POLITICA DI CONSERVAZIONE DEI DATI

Codice:	04/2022
Revisione:	2
Data di revisione:	29/05/2022
Redatto da:	Responsabile Protezione Dati
Approvato da:	Controllore - Titolare del Trattamento
Livello di Riservatezza	III

Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica
30/05/2018	0	RPD	PRIMA EMISSIONE
31/05/2019	1	RPD	SECONDA EMISSIONE

Sommario

1. Campo d'applicazione, scopo e destinatari

Questa politica stabilisce i periodi di conservazione richiesti per determinate categorie di dati personali e stabilisce gli standard minimi da applicare quando si distruggono determinate informazioni all'interno dell'azienda.

La presente politica si applica a tutte le unità gestionali della società, i processi e i sistemi in cui la società svolge attività aziendali o di altro tipo con terzi.

La presente Politica si applica a tutti i funzionari, amministratori, dipendenti, agenti, affiliati, collaboratori, consulenti o fornitori di servizi che possono raccogliere, trattare o accedere ai dati (compresi i dati personali e / o dati personali sensibili).

È responsabilità di tutti i soggetti di cui sopra familiarizzare con questa Politica e garantire un'adeguata conformità con essa.

Questa politica si applica a tutte le informazioni utilizzate presso l'Ente. Esempi di documenti includono:

- Messaggi di posta elettronica
- Documenti cartacei
- Documenti digitali
- Video e audio
- Dati generati dai sistemi di controllo degli accessi fisici

2. Documenti di Riferimento

- Il GDPR dell'UE 2016/679 (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
- Il D.Lgs.196/2003 c.d. "TESTO UNICO DELLA PRIVACY"
- Politica di Protezione dei Dati Personali dei Dipendenti
- Politica di Conservazione dei Dati
- Descrizione del Ruolo del Responsabile della Protezione dei Dati
- Linee guida per l'Elenco dei Dati e la Mappatura delle Attività di Trattamento
- Procedura per la Richiesta di Accesso ai Dati da parte dell'Interessato
- Metodologia di Valutazione d'Impatto sulla Protezione dei Dati
- Procedura di Trasferimento di Dati Personali
- Politiche di Sicurezza IT
- Procedura di Comunicazione di una Violazione di Dati

3. Regole per la Conservazione

3.1. Principio Generale della conservazione

Nel caso in cui, per qualsiasi categoria di documento non specificatamente definita altrove nella presente Politica (e in particolare nel Programma di Conservazione dei Dati) e salvo diversamente previsto dalla legge applicabile, il periodo di conservazione richiesto per tali documenti sarà considerato di 10 anni dalla data di creazione del documento e dall'erogazione della prestazione richiesta.

3.2. Programma Generale di Conservazione dei Dati

Il Responsabile della Protezione dei Dati definisce il periodo di tempo in cui i documenti e le registrazioni elettroniche devono essere conservate attraverso il programma di conservazione dei dati.

Come eccezione, i periodi di conservazione all'interno del Programma di Conservazione dei Dati possono essere prolungati in casi quali:

Indagini in corso da parte delle autorità, se esiste la possibilità che i dati personali siano necessari per dimostrare la conformità con i requisiti legali;
Nell'esercizio dei diritti legali in caso di cause legali o procedimenti giudiziari analoghi ai sensi della legge locale.

3.3. La Protezione dei Dati durante il Periodo di Conservazione

Sarà considerata la possibilità che i supporti dei dati utilizzati per l'archiviazione si esauriscano. Se vengono scelti supporti di registrazione elettronici, tutte le procedure e i sistemi che garantiscono l'accesso alle informazioni durante il periodo di conservazione (sia per quanto riguarda il supporto informativo sia per la leggibilità dei formati) devono essere anch'essi conservati al fine di salvaguardare l'informazione dalla perdita come risultato di futuri cambiamenti tecnologici. La responsabilità per la conservazione ricade sul Responsabile della Protezione dei Dati.

3.4. Distruzione dei dati

L'Azienda e i suoi dipendenti dovrebbero quindi, su base regolare, riesaminare tutti i dati, siano essi detenuti elettronicamente o su carta, per decidere se distruggere o cancellare qualsiasi dato una volta che lo scopo per cui tali documenti sono stati creati non è più rilevante. Vedere l'Allegato per il Programma di Conservazione dei Dati.

La responsabilità generale per la distruzione dei dati ricade sul Responsabile della Protezione dei Dati.

Una volta presa la decisione di smaltirli secondo il Programma di Conservazione, i dati dovrebbero essere cancellati, triturati o altrimenti distrutti in misura equivalente al loro valore per gli altri e al loro livello di riservatezza. Il metodo di smaltimento varia e dipende dalla natura del documento. Ad esempio, tutti i documenti che contengono informazioni sensibili o riservate (e dati personali particolarmente sensibili) devono essere smaltiti come rifiuti riservati e soggetti a cancellazione elettronica sicura; alcuni contratti scaduti o sostituiti richiedono soltanto la distruzione interna con il trita-carte.

La sezione Programma dello smaltimento dei documenti di seguito definisce la modalità di smaltimento.

In questo contesto, il dipendente deve svolgere i compiti e assumere le responsabilità rilevanti per la distruzione delle informazioni in modo appropriato. Il processo specifico di cancellazione o distruzione può essere effettuato da un dipendente o da un fornitore di servizi a cui il Controllore in persona del Responsabile di settore subappalta il servizio.

Devono essere rispettate, in tale operazione, tutte le disposizioni generali applicabili ai sensi delle leggi sulla protezione dei dati ed in base a quanto previsto dalla Politica sulla Protezione dei Dati Personali dell'Azienda.

Devono essere predisposti controlli adeguati che impediscano la perdita permanente delle informazioni essenziali dell'Azienda a seguito di distruzione intenzionale o involontaria delle informazioni - questi controlli sono descritti nelle Politiche di Sicurezza dell'Informazione.

Il Responsabile della Protezione dei Dati deve documentare e approvare pienamente il processo di distruzione.

Devono essere pienamente rispettati i requisiti di legge applicabili per la distruzione delle informazioni, in particolare i requisiti delle leggi applicabili sulla protezione dei dati.

3.5. Violazione, Misure di Attuazione e Conformità

La persona incaricata della protezione dei dati ha la responsabilità di garantire che ciascuno degli uffici dell'Azienda rispetti questa Politica. È anche responsabilità del Responsabile della Protezione dei Dati assistere gli uffici locali per quanto riguarda le richieste delle autorità locali competenti per la protezione dei dati o delle autorità governative.

Qualsiasi sospetto di violazione di questa Politica deve essere immediatamente segnalato al Responsabile della Protezione dei Dati. Tutti i casi di sospette violazioni della Politica devono essere investigati e devono essere attuate le relative azioni adeguate.

Il mancato rispetto di questa Politica può comportare conseguenze negative, tra cui, a titolo esemplificativo ma non esaustivo, contenziosi, perdita finanziaria e danni alla reputazione della società, lesioni personali, danni o perdite. La mancata osservanza di questa Politica da parte dei dipendenti a tempo indeterminato, a tempo determinato o collaboratori, o di terzi, cui è stato concesso l'accesso ai locali o alle informazioni dell'azienda, può pertanto comportare procedimenti disciplinari o la risoluzione del loro rapporto di lavoro o di contratto. Tale inosservanza può anche comportare un'azione legale nei confronti delle parti coinvolte in tali attività.

4. Smaltimento dei documenti

Programma dello Smaltimento di Routine

Documenti che possono essere regolarmente distrutti, a meno che non siano oggetto di un'inchiesta legale o normativa in corso, sono i seguenti:

Comunicazioni quotidiane di riunioni e altri eventi;

Richieste di informazioni ordinarie;

Prenotazioni per riunioni interne senza oneri / costi esterni;

Trasmissione di documenti quali lettere, copertine fax, messaggi e-mail, libretti di circolazione, biglietti di accompagnamento ed elementi simili che accompagnano i documenti ma non aggiungono alcun valore;

Moduli di messaggi;

Elenco indirizzi, liste di distribuzione sostituiti ecc.;

Duplicati documenti come copie inviate per conoscenza o inoltrate per informazione, bozze inalterate, stampe di snapshot o estratti da database e file temporanei;

Documenti interni di magazzino che sono obsoleti o sostituiti;

Cianografie, stampe tecniche, preventivi, cataloghi, volantini e newsletter di fornitori o altre strutture esterne esterne.

In tutti i casi, lo smaltimento è soggetto ad eventuali obblighi di divulgazione che possono esistere nel contesto di un contenzioso.

Metodo di distruzione

I documenti di livello I sono quelli che contengono informazioni di massima sicurezza e riservatezza e quelli che includono dati personali. Questi documenti devono essere smaltiti come rifiuti riservati (distrutti con un trita-carte e inceneriti) e/o devono essere sottoposti a cancellazione elettronica sicura. Lo smaltimento dei documenti deve includere la prova della distruzione.

I documenti di livello II sono documenti proprietari che contengono informazioni riservate quali nomi, firme e indirizzi delle parti o che potrebbero essere utilizzati da terzi per commettere frodi, ma che non contengono dati personali. I documenti devono essere triturati e quindi collocati in bidoni dell'immondizia chiusi per essere raccolti da una ditta di smaltimento autorizzata, e i documenti elettronici saranno soggetti a cancellazione elettronica sicura.

I documenti di livello III sono quelli che non contengono informazioni riservate o dati personali e sono documenti pubblicati. Questi dovrebbero essere tagliati in strisce da un trita-carte o eliminati tramite una società di riciclaggio e includono, tra le altre cose, pubblicità, cataloghi, volantini e newsletter. Questi possono essere smaltiti senza una catena di controllo.

5. Gestione delle registrazioni sulla base di questo documento

Nome del documento	Persona responsabile dell'archiviazione	Controlli per la protezione del documento	Tempo di archiviazione
Modulo di Consenso dell'Interessato	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Recesso dell'Interessato	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni

Modulo di Consenso dei Titolari della Responsabilità Genitoriale	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Modulo di Recesso dei Titolari della Responsabilità Genitoriale	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso ai moduli	10 anni
Accordi con i Fornitori del Trattamento dei Dati	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso alla cartella	10 anni dopo la scadenza del contratto
Registro delle Informative sulla Privacy	Il Responsabile della Protezione dei Dati	Soltanto le persone autorizzate possono avere accesso alla cartella	Permanente

6. Validità e gestione del documento

Questo documento ha effetto dal 01/06/2020.

Il responsabile per questo documento è il Responsabile della Protezione dei Dati, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.