POL Politica di conservazione e cancellazione delle informazioni

Nome della società	Partech
Data di entrata in vigore	22/04/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	22/04/2025	-- N / D --	Fabio Damiani	Giuseppe Favilli

Scopo

Lo scopo di questa politica è stabilire un framework per la gestione del ciclo di vita delle informazioni, definendo per ogni tipologia di dato i periodi di conservazione obbligatori. La politica mira a bilanciare le necessità operative con gli obblighi legali, fiscali e contrattuali, garantendo il rispetto del principio di "limitazione della conservazione" del GDPR. Assicura inoltre che le informazioni, al termine del loro ciclo di vita, siano cancellate in modo sicuro e irrecuperabile.

Indice

Campo di Applicazione

La presente policy definisce i principi e le direttive per la conservazione e la successiva cancellazione sicura delle informazioni gestite da Partech. Lo scopo è garantire che le informazioni siano conservate per un periodo di tempo adeguato a soddisfare le esigenze operative, legali, normative e contrattuali, e che siano distrutte in modo sicuro e irreversibile al termine del loro ciclo di vita, in conformità con i requisiti dello standard ISO/IEC 27001 e con il Registro delle attività di trattamento ex art. 30 GDPR.

Riferimenti Normativi

- Regolamento (UE) 2016/679 (GDPR)
- ISO/IEC 27001 - Sistemi di gestione della sicurezza delle informazioni
- Codice Civile italiano (art. 2220)
- Registro delle attività di trattamento ex art. 30 GDPR

Termini e Definizioni

- **Asset informativo**: Qualsiasi cosa che abbia valore per l'organizzazione. Le informazioni, in varie forme, sono un tipo di asset.
- **Proprietario dell'informazione**: Ruolo responsabile del controllo della produzione, sviluppo, manutenzione, uso e sicurezza di specifici asset informativi.
- **Registro delle attività di trattamento (RoPA)**: documento obbligatorio ai sensi dell’art. 30 GDPR che elenca finalità, categorie di dati e interessati, destinatari, eventuali trasferimenti, *e — ove possibile — i termini ultimi di cancellazione* e una descrizione generale delle misure di sicurezza

Ruoli e Responsabilità

- **CEO / Direzione Generale**: Approva la politica di conservazione e cancellazione e assicura la disponibilità delle risorse necessarie per la sua implementazione ed efficacia.
- **Executive - Cybersecurity e Privacy**: Supervisiona la strategia di sicurezza e privacy, garantendo che le procedure di conservazione e cancellazione siano adeguate a mitigare i rischi e conformi alle normative vigenti.
- **Executive - Risorse umane**: Collabora alla definizione dei periodi di conservazione per le informazioni relative al personale, assicurandone una gestione conforme.
- **Executive - Amministrazione & Finanza**: Collabora alla definizione dei periodi di conservazione per le informazioni di natura finanziaria e contabile, garantendone la conformità normativa.
- **Responsabile Privacy & GDPR**: Definisce, documenta e riesamina i periodi di conservazione delle informazioni, gestisce le sospensioni per obblighi legali (legal hold) e assicura la conformità al GDPR. Inoltre, assicura l’allineamento costante tra questa Policy, il Piano di conservazione e il Registro; inserisce/aggiorna nel Registro i termini di conservazione per ciascun trattamento; dispone e documenta eventuali *legal hold* nel Registro e nelle registrazioni operative.

- **RSGI (Responsabile del Sistema di Gestione Integrato)**: Assicura che il Piano di conservazione sia gestito come un'informazione documentata controllata, in linea con le procedure del sistema di gestione.
- **Responsabile IT / Infrastructure & Operations**: Garantisce che le procedure tecniche per la cancellazione sicura delle informazioni digitali siano implementate e applicate correttamente.
- **Tecnico - Sistemista**: Esegue le operazioni tecniche di cancellazione sicura delle informazioni digitali secondo le procedure approvate.

Principi di conservazione delle informazioni

Partech deve conservare le informazioni esclusivamente per il periodo necessario a soddisfare i requisiti operativi, legali, normativi e contrattuali applicabili. Al termine di tale periodo, le informazioni devono essere cancellate in modo sicuro e irreversibile. La definizione dei periodi di conservazione per ogni categoria di informazioni deve basarsi sulla loro classificazione, come stabilito nella "POL Politica di classificazione ed etichettatura delle informazioni", e sulla conformità agli obblighi applicabili.

Il Responsabile Privacy & GDPR, in collaborazione con i rispettivi responsabili di funzione, quali l'Executive - Risorse umane per i dati del personale e l'Executive - Amministrazione & Finanza per i dati finanziari, e con la supervisione dell'Executive - Cybersecurity e Privacy, ha il compito di definire e documentare i periodi di conservazione per tutte le categorie di informazioni. L'approvazione finale dei periodi di conservazione spetta alla CEO / Direzione Generale.

Il Responsabile Privacy & GDPR ha la responsabilità di disporre la sospensione delle procedure standard di cancellazione per specifiche informazioni soggette a obblighi di conservazione legale (legal hold), come in caso di contenziosi, indagini o audit. Tale sospensione, così come la sua revoca, deve essere formalmente documentata e comunicata alle funzioni competenti.

I periodi di conservazione definiti per ciascuna categoria di dati devono essere coerenti con la colonna “TERMINI ULTIMI DI CANCELLAZIONE PREVISTI” riportata nel Registro (Allegato 1). Esempi tratti dal Registro:

- **Rapporto di lavoro (dipendenti)**: 10 anni dal termine del rapporto
- **Candidati**: conservazione del CV per max 1 anno
- **Videosorveglianza**: conservazione immagini per max 48 ore

Piano di conservazione delle informazioni

Partech deve istituire e mantenere un *Piano di conservazione delle informazioni formale*, che documenti i requisiti di conservazione per tutte le categorie di dati gestite. Il Responsabile SGI è responsabile della gestione del Piano di conservazione come informazione documentata controllata, in accordo con quanto previsto dalla "PRO Procedura di gestione delle informazioni documentate". Il Responsabile Privacy & GDPR e l'Executive - Cybersecurity e Privacy sono responsabili della correttezza, completezza e adeguatezza dei contenuti del piano.

Il Piano di conservazione delle informazioni deve specificare per ogni categoria di dati almeno i seguenti elementi:

- Una descrizione chiara dell'asset informativo.
- Il proprietario dell'informazione (information owner).
- Il periodo di conservazione specifico, basato su requisiti legali, come quelli definiti dall'art. 2220 del Codice Civile che impone una conservazione di dieci anni per le scritture contabili, o su necessità operative e contrattuali.
- La giustificazione legale, normativa, contrattuale o di business che motiva il periodo di conservazione.
- Il metodo di cancellazione o distruzione sicura da applicare al termine del ciclo di vita.

Il Piano di conservazione deve essere riesaminato con cadenza almeno annuale, o a seguito di cambiamenti significativi gestiti tramite la "PRO Procedura di gestione del cambiamento", per garantirne la continua idoneità. Tale riesame è responsabilità del Responsabile Privacy & GDPR e dell'Executive - Cybersecurity e Privacy. Il Piano di conservazione recepisce e normalizza i termini indicati nel Registro. In caso di discrepanze, viene attivato un aggiornamento coordinato entro 30 giorni:

1. aggiornamento del record nel Registro,
2. aggiornamento del Piano di conservazione,
3. comunicazione alle funzioni interessate.

Il riesame periodico del Piano verifica anche la corretta valorizzazione dei *termini ultimi di cancellazione* nel Registro e la coerenza con le misure tecniche/organizzative ivi descritte (inclusi password policy, backup, formazione).

Cancellazione sicura delle informazioni

Tutte le informazioni, indipendentemente dal supporto (digitale o fisico), devono essere cancellate o distrutte in modo sicuro e irreversibile al termine del loro periodo di conservazione, a condizione che non siano più necessarie per scopi legittimi e non siano soggette a sospensioni per obblighi legali.

Le metodologie di cancellazione devono essere adeguate al livello di classificazione dell'informazione, come definito nella "POL Politica di classificazione ed etichettatura delle informazioni". Le tecniche approvate, che includono sovrascrittura, cancellazione crittografica o distruzione fisica, sono descritte nella "PRO Procedura di cancellazione sicura". Il Responsabile IT / Infrastructure & Operations deve assicurare che il personale tecnico, come il Tecnico - Sistemista, esegua la cancellazione sicura delle informazioni digitali utilizzando le tecniche approvate.

Ogni attività di cancellazione o distruzione deve essere tracciata e documentata nel "MOD Registro di cancellazione dei dati". La compilazione di tale registro è responsabilità del ruolo che esegue l'operazione. Il registro deve contenere almeno:

- Data e ora della cancellazione.
- Motivo della cancellazione (es. scadenza del periodo di conservazione, richiesta dell'interessato).
- Categoria dei dati cancellati.

- Interessato o gruppo di soggetti (se applicabile).
- Metodo di cancellazione utilizzato.
- Ruolo del responsabile dell'esecuzione.

L'Executive - Cybersecurity e Privacy è responsabile della revisione periodica del "MOD Registro di cancellazione dei dati" e della verifica dell'efficacia delle procedure di cancellazione per assicurare la conformità alla presente politica. La pianificazione delle cancellazioni si basa sui *termini ultimi di cancellazione* riportati nel Registro. Per trattamenti con tempistiche specifiche (es. disattivazione account/log) devono essere predisposte job/attività periodiche e controlli di efficacia. Ogni intervento è tracciato nel MOD Registro di cancellazione dei dati, riportando anche l'ID/voce del Registro cui si riferisce.

Archiviazione e Aggiornamenti

Questo documento è gestito come informazione documentata controllata all'interno del Sistema di Gestione Integrato. Viene sottoposto a revisione con cadenza almeno annuale, o in occasione di cambiamenti organizzativi, normativi o tecnologici rilevanti, per assicurarne la continua adeguatezza. Ogni aggiornamento è soggetto ad approvazione formale.

Documenti di Riferimento

- Registro delle attività di trattamento ex art. 30 GDPR
- MOD Registro di cancellazione dei dati
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione del cambiamento
- PRO Procedura di cancellazione sicura