01.CP_05 - Politica per la protezione dei dati e la privacy

Principi di Protezione dei Dati

Archiva è attenta al trattamento dei dati personali nel rispetto delle proprie responsabilità ai sensi del Regolamento (UE) 2016/679 (GDPR) e di altri requisiti normativi applicabili. L'articolo 5 del GDPR richiede che i dati personali siano:

1. trattati in modo lecito, corretto e trasparente nei confronti delle persone fisiche;
2. raccolti per finalità determinate, esplicite e legittime e non ulteriormente trattati in modo incompatibile con tali finalità; l'ulteriore trattamento per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. esatti e, ove necessario, aggiornati; deve essere adottata ogni misura ragionevole per garantire che i dati personali inesatti, rispetto alle finalità per le quali sono trattati, siano cancellati o rettificati senza indugio;
5. conservati in una forma che consenta l'identificazione degli interessati per il tempo necessario alle finalità per le quali i dati personali sono trattati; i dati personali possono essere conservati per periodi più lunghi nella misura in cui i dati personali saranno trattati esclusivamente per finalità di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici previa attuazione delle misure tecniche e organizzative adeguate previste dal GDPR al fine di salvaguardare i diritti e le libertà degli individui;
6. trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e da perdite, distruzioni o danni accidentali, utilizzando misure tecniche o organizzative adeguate.

Disposizioni generali

La presente Politica aziendale si applica a tutti i dati personali trattati da Archiva S.r.l.
Le funzioni aziendali a cui è assegnata la responsabilità in materia di Data Protection e Privacy, come evidenziato nell'organigramma Data protection, si assumono la responsabilità del costante rispetto da parte di Archiva della presente politica.
La presente politica deve essere riesaminata almeno una volta all'anno.

Trattamento lecito, equo e trasparente

Al fine di garantire che il trattamento dei dati sia lecito, corretto e trasparente, Archiva mantiene un registro ai sensi del GDPR, art. 30.;
Il citato registro deve essere rivisto almeno una volta all'anno (al riguardo si veda la specifica procedura POA.DP.01 - Creazione e aggiornamento del registro delle attività di trattamento del Titolare;
Le persone fisiche hanno il diritto di accedere ai propri dati personali: i diritti previsti dagli artt. da 15 a 21 del GDPR e le eventuali ulteriori richieste rivolte ad Archiva dovranno essere evase con tempestività e comunque entro 30 giorni secondo quanto previsto dalla procedura POA.DP.02 - Esercizio dei diritti dell'interessato (ex artt. 15-22 Reg. UE 2016/679).

Basi giuridiche del trattamento

1. Tutti i trattamenti effettuati da Archiva devono essere fondati su una delle seguenti basi legali:
   a. consenso dell'interessato;
   b. contratto di cui l'interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dell'interessato;
   c. adempimento di un obbligo legale al quale è soggetto il Titolare del trattamento
   d. salvaguardia di interessi vitali dell'interessato;
   e. esecuzione di un compito pubblico di interesse pubblico di cui è investito il Titolare del trattamento;
   f. perseguimento del legittimo interesse del Titolare del trattamento;
2. Archiva annoterà la base giuridica appropriata nel Registro dei trattamenti, ove applicabile;
3. laddove si faccia affidamento sul consenso come base legale per il trattamento dei dati, la prova del rilascio del consenso deve essere conservata con i dati personali;
4. laddove le comunicazioni siano inviate alle persone sulla base del loro consenso, deve essere chiaramente indicata la possibilità per la persona di revocare il proprio consenso e devono essere predisposti sistemi per garantire tale revoca.

Misure tecniche ed organizzative (TOM)

Devono essere implementate adeguate misure tecniche e organizzative tenendo conto delle finalità del trattamento, dello stato della tecnologia e dei costi di attuazione.
La descrizione delle TOMs si basa sulla struttura dello SoA (Statement of Applicability) sviluppato da Archiva nell'ambito dell'implementazione della certificazione ISO/IEC 27001, tenendo conto anche della ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 e altri standard di livello internazionale.
Queste TOMs includono i seguenti ambiti (quindi non sono limitate agli stessi):

1. Riconoscimento dei diritti degli interessati;
2. Controllo di accesso;
3. Classificazione delle informazioni (e trattamento delle stesse);
4. Sicurezza fisica e ambientale per gli utenti finali:
   a. uso accettabile del bene;
   b. dispositivi mobili e telelavoro;
   c. limitazione dell'installazione e dell'utilizzo del software;
5. Backup dei dati;
6. Trasferimento di informazioni;
7. Protezione contro malware;
8. Gestione delle vulnerabilità tecniche;
9. Misure crittografiche;
10. Sicurezza delle comunicazioni;
11. Privacy e protezione dei dati personali;
12. Formazione e sensibilizzazione;
13. Rapporti con i fornitori.

Questo documento non può essere duplicato o diffuso senza l'esplicito consenso scritto di Archiva S.r.l. Qualsiasi divulgazione, anche parziale, delle informazioni contenute nel presente documento che non sia stata preventivamente autorizzata da Archiva S.r.l. può costituire una violazione di legge. Per qualsiasi richiesta, si prega di contattare ciso@archivagroup.it.