

POL Politica di conservazione e cancellazione delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	28/04/2026	Glauco Timoteo	William Palozzo

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Principi di conservazione delle informazioni
- Piano di conservazione delle informazioni
- Cancellazione sicura delle informazioni
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica stabilisce il framework di riferimento per la gestione del ciclo di vita delle informazioni di DG Impianti Industriali S.p.A., definendo per ciascuna tipologia di dato i periodi di conservazione obbligatori e le modalità di cancellazione sicura al termine di tali periodi. L'obiettivo è bilanciare le esigenze operative dell'organizzazione — attiva nella progettazione e costruzione di impianti industriali nei settori energia, oil & gas, petrolchimico e farmaceutico — con gli obblighi legali, fiscali e contrattuali applicabili.

La politica garantisce il rispetto del principio di limitazione della conservazione, assicurando che i dati personali non siano mantenuti oltre il tempo strettamente necessario al conseguimento delle finalità per cui sono stati raccolti. Al contempo, essa stabilisce le regole affinché le informazioni, al raggiungimento del termine di conservazione, siano cancellate in modo sicuro e irrecuperabile, riducendo il rischio di accesso non autorizzato, furto di dati o violazione della riservatezza.

Campo di applicazione

La presente politica si applica a tutte le informazioni, in qualsiasi formato — digitale e cartaceo — e a tutti gli asset informativi che sono creati, ricevuti, trattati o archiviati dall'organizzazione. Rientrano nel perimetro di applicazione server, database, piattaforme cloud (Microsoft 365, SharePoint, OneDrive), dispositivi utente, supporti rimovibili e archivi fisici presenti presso la sede legale di Via Napo Torriani n. 22, Milano, e la sede operativa di Via Antonio Vivaldi n. 4, Montesilvano (PE).

L'ambito si estende a tutto il personale dipendente, ai collaboratori esterni, ai consulenti e alle terze parti che gestiscono informazioni per conto di DG Impianti Industriali S.p.A., inclusi i collaboratori assegnati a specifiche commesse e i fornitori ai quali sono conferite credenziali di accesso ai sistemi aziendali.

Riferimenti normativi

- **ISO 27001:2022** — Requisiti per i sistemi di gestione della sicurezza delle informazioni
- **ISO 27002:2022** — Linee guida per i controlli di sicurezza delle informazioni
- **Regolamento (UE) 2016/679 (GDPR)** — Protezione delle persone fisiche con riguardo al trattamento dei dati personali
- **D.Lgs. 196/2003 e s.m.i.** — Codice in materia di protezione dei dati personali

Termini e definizioni

- **Conservazione** — Processo di mantenimento delle informazioni per un periodo di tempo predefinito e giustificato, in formato attivo o archiviato, in conformità ai requisiti legali, contrattuali e operativi dell'organizzazione.

- **Cancellazione sicura** — Processo che rende le informazioni irrecuperabili, garantendo che non possano essere ricostruite, lette o ripristinate da alcun soggetto, autorizzato o meno.
- **Archiviazione** — Trasferimento delle informazioni non più in uso attivo in un ambiente di conservazione a lungo termine, sicuro e a costo contenuto, nel rispetto dei periodi di conservazione stabiliti.
- **Sospensione legale (Legal Hold)** — Istruzione formale emessa dal Top Management per sospendere le normali procedure di cancellazione di specifiche informazioni in ragione di un contenzioso in corso, un'indagine o un obbligo di audit, fino a revoca esplicita.
- **Decommissioning** — Processo strutturato di disattivazione e rimozione degli account, delle credenziali e dei dati associati a un utente o a un asset al termine del rapporto lavorativo o contrattuale.

Ruoli e responsabilità

- **Chief Executive Officer** — Supervisiona l'attuazione della presente politica, assicura la disponibilità delle risorse necessarie e autorizza le eventuali sospensioni legali delle attività di cancellazione.
- **ICT-RSGSI** — Implementa e mantiene le misure tecniche per l'archiviazione sicura e la cancellazione irrecuperabile delle informazioni digitali, eseguendo le operazioni di decommissioning degli account e dei supporti in conformità alla presente politica.
- **HSEQ** — Collabora alla definizione dei periodi di conservazione per la documentazione relativa a salute, sicurezza, ambiente e qualità di cantiere, assicurandone la conformità alla normativa settoriale.
- **Dipendenti, Collaboratori e Terze parti** — Sono tenuti ad aderire ai periodi di conservazione definiti nella presente politica, a non conservare copie non autorizzate di informazioni aziendali e, ove necessario, a smaltire le informazioni in modo sicuro secondo le indicazioni ricevute.

Principi di conservazione delle informazioni

I dati personali non devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo superiore a quello strettamente necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati. Tale principio di limitazione della conservazione costituisce un pilastro della presente politica e si applica trasversalmente a tutte le categorie di informazioni gestite dall'organizzazione.

Le informazioni sono conservate esclusivamente per il tempo necessario a soddisfare finalità specifiche e documentate, che possono essere di natura:

- **Operativa** — continuità del servizio, gestione dei progetti di ingegneria e costruzione, supporto alle commesse attive
- **Legale** — obblighi fiscali, tributari, civilistici e penali previsti dalla normativa italiana ed europea
- **Contrattuale** — requisiti specifici dei clienti pubblici e privati, in particolare nei settori energia, oil & gas, petrolchimico e farmaceutico
- **Di sicurezza** — conservazione dei log di sistema per il monitoraggio degli eventi e le eventuali indagini forensi

I periodi di conservazione sono riesaminati almeno una volta all'anno dal Chief Executive Officer, in collaborazione con l'ICT-RSGSI, per garantirne la continua adeguatezza rispetto al contesto normativo, contrattuale e operativo vigente. L'esito del riesame è formalizzato e reso disponibile nell'ambito del riesame della direzione.

Piano di conservazione delle informazioni

L'organizzazione classifica le proprie informazioni in categorie logiche al fine di assegnare a ciascuna un periodo di conservazione proporzionato e giustificato. La tabella seguente riporta le principali categorie, il supporto prevalente, il periodo di conservazione applicabile e la relativa motivazione normativa o operativa.

Categoria di informazione	Supporto	Periodo di conservazione	Motivazione
Documentazione contabile e fiscale	Digitale / Cartaceo	10 anni dalla data di registrazione	Art. 2220 Codice Civile; normativa fiscale
Contratti con clienti e fornitori	Digitale / Cartaceo	10 anni dalla conclusione del contratto	Art. 2946 Codice Civile (prescrizione ordinaria)
Documentazione di progetto (FEED, EPC, P&ID)	Digitale	10 anni dalla consegna definitiva dell'opera	Obblighi contrattuali e responsabilità professionale
Fascicoli del personale dipendente	Digitale / Cartaceo	10 anni dalla cessazione del rapporto di lavoro	Termini prescrizionali giuslavoristici
Dati retributivi e previdenziali	Digitale / Cartaceo	10 anni dalla cessazione del rapporto di lavoro	Obblighi fiscali e previdenziali

Dati dei candidati non assunti	Digitale	24 mesi dalla raccolta	Principio di limitazione della conservazione (GDPR)
Registrazioni di formazione	Digitale / Cartaceo	Durata del rapporto più 5 anni	Requisiti normativi e contrattuali
Documentazione HSEQ di cantiere	Digitale / Cartaceo	10 anni dalla conclusione del progetto	Obblighi normativi in materia di salute e sicurezza
Account e credenziali utente (dipendenti)	Digitale	Disattivazione immediata alla cessazione del rapporto	Principio del minimo privilegio; ISO 27001
Account e credenziali utente (collaboratori di commessa)	Digitale	Disattivazione al termine della commessa	Requisiti contrattuali e di sicurezza
Caselle di posta elettronica (utenti cessati)	Digitale	Cancellazione entro 30 giorni dalla cessazione	Principio di minimizzazione (GDPR); Provvedimenti del Garante Privacy
Log di accesso degli amministratori di sistema	Digitale	Minimo 6 mesi	Provvedimento Garante Privacy 27/11/2008
Log di sicurezza informatica	Digitale	12 mesi	Esigenze di monitoraggio e indagine forense
Documentazione del SGSI	Digitale	3 anni dopo la revisione o la sostituzione	Requisiti di audit e tracciabilità ISO 27001

Il dettaglio completo dei periodi di conservazione per ogni singola categoria di informazione o asset — comprensivo di tipologia di record, supporto, durata e motivazione — è mantenuto dal Chief Executive Officer in collaborazione con l'ICT-RSGSI e le altre parti interessate. Tale documento è controllato, aggiornato con cadenza almeno annuale e reso disponibile a tutto il personale coinvolto nelle attività di gestione delle informazioni.

Cancellazione sicura delle informazioni

Al termine del periodo di conservazione stabilito dall'organizzazione, le informazioni devono essere cancellate in modo sicuro e irrecuperabile. L'ICT-RSGSI è responsabile dell'esecuzione delle operazioni di cancellazione sui supporti digitali, mentre ogni responsabile di area deve assicurare la corretta eliminazione dei materiali cartacei di propria competenza.

Metodi di cancellazione per supporti digitali

La scelta del metodo di cancellazione deve essere proporzionata al livello di classificazione delle informazioni, in conformità alla *POL Politica di classificazione ed etichettatura delle informazioni*. I metodi ammessi sono i seguenti:

- **Cancellazione crittografica** — distruzione irreversibile della chiave di cifratura associata ai dati protetti, rendendo il contenuto permanentemente illeggibile. Questo metodo è applicabile ai dati cifrati in conformità alla *PRO Procedura di crittografia e gestione delle chiavi crittografiche*.
- **Sovrascrittura multipla** — sovrascrittura dell'intero supporto di archiviazione con pattern casuali per un numero di passaggi adeguato alla sensibilità dei dati, secondo gli standard riconosciuti a livello internazionale.
- **Smagnetizzazione (degaussing)** — esposizione dei supporti magnetici (hard disk tradizionali, nastri) a un campo magnetico ad alta intensità, tale da rendere i dati irrecuperabili.
- **Distruzione fisica** — triturazione, perforazione o frantumazione dei supporti (hard disk, SSD, chiavette USB) quando la cancellazione logica non è tecnicamente sufficiente a garantire l'irrecuperabilità.

Metodi di cancellazione per supporti cartacei

I materiali cartacei contenenti informazioni classificate come "limited" o "confidential" devono essere distrutti tramite distruggi documenti con taglio a frammento (cross-cut). I supporti cartacei contenenti informazioni classificate come "public" possono essere smaltiti attraverso i normali canali di raccolta differenziata.

Decommissioning degli account e delle risorse digitali

Al verificarsi della cessazione di un rapporto di lavoro o del termine di una commessa, l'ICT-RSGSI deve procedere alla disattivazione e successiva cancellazione delle risorse digitali associate all'utente. Le categorie di risorse soggette a decommissioning comprendono:

- Account sul dominio Active Directory (Server AD)
- Tenant di posta elettronica, OneDrive e SharePoint

- Licenze di assistenza remota
- Agente antivirus e profili di sicurezza endpoint
- Formattazione sicura del dispositivo assegnato
- Cartelle personali su file server

Ogni operazione di decommissioning deve essere tracciata con indicazione della data di cancellazione, dell'autore dell'attività, del nominativo dell'utente interessato, della motivazione e delle categorie di dati cancellati.

Gestione dei file temporanei

I file temporanei generati dai sistemi nel corso delle normali operazioni devono essere identificati e rimossi in modo sicuro entro trenta giorni dal momento in cui non sono più necessari. L'ICT-RSGSI deve definire e mantenere attive le politiche di pulizia automatica sui sistemi aziendali.

Riutilizzo dei supporti di archiviazione

Lo spazio di archiviazione riutilizzabile deve essere sottoposto a un processo di cancellazione sicura prima di essere riassegnato a un nuovo utente o destinato a un diverso impiego. Il metodo di cancellazione deve essere selezionato in funzione della classificazione delle informazioni precedentemente contenute nel supporto, in conformità alla *PRO Procedura di configurazione, gestione e smaltimento degli asset*.

Sospensione legale (Legal Hold)

Il Chief Executive Officer può disporre, con comunicazione scritta, la sospensione delle normali procedure di cancellazione per specifiche categorie di informazioni qualora ricorra una delle seguenti circostanze:

- Contenzioso in corso o ragionevolmente prevedibile
- Indagine da parte di autorità competenti
- Audit regolamentare o contrattuale che richieda la conservazione dei dati originali
- Richiesta formale da parte di un'autorità giudiziaria o di vigilanza

La sospensione legale prevale su qualsiasi periodo di conservazione ordinario e resta in vigore fino a revoca esplicita da parte del Chief Executive Officer. L'ICT-RSGSI deve isolare le informazioni oggetto di sospensione, garantendone l'integrità e impedendone la modifica o la cancellazione accidentale. L'ICT-RSGSI tiene traccia di tutte le sospensioni attive, documentandone la data di emissione, l'ambito di applicazione e la data di eventuale revoca.

Archiviazione e aggiornamento

La presente politica è un documento controllato del Sistema di Gestione della Sicurezza delle Informazioni di DG Impianti Industriali S.p.A. e sarà riesaminata con cadenza annuale, o a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia, nel contesto normativo o nel panorama delle minacce, sotto la supervisione del Chief Executive Officer e dell'ICT-RSGSI. Ogni modifica sostanziale deve essere approvata dal Chief Executive Officer prima della distribuzione. Le versioni superate sono conservate in conformità ai periodi di conservazione della documentazione del SGSI definiti nella presente politica e gestite secondo la *PRO Procedura di gestione delle informazioni documentate*.

Documenti di riferimento

- *POL Politica di sicurezza delle informazioni*
- *POL Politica di classificazione ed etichettatura delle informazioni*
- *POL Politica di sicurezza operativa*
- *PRO Procedura di configurazione, gestione e smaltimento degli asset*
- *PRO Procedura di crittografia e gestione delle chiavi crittografiche*
- *PRO Procedura di gestione e controllo degli accessi logici*
- *PRO Procedura di gestione delle informazioni documentate*