

Politica per la Sicurezza delle Informazioni

| | |
|--------------------------------|---------------------|
| REDAZIONE: | <i>DATASOFT RE</i> |
| Creazione: | <i>03/12/2025</i> |
| Ultima Modifica: | <i>17/02/2026</i> |
| Approvazione: | <i>Andrea Oliva</i> |
| Data Approvazione: | <i>17/02/2026</i> |
| Distribuzione o Stampa: | <i>07/04/2026</i> |

SOMMARIO

| | | |
|----|---|---|
| 1 | STORIA DELLE REVISIONI | 3 |
| 2 | PREMESSA..... | 4 |
| 3 | CONTESTO NORMATIVO E REGOLAMENTARE..... | 4 |
| 4 | PRINCIPI FONDAMENTALI | 4 |
| 5 | CAMPO DI APPLICAZIONE | 5 |
| 6 | OBIETTIVI | 5 |
| 7 | RESPONSABILITÀ E GOVERNANCE | 5 |
| 8 | GESTIONE DEI RISCHI E RESILIENZA OPERATIVA..... | 6 |
| 9 | MIGLIORAMENTO CONTINUO..... | 6 |
| 10 | DIFFUSIONE E REVISIONE..... | 7 |

1 Storia delle Revisioni

| Versione | Data | Paragrafo o Pagina | Descrizione della Variazione |
|-----------------|-------------|---------------------------|-------------------------------------|
| 1 | 03/12/2025 | Tutto il documento | Versione iniziale del documento |
| 1.1 | 17/02/2026 | Tutto il documento | Approvazione |

2 Premessa

Datasoft RE Srl (di seguito Datasoft), in qualità di software house specializzata nello sviluppo di soluzioni per la gestione del patrimonio immobiliare, riconosce il valore strategico e critico delle informazioni gestite, sia proprietarie che dei propri clienti del settore bancario e finanziario. Le informazioni costituiscono un asset aziendale di primaria importanza e necessitano di una protezione adeguata contro minacce di qualsiasi natura, siano esse accidentali o intenzionali, interne o esterne. Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) rappresenta lo strumento organizzativo e operativo mediante il quale Datasoft persegue la tutela della confidenzialità, dell'integrità e della disponibilità delle informazioni, compresi tutti i sistemi informativi, le infrastrutture tecnologiche e i processi organizzativi correlati. L'azienda si impegna a tutelare l'intero ciclo di vita delle informazioni, dalla loro creazione ed elaborazione fino all'archiviazione, trasmissione e dismissione finale.

3 Contesto Normativo e Regolamentare

Datasoft opera in un contesto altamente regolamentato, fornendo servizi e prodotti software a istituti finanziari. L'azienda riconosce l'importanza di conformarsi allo standard internazionale ISO/IEC 27001:2022 per i Sistemi di Gestione della Sicurezza delle Informazioni, nonché al Regolamento (UE) 2022/2554 - DORA (Digital Operational Resilience Act) che disciplina la resilienza operativa digitale per il settore finanziario.

Particolare attenzione è rivolta altresì al **GDPR** e alla **sostenibilità ambientale ed efficienza energetica**.

4 Principi Fondamentali

L'organizzazione adotta un approccio integrato alla sicurezza delle informazioni basato sui principi di riservatezza, integrità e disponibilità. La riservatezza assicura che le informazioni siano accessibili esclusivamente a soggetti autorizzati e per finalità legittime, mentre l'integrità garantisce l'accuratezza e la completezza delle informazioni proteggendole da modifiche non autorizzate. La disponibilità assicura che le informazioni e i servizi siano accessibili quando necessario agli utenti autorizzati. A questi principi si aggiungono la tracciabilità delle operazioni svolte sui sistemi informativi per garantire accountability, la resilienza operativa per prevenire e recuperare da eventi

avversi che possano impattare i sistemi ICT, e il miglioramento continuo basato sul ciclo Plan-Do-Check-Act.

La presente politica si applica a:

- tutti i dipendenti e collaboratori di Datasoft
- ai consulenti, fornitori e partner che accedono ai sistemi informativi aziendali
- a tutte le informazioni aziendali indipendentemente dal supporto utilizzato
- a tutti i sistemi informativi e infrastrutture tecnologiche
- ai prodotti software sviluppati e ai servizi erogati ai clienti del settore finanziario.

5 Campo di applicazione

Attività di progettazione, sviluppo, manutenzione ed erogazione di soluzioni software per la gestione dei patrimoni immobiliari, distribuite sia in modalità on-premise che in modalità cloud, inclusi i relativi servizi di supporto tecnico e assistenza clienti.

6 Obiettivi

L'Organizzazione persegue l'implementazione e il mantenimento di un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma ISO/IEC 27001:2022, sottoponendosi a verifiche periodiche da parte di organismi di certificazione accreditati.

Datasoft definisce ruoli e responsabilità in materia di sicurezza a tutti i livelli, allocando risorse adeguate a implementare e mantenere efficace il SGSI. Un programma continuativo di formazione sensibilizza il personale sui temi della sicurezza delle informazioni, della resilienza operativa digitale e della protezione dei dati personali. L'azienda implementa procedure per la gestione tempestiva degli incidenti di sicurezza, garantendo capacità di risposta e ripristino anche in presenza di eventi avversi.

7 Responsabilità e Governance

La **Direzione** di Datasoft approva la presente politica e ne assicura la diffusione a tutti i livelli organizzativi, promuovendo attivamente la cultura della sicurezza delle informazioni e della resilienza operativa. La Direzione alloca le risorse necessarie per l'implementazione e il mantenimento del SGSI, esamina periodicamente l'adeguatezza e l'efficacia del sistema attraverso riesami formali e

assume la responsabilità ultima della gestione dei rischi ICT e della conformità al Regolamento DORA.

Il **Responsabile del SGSI** coordina le attività di implementazione, manutenzione e miglioramento del sistema, monitora la conformità alle politiche e alle procedure di sicurezza, supporta la Direzione nel riesame del sistema, gestisce i processi di risk assessment e risk treatment e coordina le attività di audit interno.

Ciascun **dipendente** e **collaboratore** è tenuto a conoscere e rispettare le politiche e le procedure di sicurezza, deve utilizzare le risorse informatiche aziendali in modo responsabile e conforme, ha l'obbligo di segnalare tempestivamente incidenti, anomalie o sospette violazioni della sicurezza e partecipa ai programmi di formazione sulla sicurezza.

I **fornitori**, i **partner** ed eventuali **collaboratori esterni** sono contrattualmente vincolati al rispetto delle politiche di sicurezza di Datasoft, sono soggetti a valutazioni di sicurezza prima dell'instaurazione del rapporto, possono essere oggetto di audit e verifiche periodiche e devono notificare tempestivamente eventuali incidenti di sicurezza.

8 Gestione dei Rischi e Resilienza Operativa

Datasoft adotta un approccio strutturato e sistematico alla gestione dei rischi per la sicurezza delle informazioni e dei rischi ICT. Il processo prevede l'identificazione degli asset informativi e delle minacce, la valutazione dei rischi attraverso metodologie riconosciute, il trattamento mediante implementazione di controlli appropriati, il monitoraggio continuo e il riesame periodico dei rischi, nonché il testing periodico della resilienza operativa attraverso test di vulnerabilità, analisi di scenario e test di penetrazione. Il processo di risk assessment è condotto con periodicità almeno annuale e ogni qualvolta si verificano cambiamenti significativi nell'organizzazione, nelle tecnologie o nel contesto di minaccia.

9 Miglioramento Continuo

L'organizzazione si impegna a mantenere un processo di miglioramento continuo del SGSI attraverso:

- audit interni periodici per verificare la conformità e l'efficacia dei controlli
- riesami della Direzione per valutare le prestazioni del sistema, analisi degli incidenti di sicurezza e implementazione di azioni correttive

- monitoraggio dell'evoluzione delle minacce e delle vulnerabilità, aggiornamento continuo delle competenze del personale e valutazione delle tecnologie emergenti e delle best practice di settore.

10 Diffusione e Revisione

La presente politica è approvata dalla Direzione di Datasoft RE Srl, comunicata a tutto il personale dipendente e collaboratori e resa disponibile alle parti interessate rilevanti quali clienti, fornitori e partner.

Il documento è soggetto a revisione annuale e comunque in presenza di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, ed è mantenuto aggiornato in relazione all'evoluzione delle minacce, delle tecnologie e del quadro regolamentare.

Data

La Direzione

17/02/2026

dott. Andrea Oliva