

DATA PROTECTION POLICY

General Statement

Arboricare Limited is committed to protecting the rights and freedoms of clients, customers and employees by safely controlling and processing their data in accordance with all our legal obligations under the General Data Protection Regulation (GDPR).

Scope & Definition

We hold personal data about our employees, clients and other individuals for a variety of business purposes as follows:

Business Purposes – Means personal data which may be used by Business Name for:

- Personnel, administrative, financial, regulatory, payroll, and training purposes

Personal Data - Means any information relating to a person as categorised to include;

- **Client / Customer / Suppliers:** Address, phone numbers, email address.
- **Suppliers:** Address, phone numbers, email address, financial details (payment)
- **Employees:** Address, phone numbers, email address, educational background, financial details (payroll), qualifications, nationality and job history.

Special Categories of Personal Data - Includes;

- **Employees:** Physical or mental health, criminal offences.

General Policy Principles

Arboricare Ltd makes every effort to comply with the following principles:

- To be lawful, fair, respectful and act with consent
- To be transparent
- To collect minimum data and only for a specific purpose
- To be accurate and up to date
- To store data only until necessary
- To ensure data is stored and disposed of safely and securely

This policy sets out how Arboricare Limited will protect personal data and will ensure that its employees, sub-contractors and suppliers understand the rules governing their use of the personal data to which they have access in the course of their work.

- Where appropriate the individual is made aware of a privacy notice at the time of collecting the personal data.
- No third parties will be used for collecting or processing personal data.
- Client or customer data is only used for this business's marketing purposes having gained consent first.
- The business will **NOT** pass customer data to third parties for marketing purposes.
- The business as an employer will ensure that all personal data is stored in a safe, secure and lawful way.

Arboricare Limited

- Any printed data will be shredded or destroyed securely when no longer needed.

Responsibilities

The levels of responsibility for data protection are as follows:

- The directors of Arboricare Limited have overall responsibility for compliance with GDPR.
- Caroline Bedford is the Data Protection Officer and has day to day responsibility for compliance, ensuring all employees, sub-contractors and third parties service suppliers with controlled data access are aware of their obligations.
- Employees, Sub-contractors and third party service suppliers e.g. IT, H&S, HR, are aware of their responsibility and abide by this policy.

Rights of Individuals

- Right to be informed – *their data has been collected and for what purpose.*
- Right of access – *to their data.*
- Right to rectification – *to know their data is accurate & rectify mistakes.*
- Right to erase and be forgotten – *to ensure data is erased securely on request and when we no longer need it.*
- Right to restrict processing – *to know it is only used for the stated purposes.*
- Right to data portability – *to make personal data held available to the individual on request in a format they can handle.*
- Right to object – *to the use of personal data*
- Rights in relation to automated decision making and profiling – *Does not apply to this business*

Signed



Date 10/07/2018

Position: Company Secretary

Review Log & Revisions Record

	Additions / Revisions Made	Date	Made By
01	Issued as Draft	01/04/18	AML
02	Data Processing Officer changed to Data <u>Protection</u> Officer, added email footer text.	18/06/18	AML

Client / Customer Personal Data

Data Held	Purpose	Format	Security
Name, address, phone, email	Business correspondence, appointments, quotes, estimates, invoicing, statutory permissions.	Customer Database (Digital) – Electronic Documents	Digital - Firewall & Anti-Virus Software. Computers are password protected
	Issued to team leaders to progress works	Printed Job Sheets	Hardcopy - Personally assigned to an individual. Returned to the office.
Quote Information – Value of the work, work history	Invoicing & Future Work Specification.	Digital & Printed Quote Sheets	Archived securely
Property Information – security codes, gate codes, vacation dates.	To allow access when work is authorised.	Digital & Printed on Job Sheets	Destroy Date

Precautions:

1. GDPR Statement on the website & email footer.
2. Training given to Managers and Employees regarding data protection.
3. Customer Invoices provide opportunity to be 'forgotten'.
4. Customer Satisfaction Questionnaire provides opportunity to be forgotten or to be contacted by the business in the future.

Employee Personal Data

Data Held	Purpose	Format	Security
Name, address, phone, email	Correspondence.	Digital – Payroll software, spreadsheets, documents	Digital - Firewall & Anti-Virus Software. Computers are password protected
		Hard Copy Personnel Files	Hard Copy - Secured Filing Cabinet Archive & Destroy Dates
Financial Details / NI Number / Terms of Employment	Payroll, Tax & Employment	Digital – Payroll software, spreadsheets, documents	Digital - Firewall & Anti-Virus Software. Computers are password protected
		Hard Copy Personnel Files	Hard Copy - Secured Filing Cabinet Archive & Destroy Dates
Education & Certification	Employment & Third Party Compliance	Hard Copies	Secured Filing Cabinet
		Scanned Copies*	Firewall & Anti-Virus Software. Computers are password protected

Arboricare Limited

Precautions:

1. Third Party Service Providers are checked and have adequate GDPR compliant procedures in place.
2. Certification with personal data is not passed to outside agencies unless employee consent has been given, the data is necessary, the agency can demonstrate compliance with GDPR and the records will be destroyed once they are no longer used.

Employee Personal Data – Special Category

Data Held	Purpose	Format	Security
Occupational health information	Compliance with H&S Legislation, Monitoring employee health.	Hard Copy – Questionnaires & Declarations. Medical Notes Scanned Copies Digital Register of OHS	Secured Filing Cabinet with specified access. System Firewall. Computers are password protected Archive & Destroy Dates
Criminal Records (DBS)	Required for authorised entry on specific sites.	Hardcopy	Secured Filing Cabinet with specified access. Archive & Destroy Dates
Accident Reports	Compliance with H&S Legislation.	Hard Copy Reports	Secured Filing Cabinet with specified access. Archive & Destroy Dates

Precautions:

1. Third Party Service Providers are checked and have adequate GDPR compliant procedures in place.
2. Certification with personal data is not passed to outside agencies unless employee consent has been given, the data is necessary, the agency can demonstrate compliance with GDPR and the records will be destroyed once they are no longer used.