POLITICA DI CONSERVAZIONE DEI DATI

Revisione	DOCUMENTO INIZIALE
Data di revisione	22 MAGGIO 2018
Redatto da	LINDA GIACOMUZZI
Approvato da	CONSIGLIO DI AMMINISTRAZIONE

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 di Aegis Fiduciaria Srl (da ora in avanti "Società").

La presente politica si applica a tutte le unità, i processi e i sistemi in tutti i paesi in cui la Società svolge la sua attività e intrattiene rapporti commerciali o di altro tipo con terzi.

La presente Politica si applica a tutti i funzionari, amministratori, dipendenti, collaboratori, consulenti, procuratori o fornitori di servizi della Società 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 la Società. 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);
- Legislazione nazionale in materia di privacy e provvedimenti del Garante per la protezione dei dati personali;
- Politica sulla Protezione dei Dati Personali.

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 salvo diversamente previsto dalla legge applicabile, il periodo di conservazione richiesto per tale documento sarà considerato 10 dalla data di creazione del documento.

3.2. Programma di Generale 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 possono essere prolungati qualora si renda necessario:

- a fronte di indagini da parte delle competenti autorità;
- qualora si renda necessario per esigenze di tutela legale della Società.

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 DPO, che vi provvede dando specifiche istruzioni al personale addetto alla privacy ed al Responsabile IT.

3.4. Distruzione dei dati

La Società e i suoi dipendenti dovrebbero quindi, su base regolare, riesaminare tutti i dati, siano essi detenuti elettronicamente sul loro dispositivo 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 DPO, che vi provvede vigilando il corretto adempimento di ciò da parte del personale addetto alla privacy.

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.

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 interno o esterno che il DPO subappalta a tale scopo.

Devono essere predisposti controlli adeguati che impediscano la perdita permanente delle informazioni essenziali della Società a seguito di distruzione intenzionale o involontaria delle informazioni.

3.5. Violazione, Misure di Attuazione e Conformità

La persona incaricata della protezione dei dati (DPO) ha la responsabilità di garantire che ciascuno degli uffici della Società rispetti questa Politica. È anche responsabilità del DPO riscontrare le eventuali richieste del Garante per la protezione dei dati personali.

Qualsiasi sospetto di violazione di questa Politica deve essere immediatamente segnalato al DPO. 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, la perdita della fiducia del cliente, contenziosi e perdita di vantaggio competitivo, perdita finanziaria e danni alla reputazione dell'Azienda, 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 della Società, 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

4.1. 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 di riunioni quotidiane e altri eventi;
- Trasmissione di documenti quali lettere, copertine fax, messaggi e-mail ed elementi simili che accompagnano i documenti ma non aggiungono alcun valore;
- Moduli di messaggi;
- Elenco indirizzi, liste di distribuzione sostituiti ecc.;
- Curriculum ricevuti di personale non assunto o da assumere;
- Duplicati documenti come copie inviate per conoscenza o inoltrate per informazione, bozze inalterate, estratti da database e file temporanei;
- Riviste del settore, volantini e newsletter da fornitori o altre organizzazioni esterne.

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

4.2. Metodo di distruzione

I documenti che contengono dati personali devono essere smaltiti come rifiuti riservati (distrutti con un trita-carte) e devono essere sottoposti a cancellazione elettronica.

5. Validità e gestione del documento

Questo documento ha effetto dal 24 maggio 2018.

Il responsabile per questo documento è il DPO, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale, e sottoporlo all'approvazione del CDA che è il responsabile ultimo della conformità dell'Azienda alla normativa sul GDPR.

6. Allegati

- Allegato – Programma di Conservazione dei Dati