01.CP_05 - Data protection & Privacy policy

Version 25/07/2024

Data protection principles

Archiva is committed to processing data in accordance with its responsibilities under the Regulation (EU) 2016/679 (GDPR) and other applicable normative requirements. Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

General provisions

1. this Corporate policy applies to all personal data processed by Archiva Srl a socio unico and is intended for all the companies belonging to Archiva's group.
2. the company roles with assigned responsibility in Data Protection and Privacy, as pointed out in the Privacy organizational chart, shall take responsibility for Archiva's ongoing compliance with this policy
3. this policy shall be reviewed at least annually;

Lawful, fair and transparent processing

1. to ensure its processing of data is lawful, fair and transparent, Archiva maintain a registry as per GDPR, Art. 30.;
2. the mentioned register shall be reviewed at least annually;
3. individuals have the right to access their personal data: the rights expected by GDPR articles from 15 to 21 and any further requests made to Archiva shall be dealt with in a timely manner and in any case within 30 days.

Lawful purposes

1. All processing performed by Archiva must be done on one of the following lawful bases:
   a. consent;
   b. contract;
   c. legal obligation;
   d. vital interests;
   e. public task, or;
   f. legitimate interests.
2. Archiva shall note the appropriate lawful basis in the Processing Register when applicable;
3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
4. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent shall be clearly pointed-out and systems shall be in place to ensure such revocation.

Existing Technical and Organisational Measures (TOM)

Appropriate technical and organizational measures that are implemented and substantiated, taking into account, the purpose of the processing, the state of the technology and the implementation costs.
The description of the implemented TOMs is based on the structure of the SoA (Statement of Applicability) developed by Archiva while implementing the ISO/IEC 27001 certification, taking into account ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 and other world-class standards.
These TOMs includes but are not limited to:

1. Provision the rights of data subjects;
2. Access control;
3. Information classification (and handling thereof);
4. Physical and environmental-related security for end-users such as:
   - Acceptable use of asset;
   - Mobile devices and telecommuting;
   - Restriction of software installation and usage;
5. Data backup;
6. Information transfer;
7. Protection against malware;
8. Handling technical vulnerabilities;
9. Cryptographic measures;
10. Communication security;
11. Privacy and protection of personal information;
12. Training and awareness;
13. Supplier relationships.