Metronotte S.r.l.

Via Martino Cilestri, 41

95129 Catania

POLITICA DI CONSERVAZIONE DEI DATI

Codice:	GDPR/4
Revisione:	0
Data di creazione:	8/7/2018
Redatta da:	S.G.R. Consulting S.r.l.
Approvata da:	
Livello di Riservatezza:	Medio

Cronologia delle revisioni

Data	Revisione	Creata da	Descrizione della modifica

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 di Metronotte S.r.l. (da ora in avanti "L'Azienda").

La presente politica si applica a tutte le unità aziendali, i processi e i sistemi in tutti i paesi in cui l'Azienda svolge attività commerciali e intrattiene rapporti commerciali 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 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)
- 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 in particolare nel Programma di Conservazione dei Dati) e salvo diversamente previsto dalla legge applicabile, il periodo di conservazione richiesto per tale documento sarà considerato 5 (cinque) 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 all'interno del Programma di Conservazione dei Dati possono essere prolungati in casi quali:

- Indagini in corso da parte delle autorità degli Stati Membri, se esiste la possibilità che i dati personali siano necessari all'Azienda per dimostrare la conformità con i requisiti legali; o
- 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 dei Sistemi Informativi.

3.4. Distruzione dei dati

L'Azienda e i suoi dipendenti devono, 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 su Amministrazione per i documenti cartacei e su Sistemi Informativi per i dati elettronici.

Una volta presa la decisione di smaltirli secondo il Programma di Conservazione, i dati devono 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 esterno che il Responsabile degli Acquisti appalta a tale scopo. Devono essere rispettate tutte le disposizioni generali applicabili ai sensi delle leggi sulla protezione dei dati e la 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.

3.5. Violazione, Misure di Attuazione e Conformità

Il Responsabile della Protezione dei Dati ha la responsabilità di garantire che ciascuno degli uffici dell'Azienda rispetti questa Politica. È anche sua responsabilità assistere 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.

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

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:

- Annunci e comunicazioni di riunioni quotidiane e altri eventi, comprese le accettazioni e le scuse;
- Richieste di informazioni ordinarie come le indicazioni di viaggio;
- 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;
- Pubblicazioni interne di magazzino che sono obsolete o sostituite;
- Riviste del settore, cataloghi di venditori, volantini e newsletter da fornitori o altre organizzazioni esterne.

4.2. 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 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 aziendali 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	Luogo di archiviazione	Persona responsabile dell'archiviazione	Controlli per la protezione del documento	Tempo di archiviazione
Programma di Conservazione dei Dati	Google Drive percorso GDPR/Metronotte S.r.l.	il Responsabile della Protezione dei Dati	Solo le persone autorizzate possono accedere a questo documento	Permanente

6. Validità e gestione del documento

Questo documento ha effetto dal 8/7/2018

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.

7. Allegati

- Allegato – Programma di Conservazione dei Dati

Vito Giunta

_____