rischio di cybersecurity (ID.RA-05) cui sono ancorate le misure di protezione dei dati a riposo e in transito;

- monitora la tracciabilità delle deroghe motivate da ragioni normative o tecniche.

### 5.4. Amministratore Sistemi / Responsabile BC-DR (Luca Urbinati)

- attua e mantiene le misure tecniche di cifratura dei dati a riposo e in transito;
- pianifica, esegue e verifica i backup dei dati e delle configurazioni, ivi incluse le copie offline per i sistemi rilevanti, e i relativi test di ripristino;
- documenta le procedure operative attuative della presente politica, in coordinamento con il SOC.

## 6. RIFERIMENTI NORMATIVI

- UNI CEI ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni;
- Decreto legislativo 4 settembre 2024, n. 138 (recepimento direttiva NIS2);
- Determinazione ACN n. 164179/2025 – Allegato 1 “Misure di sicurezza di base per i soggetti importanti”, in particolare misura GV.PO-01 (ambito l, “Sicurezza dei dati”) e misure PR.DS-01, PR.DS-02, PR.DS-11;
- Framework Nazionale per la Cybersecurity e la Data Protection (FNCS), versione 2025.

## 7. REVISIONE

La Direzione approva la presente Politica di Sicurezza dei Dati. In conformità ai requisiti legislativi NIS2 (misura GV.PO-02), la presente politica è riesaminata e, se opportuno, aggiornata periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell’esposizione alle minacce e ai relativi rischi.

Ai fini del riesame, è verificata almeno la conformità della presente politica ai requisiti dell’ambito l) “Sicurezza dei dati” previsti dall’Allegato 1 alla Determinazione ACN n. 164179/2025, nonché la sua coerenza con la più ampia Politica per la Sicurezza delle Informazioni e con le altre politiche di sicurezza informatica adottate da Data Vision per i restanti ambiti previsti dalla misura GV.PO-01.