Internal Privacy and Data Usage Policy

Introduction

Alcema, Alcema Construction, Alcema Fire Safety & Alcema Services Limited is committed to protecting the rights and freedoms of Data Subjects and safely and securely processing their Personal Data in accordance with all of our legal obligations.

We hold Personal Data about our employees, certain clients, suppliers and other individuals for a variety of business purposes.

This Policy sets out how we seek to protect Personal Data and ensure that our staff understand the rules governing their use of the Personal Data to which they have access in the course of their work.

In particular, this Policy requires staff to ensure that relevant compliance steps are addressed before any materially new Personal Data processing activity is initiated.

Definitions

Business Purposes	The purposes for which Personal Data may be used by us is as follows: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice;* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests;* - *Ensuring business policies are adhered to (such as policies covering email and internet use);* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking;* - *Investigating complaints;* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments;* - *Monitoring staff conduct, disciplinary matters;* - *Marketing our business; or* - *Improving services.*
Data Protection Legislation	means, without limitation and where applicable, the Data Protection Act 2018 (**DPA 2018**); the UK General Data Protection Regulation (Retained Regulation (EU) 2016/679) (**UK GDPR**); the General Data Protection Regulation (EU) 2016/679 (**EU GDPR**); the Privacy and Electronic Communication (EC Directive) Regulations 2003 (**PECR**); and any other applicable data protection and privacy laws, regulations, guidance, rules, requirements, directions, guidelines, recommendations, advice, codes of practice, policies, measures, or publications of the Information Commissioner's Office, or other relevant regulator or industry body, in each case in any relevant jurisdiction(s) from time to time and the equivalent in any other relevant jurisdictions, all as amended or replaced from time to time.
Personal Data	means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one 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.

	Personal Data we gather may include: an individual's phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Senior Leadership	means the senior management team, of which there are currently eight members.
Special Category Personal Data	means Personal Data revealing information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, or trade union membership (or non-membership); genetic and biometric data; and data concerning an individual's physical or mental health, sex life and/or sexual orientation. *Any use of Special Category of Personal Data should be strictly controlled in accordance with this Policy.*
Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
Data Processor	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
Processing (and process, processes, and processed shall be construed accordingly)	means any 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	means the national body responsible for data protection - the Information Commissioner's Office in the UK.

Scope

This Policy applies to all staff, who must be familiar with this Policy and comply with its terms.

This Policy addresses Alcema, Alcema Construction & Alcema Fire Safety Limited's approach and procedure to collection, use, disclosure, and retention of Personal Data relating to any natural persons and supplements our other policies relating to internet and email use. We may supplement or amend this Policy by additional policies and guidelines from time to time. Any new or modified Policy will be circulated to staff before being adopted.

Who is responsible for this Policy?

Our Administration Manager has overall responsibility for the day-to-day implementation of this Policy. You should contact them for further information about this Policy if necessary.

All staff are responsible for handling Personal Data in accordance with this Policy and must escalate any concerns or incidents without delay.

The Principles

Alcema, Alcema Construction, Alcema Fire Safety and Alcema Services Limited shall comply with the principles of data protection (the "**Principles**") enumerated in the UK GDPR. The Principles are:

1. Lawfulness, fairness, and transparency
Data collection must be fair, for a legal purpose and we must be open and transparent as to how the Personal Data will be used.

2. Limited for its purpose
Data can only be collected for a specific purpose.

3. Data minimisation
Any Personal Data collected must be necessary and not excessive for its purpose.

4. Accuracy
The Personal Data we hold must be accurate and kept up to date.

5. Storage limitation
We cannot store Personal Data longer than necessary.

6. Integrity and confidentiality
The Personal Data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all our use of Personal Data. We must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and with be reviewed by the Quality and Compliance Manager.

To comply with Data Protection Legislation, and the accountability and transparency Principle of the UK GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures;
- Maintain up to date and relevant documentation on all processing activities;
- Conducting Data Protection Impact Assessments;
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security and enhanced privacy procedures on an ongoing basis.

Our Procedures

Fair and lawful processing
We must process Personal Data fairly and lawfully in accordance with individuals' rights under the first Principle. Personal Data will only be processed where there is a valid lawful basis under Data Protection Legislation. In most cases this will be because the processing is necessary to perform a contract, comply with a legal obligation, or pursue the organisation's legitimate interests. Consent will only be relied upon where it is appropriate, freely given and capable of being withdrawn without detriment.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data Subjects have the right to have any Personal Data unlawfully processed erased.

Controlling vs. processing Personal Data
Alcema, Alcema Construction & Alcema Fire Safety Limited is classified as a Data Controller for the Personal Data referenced .

Lawful basis for processing Personal Data

We must establish a lawful basis for processing Personal Data and ensure that any Personal Data we are responsible for managing has a written lawful basis in compliance with the Regulations. It is our responsibility to check the lawful basis for any Personal Data we are working with and ensure all of our actions comply the lawful basis. At least one of the following conditions must apply whenever we process Personal Data:

1. **Consent**
   We hold recent, clear, explicit, and defined consent for the individual's Personal Data to be processed for a specific purpose.

2. **Contract**
   The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**
   We have a legal obligation to process the Personal Data (excluding a contract).

4. **Legitimate interests**
   The processing is conducted pursuant to our legitimate interests. This condition does not apply if there is a good reason to protect the individual's Personal Data which overrides the legitimate interest.

Deciding which condition to rely on

If we are making an assessment of the lawful basis, we must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and we should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the Personal Data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the Personal Data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the Data Subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose Personal Data is being processed by us are informed of the lawful basis for processing their Personal Data, as well as the intended purpose. This should occur via our Privacy Notice. This applies whether we have collected the Personal Data directly from the individual, or from another source.

Special Category Personal Data

Special Category Personal Data is data about an individual which is more sensitive, so requires more protection (see the Definitions for more detail). This type of Personal Data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

In most cases where we process Special Category Personal Data we will require the Data Subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant Special Category Personal Data is, why it is being processed, and to whom it will be disclosed.

The condition for processing Special Category Personal Data must comply with the law. If we do not have a lawful basis for processing Special Category Personal Data, that processing activity must cease.

Responsibilities

Our responsibilities:

- Analysing and documenting the type of Personal Data we hold;
- Checking procedures to ensure they cover all the rights of the individual;
- Identify the lawful basis for processing Personal Data;
- Ensuring consent procedures are lawful;
- Implementing and reviewing procedures to detect, report and investigate Personal Data breaches;
- Storing Personal Data in safe and secure ways;
- Assessing the risk that could be posed to individual rights and freedoms should Personal Data be compromised;
- Fully understanding our data protection obligations;
- Checking that any data processing activities we are dealing with comply with our Policy and are justified;
- Not using Personal Data in any unlawful way;
- Not storing Personal Data incorrectly, being careless with it or otherwise causing us to breach Data Protection Legislation and our policies through our actions;
- Complying with this Policy at all times; and
- Raising any concerns, notifying of any breaches or errors, and reporting anything suspicious or contradictory to this Policy or our legal obligations without delay.

Responsibilities of the Quality & Compliance Manager:

- Keeping Senior Leadership updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;
- Arranging data protection training and advice for all staff members and those included in this Policy;
- Answering questions on data protection from staff, Senior Leadership and other stakeholders;
- Responding to individuals such as clients and employees who wish to know which Personal Data is being held on them by us; and
- Checking and approving any contracts or agreements regarding data processing with third parties that handle Personal Data that the company holds.

Responsibilities of the IT Consultancy:

- Ensure all systems, services, software and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly to ensure it is functioning properly; and
- Researching third-party services, such as cloud services the company is considering using to store or process Personal Data.

Responsibilities of the Account Executive:

- Approving data protection statements attached to emails and other marketing copy;
- Addressing data protection queries from clients, target audiences or media outlets; and
- Coordinating with the QC Manager to ensure all marketing initiatives adhere to Data Protection Legislation and the company's Privacy Notice.

Accuracy and relevance

We will ensure that any Personal Data we process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. We will not process Personal Data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate Personal Data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform our QC Manager.

Data security

We must keep Personal Data secure against loss or misuse. Where other organisations process Personal Data as a service on our behalf, the QC Manager will establish what, if any, additional specific data security arrangements need to be implemented in contracts/ agreements with those third-party organisations.

Storing Personal Data securely

- In cases when Personal Data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed Personal Data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- The Managing Director must approve any cloud used to store Personal Data.
- Servers containing Personal Data must be kept in a secure location, away from general office space.
- Data should be regularly backed up in line with the company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing Special Category Personal Data must be approved and protected by security software.
- All possible technical measures must be put in place to keep Personal Data secure.

Data retention

Personal Data will be retained only for as long as necessary and in line with the organisation's Data Retention Schedule and applicable legal requirements.. What is necessary will depend on the circumstances of each case, taking into account the reasons that the Personal Data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring Personal Data outside of the UK

There are restrictions on transfers of Personal Data outside of the UK. You must not transfer Personal Data outside of the UK, or anywhere else outside of normal rules and procedures, without express permission from the Managing Director. If Personal Data is permitted to be transferred outside of the UK under this paragraph then an international data transfer agreement may be required.

Any international data transfer must be subject to an appropriate risk assessment and supported by suitable safeguards, such as an International Data Transfer Agreement or adequacy decision.

Rights of Individuals

Individuals have rights to their Personal Data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- By providing Privacy Notices which are concise, transparent, intelligible, easily accessible, free of charge and that are written in clear and plain language.
- By keeping a record of how we use Personal Data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- By enabling individuals to access their Personal Data and supplementary information.
- By allowing individuals to be aware of and verify the lawfulness of the processing activities.

3. Right to rectification

- We must rectify or amend the Personal Data of a Data Subject where it is inaccurate or incomplete, if requested.
- This must be done without delay, and no later than one calendar month from the request.

4. Right to erasure

- We must delete or remove an individual's Personal Data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of Personal Data.
- We are permitted to store Personal Data if it has been restricted, but not process it further. We must retain enough Personal Data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their Personal Data so that they can re-use it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another Data Controller if requested.

7. Right to object

- We must respect the right of an individual to object to the processing of their Personal Data based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their Personal Data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy Notices

When to supply a Privacy Notice

A Privacy Notice must be supplied at the time Personal Data is obtained if obtained directly from a Data Subject. If the Personal Data is not obtained directly from the Data Subject, the Privacy Notice must be provided within a reasonable period of having obtained the Personal Data, which means within one month.

If the Personal Data is being used to communicate with the individual, then the Privacy Notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the Privacy Notice must be supplied prior to the Personal Data being disclosed.

What to include in a Privacy Notice

Privacy Notices must be concise, transparent, intelligible, and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a Privacy Notice to all Data Subjects:

- The purpose of processing the Personal Data and the lawful basis for doing so;
- The legitimate interests of the Data Controller or third party, if applicable;
- The right to withdraw consent at any time, if applicable;
- The category of the Personal Data (only for Personal Data not obtained directly from the Data Subject);
- Any recipient or categories of recipients of the Personal Data;
- Detailed information of any transfers to third countries and safeguards in place;

- The retention period of the Personal Data or the criteria used to determine the retention period, including details for the data disposal after the retention period;
- The right to lodge a complaint with the ICO, and internal complaint procedures;
- The source of the Personal Data, and whether it came from publicly available sources (only for Personal Data not obtained directly from the Data Subject);
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the Data Subject; and
- Whether the provision of Personal Data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the Personal Data (only for Personal Data obtained directly from the Data Subject).

Subject Access Requests

All Subject Access Requests must be handled in accordance with the organisation's Subject Access Request procedure. Staff must notify the Quality and Compliance Manager immediately upon receipt of any request.

What is a subject access request?

An individual has the right to receive confirmation that their Personal Data is being processed, access to their Personal Data and supplementary information which means the information which should be provided in a Privacy Notice.

How we deal with subject access requests

We must provide an individual with a copy of the information request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide Data Subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of Personal Data, we can request the individual specify the information they are requesting.

Once a subject access request has been made, you must not change or amend any of the Personal Data that has been requested. Deleting the Personal Data could also be a criminal offence.

Data portability requests

We must provide the Personal Data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this Personal Data either to the individual who has requested it, or to the Data Controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month.

Right to Erasure

What is the right to erasure?

Individuals have a right to have their Personal Data erased and for processing to cease in the following circumstances:

- Where the Personal Data is no longer necessary in relation to the purpose for which it was originally collected and / or processed;

Where consent is withdrawn;

- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing;

- The Personal Data was unlawfully processed or otherwise breached Data Protection Legislation;
- To comply with a legal obligation; or
- The processing relates to a child.

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- The exercise or defence of legal claims.

If Personal Data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the Personal Data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their Personal Data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual; or
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the Privacy Notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract;
- Based on the individual's explicit consent; or
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing;
- Offer simple ways for them to request human intervention or challenge any decision about them; and
- Carry out regular checks and user testing to ensure our systems are working as intended.

Third Parties

Using third party controllers and processors

As a Data Controller, we must have written contracts in place with any third party Data Controllers (and/or) Data Processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a Data Controller, we must only appoint Data Processors who can provide sufficient guarantees under Data Protection Legislation, such as that the rights of Data Subjects will be respected and protected.

Contracts

Our contracts will aim to comply with the standards set out by the ICO and, where applicable for data transfers outside of the UK, follow the international data transfer agreement. Our contracts / agreements with Data Controllers (and/or) Data Processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of Personal Data and categories of Data Subject, and the obligations and rights of the Data Controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions;
- Those involved in processing the Personal Data are subject to a duty of confidence;
- Appropriate measures will be taken to ensure the security of the processing;
- Sub-processors will only be engaged with the prior consent of the Data Controller and under a written contract;
- The Data Controller will assist the Data Processor in dealing with subject access requests and allowing Data Subjects to exercise their rights under Data Protection Legislation;
- The Data Processor will assist the Data Controller in meeting its obligations under Data Protection Legislation in relation to the security of processing, notification of Personal Data Breaches, and implementation of Data Protection Impact Assessments;
- Delete or return all Personal Data at the end of the contract;
- Submit to regular audits and inspections, and provide whatever information necessary for the Data Controller and Data Processor to meet their legal obligations; and
- Nothing will be done by either the Data Controller or Data Processor to infringe on Data Protection Legislation.
-

Criminal Offence Personal Data

Criminal record checks

Any criminal record checks (i.e. the processing of criminal offence data) must be justified by law. It may be relevant for us to conduct criminal record checks on the basis of:

- Employment, social security and social protection; or
- Consent.

Do not conduct any criminal record checks without confirming a legal basis for the processing with the QC Manager.

We cannot keep a comprehensive register of criminal offence data.

Audits, Monitoring, and Training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must assist the company in conducting a regular data audit as required by the QC Manager and normal procedures.

Monitoring

Everyone must observe this Policy. The QC Manager has overall responsibility for this Policy. Alcema, Alcema Construction & Alcema Fire Safety Limited will keep this Policy under review and amend or change it as required. You must notify the QC Manager of any breaches of this Policy. You must comply with this Policy fully and at all times.

Training

You will receive adequate training on the provisions of Data Protection Legislation specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the QC Manager.

Reporting Breaches

Any breach of this Policy or of Data Protection Legislation must be reported as soon as practicably possible. This means as soon as you have become aware of a breach. Alcema, Alcema Construction & Alcema Fire Safety Limited has a legal obligation to report certain Personal Data Breaches to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary;
- Maintain a register of compliance failures; and
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures.

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our HR Policy Manual for our reporting procedure.

Failure to comply

We take compliance with this Policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this Policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this Policy, do not hesitate to contact the QC Manager.

Signed

Jason Spencer, Managing Director

Date: 12/03/2026

Review Date: 11/03/2027