Data Protection Policy (SP 012)

April 2018

Version 1

AIRCO Refrigeration & Air Conditioning Ltd
Head Office: Airco House, Goulton Street, Hull, HU3 4DL, Tel: 0870 200 37 37 Fax: 01482 229997

1. Introduction

Airco is committed to the processing of data in compliance with General Data Protection Regulations (GDPR). This Policy sets forth the basic principles by which the Company processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

2. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

3. General provisions

a. This policy shall be reviewed at least annually.
b. Airco shall maintain registration with ICO as a data processor

4. Basic Principles

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*."

4.1 Lawfulness, Fairness, and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.2 Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3 Data Minimization

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps 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 in a timely manner.

4.5 Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.

4.6 Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Company must use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

4.7 Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

5. Data Retention and Removal/Disposal

To ensure that this data is not kept for longer than necessary, a backup and archiving plan will be maintained with our IT support contractors in accordance with the following schedule:

Financial Records

Personal Data Category	Mandated Retention Period	Record Owner
Payroll Records	Seven years after audits	Finance
Supplier Contracts	Seven years after contract termination	Finance
Chart of Accounts	Permanent	Finance
Fiscal Policies and Procedures	Permanent	Finance
Permanent Audits	Permanent	Finance
Financial Statements	Permanent	Finance
General Ledger	Permanent	Finance
Investment Records (Deposits, earnings, withdrawals)	7 Years	Finance
Invoices	7 Years	Finance
Cancelled Checks	7 Years	Finance
Bank Deposit Slips	7 Years	Finance
Business Expenses Documents	7 Years	Finance
Check Registers/Books	7 Years	Finance
Property/Asset Inventories	7 Years	Finance
Credit Card Receipts	3 Years	Finance
Petty Cash Receipts/Documents	3 Years	Finance

Business Records

Personal Data Category	Mandated Retention Period	Record Owner
Article of Incorporation to apply for corporate status	Permanent	Finance
Board Policies	Permanent	Finance
Board Meeting Minutes	Permanent	Finance
Tax or Employee Identification Number Designation	Permanent	Finance
Office and Team Meeting Minutes	Permanent	Finance
Annual Corporate Filings	Permanent	Finance

HR: Employee Records

Personal Data Category	Mandated Retention Period	Record Owner
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	7 Years	HR
Recruitment Documentation (Applications, interview notes etc)	Deleted immediately following appointment	HR
Payroll input forms, wages/salary records, overtime/bonus payments, payroll sheets	7 Years	HR & Finance
Bank details	Duration of employment	HR & Finance
Payrolls/wages	Duration of employment	Finance
Job History including staff personal records	Per legal requirements – May be required for the purpose of tendering	HR
Employee address details	Durations of employment	HR & Finance
Expense claims	Per legal requirement	HR
Annual leave records	Duration of employment	HR
Accident books & Reports (including correspondence)	Per legal requirement	HR
Parental leave	Duration of employment	HR
Maternity pay records and calculations	3 Years after the end of the tax year in which the maternity period ends	HR & Finance
Training and development records	Duration of employment	Training Matrix Manager

Contracts

Personal Data Category	Mandated Retention Period	Record Owner
Signed	Permanent	Finance
Contracts	Permanent	Finance
Successful tender documents	Permanent	Sales
Unsuccessful tender's documents	Permanent	Sales
Tender – user requirements, specification, evaluation criteria, invitation	Permanent	Sales
Contractors' Reports	Permanent	Finance
Operation and monitoring, e.g complains	Permanent	Quality Manager

Customer Data

Personal Data Category	Mandated Retention Period	Record Owner
Platform data – inclusive of video data, comments, attachments, profile picture, email address, first and second name	Retained whilst a customer. Removed upon request within 9 months	Customer
CRM Data (Name, email, mobile number, address, emails, phone call summaries)	Retained whilst a customer. Removed upon request within 9 months	Departmental
Metrics	Retained whilst a customer. Removed upon request within 9 months	Departmental

Non-Customer Data

Personal Data Category	Mandated Retention Period	Record Owner
Name, email address, number	Retained until the person unsubscribes or requests to be removed	Sales

IT

Personal Data Category	Mandated Retention Period	Record Owner
Recycle Bins	Cleared monthly	Individual
Downloads	Cleared monthly	Individual
Inbox	3 Years (if containing personal information)	Individual
Deleted Emails	Cleared monthly	Individual
Personal Network Drive	Review quarterly with any documents containing personal information deleted after 3 years	Individual
Local Drives & Files	Moved to network drive monthly then deleted from local drive	Individual
Google Drive, drop box	Review quarterly with any documents containing personal information deleted after 3 years	Individual

5.1 Destruction Method

Airco and its employees shall, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document.

Level 1 documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Level 2 documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Level 3 documents are those that do not contain any confidential information or personal data and are published Company documents. These should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

6. Security

To ensure that data is secured as necessary, data will be stored electronically in folders that are restricted with security groups which only permit those with a requirement to process the data access. Any hard copy forms of data will be kept under lock and key with the individual responsible for the data.

7. Breach

In the event of a breach or suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Airco shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

Signature		**Signature**	
Name	**Neil Fisher**	**Name**	**Nick Oxtoby**
Position	**Managing Director**	**Position**	**Operations Director**
Date	**04/04/2018**	**Date**	**04/04/2018**