

# Politica per la protezione dei dati e la privacy

01.CP\_05 - 19/06/2024

## 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

1. la presente Corporate policy si applica a tutti i dati personali trattati da Archiva Srl a socio unico ed è destinata a tutte le società appartenenti al gruppo Archiva.
2. i ruoli aziendali con responsabilità assegnata in materia di protezione dei dati e della privacy, come indicato nell'organigramma della privacy, si assumono la responsabilità della costante osservanza da parte di Archiva della presente informativa
3. la presente politica sarà riesaminata almeno annualmente;

## Trattamento lecito, equo e trasparente

1. per garantire che il trattamento dei dati sia lecito, equo e trasparente, Archiva mantiene un registro ai sensi dell'art. 30 del GDPR. 30.;
2. il registro di cui sopra sarà rivisto almeno una volta all'anno;
3. le persone fisiche hanno il diritto di accedere ai propri dati personali: i diritti previsti dal GDPR agli articoli da 15 a 21 e ogni ulteriore richiesta fatta ad Archiva sarà evasa in modo tempestivo e comunque entro 30 giorni.

## Scopi leciti

1. Tutti i trattamenti effettuati da Archiva devono essere effettuati su una delle seguenti basi legali:
  - a. consenso;
  - b. contratto;
  - c. obbligo legale;
  - d. interessi vitali;
  - e. compito pubblico, o
  - f. interessi legittimi.
2. Archiva annoterà la base legittima appropriata nel Registro del trattamento, quando applicabile;
3. Qualora il consenso sia invocato come base legittima per il trattamento dei dati, la prova del consenso opt-in deve essere conservata insieme ai dati personali.
4. Quando le comunicazioni sono inviate a individui sulla base del loro consenso, l'opzione per l'individuo di revocare il proprio consenso deve essere chiaramente indicata e devono essere predisposti sistemi per garantire tale revoca.

## Misure tecniche e organizzative esistenti (TOM)

Misure tecniche e organizzative adeguate, implementate e documentate, tenendo conto dello scopo del trattamento, dello stato della tecnologia e dei costi di implementazione.

La descrizione dei TOM implementati si basa sulla struttura del SoA (Statement of Applicability) sviluppato da Archiva durante l'implementazione della certificazione ISO/IEC 27001, tenendo conto di ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 e altri standard di livello mondiale.

Questi TOM includono, ma non si limitano a:

1. Prevedere i diritti delle persone interessate;
2. Controllo dell'accesso;
3. classificazione delle informazioni (e relativa gestione);
4. Sicurezza fisica e ambientale per gli utenti finali, come ad esempio:
  - Uso accettabile delle risorse;
  - Dispositivi mobili e telelavoro;
  - Limitazione dell'installazione e dell'utilizzo di software;
5. Backup dei dati;
6. Trasferimento di informazioni;
7. Protezione contro il malware;
8. Gestione delle vulnerabilità tecniche;
9. Misure crittografiche;
10. Sicurezza delle comunicazioni;
11. Privacy e protezione delle informazioni personali;
12. Formazione e consapevolezza;
13. Rapporti con i fornitori.

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