Data Protection Policy

To comply with GDP Regulations

Data Protection Policy

Introduction

The General Data Protection Regulation (2016/679 EU) (GDPR) provides strict rules on what data can be held and how it should be gathered, processed, stored, deleted and rules regarding the free movement of personal data. Under the Regulation the Information Commissioner has powers to issue notices where data controllers and/or data processors have contravened any of the data protection principles. The main contraventions are likely to be unlawful reason for the collection of data, keeping data which is no longer required or where consent has been withdrawn/expired, unauthorised processing and/or disclosure of data. Failure to comply with such a notice is an offence under the legislation and could result in large fines.

In order to operate efficiently A1 Sheet Metal Flues Limited T/A A1 Flue Systems (the Company) needs to collect and process information about people, which may include past and present employees, past and present Directors, suppliers and clients.

The Company is committed to ensure that all personal data gathered is processed and managed in compliance with the General Data Protection Regulation. Every effort will be made to meet the obligations set out in legislation.

Scope

This policy applies to all employees, Directors, contractors and representatives working for or on behalf of the Company.

This policy applies to all personal data, including special categories and sensitive data, processed by the Company and applies to data both manually and electronically held. It also applies to personal data processed wholly or partially by automated means.

Images including CCTV footage, will also be covered by this policy.

Responsibilities

The Data Controller will have the overall responsibility to ensure compliance with GDPR. The Data Controller and the Data Processors will ensure the day-to-day activities of the Company comply with GDPR and are responsible for:

- Notifying individuals at the point of collection of how their personal data will be processed, stored, who will have access, accountability, the reason for processing and how long it will be used for.
- Ensuring that consent or reason for personal data processing is collected and are able to provide evidence upon request.
- Comply with subject data requests.
- Providing a central point for advice regarding data protection matters.
- Arranging appropriate data protection training.
- Keeping up to date with latest legislation and guidance regarding data protection.
- Ensuring adequate systems are in place to comply with this policy.

If any member of staff has any concerns regarding the policy, compliance with the regulations or suspects there has been a breach of the regulations they should report this to the Data Controller as soon as possible. The Data Controller will then complete their duties and record, report, deal and resolve the incident as necessary within the guidelines of GDPR. All breaches are required to be reported to the Supervisory Authority within 72 hours.

Definitions

Personal data

Information which relates to a living individual that is processed as data, which can be identified from the data. It also includes photographs, e-mail messages, IP addresses and data recorded by CCTV. It also covers data identified by reference numbers where a separate list can be used to match the reference numbers to named individuals.

Sensitive personal data

Personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs, (d) whether they are a member of a Trade Union, (e) their physical or mental health, (f) their sexual life, (g) the commission or alleged commission by them of any offence and (h) any proceedings for any offence committed or alleged to have been committed by them.

Processing data

Collecting, processing, storing, disclosing, access, or deletion of data.

Data controller

The person or organisation that is responsible for the manner and purpose in which personal data is processed along with ensuring compliance of GDPR.

Data processor/user

Any person that processes or uses the personal data on behalf of the Data Controller. Note that this is any third party who processes/uses data on behalf of the Company.

Restriction of processing

The marking of stored personal data with the aim of limiting their processing in the future.

Profiling

Any form of automated processing of personal data to evaluate certain personal aspects. An example could be during the shortlisting of candidates if this is done automatically.

Pseudonymisation

The processing of personal data that cannot be identified as a single individual without additional information.

Filing system

Means both electronic and manual filing systems.

Consent

Freely given, informed and unambiguous indication of the data subject's wishes by which they are providing their agreement for their personal data to be processed.

Data subject

Individual to whom the personal data relates.

Requirements

The GDPR stipulates that anyone processing personal data should comply to:

- Ensure data is processed lawfully, fairly and in a transparent manner to the data subject.
- Ensure data is collected for a specific, explicit and legitimate reason and not processed for any other reason than that given at time of collection.
- Ensure data is only held if there is a necessity to hold it (data minimisation).
- Ensure data is accurate and up to date. Steps should be taken to ensure accuracy and rectify or delete inaccurate records (accuracy).
- Ensure data is kept in a form which can identify the data subject for no longer than necessary.
- Ensure data is processed in a secure manner with only authorised access. Steps should be taken to prevent against unauthorised, unlawful processing and against loss or damage.
- The Data Controller is responsible for showing compliance with the legislation.

Gathering and Notification of Personal Data

Data subjects will be notified at the time of collection of:

- The reason for collecting the personal data.
- How it will be processed.
- Who will process it/have access to it.
- Where and how it will be stored.
- Security measures.
- How long it will be held.
- When it will be deleted and how.
- Employee rights under GDPR.
- The contact details for the Data Controller.

Personal data will only be collected for lawful purposes and only processed in a manner and reason for which it was gathered.

Protection statements will be included on the forms used to collect personal data.

If personal data is received by a third party the data subject will be made aware of:

- The reason for collecting the personal data.
- How it will be processed.
- Who will process it/have access to it.
- Where and how it will be stored.
- Security measures.
- How long it will be held.
- When it will be deleted and how.
- The identity and contact of the Data Controller.

The Storage of Data

Personal data gathered will be stored in a safe and secure manner. The following measures have been put in place to assist with this:

- Manual data is secured away in filing systems, with access only available to authorised personnel with a legitimate reason to view or process the data.

- Sensitive data is secured away in a locked cabinet with limited access to the Data Controller only. In some cases the data may be pseudonymised.

- Electronic data is protected through secure passwords and firewall systems.

Checking of Data

Personal data held will be periodically reviewed to ensure it is accurate and up to date. Employees will be provided with details of the contact details, next of kin and address details on an annual basis to enable them to check and amend as necessary.

Any data that should be removed after a length of time will be diarised and deleted accordingly. The removal of certain data may be restricted for example for historical records such as for HMRC or for other legal or legitimate reasons.

Any records that are inaccurate will be reported and rectified as soon as possible.

Disclosing Data

Personal data will only be disclosed to the authorised companies or individuals as notified at the time of gathering the data with the exception of the organisations which have a legal right to process the data without consent.

Personal data disclosure requests via telephone will be verified to ensure the person requesting are entitled to receive the data and further checks may be carried out such as contacting the Company direct to check, before the data is released.

Data Subject Access Requests

Data subjects have the right to request to see the personal data held concerning him or her. They should be provided with the following:

- Access to the data and a copy of it.
- The purpose of the processing.
- Categories of the personal data.
- Details of who has or will have access to the data.
- Where the data has or will be stored.
- How long the data has or will be stored for.

- Provided the right to lodge a complaint with the supervisory authority.
- Provided the details of the Employees Rights.
- Details of source of data if not collected from data subject.
- Details of any automated decision making or profiling of data such as recruitment and selection.

Employee Rights

Right to be forgotten	Employees have the right to request information is forgotten.
Right to be amended	Employees have the right to request information is amended.
Right to withdraw consent	Employees can withdraw consent to the processing of their data.
Right to data portability	Employees can use and obtain their own data for their own purpose.
Right to object	Right to object to automated decision made in decision-making, including profiling.
Right to object to the data being used for direct marketing purposes	Right to object to the personal data being processed, therefore cannot be processed further unless there is a legitimate reason for doing so.

Destroying Data

Data will be discarded if no longer required for the reason given at the time of collection or if the data is out of date. If there is no legal or business reason to keep the data it will be removed.

Breach of this Policy

Any members of staff who do not comply with this policy, along with the data protection regulations and legislation, may warrant disciplinary action which dependent upon the circumstances, could result in their dismissal.

Monitoring

The Data Controller will review this policy and update it as necessary.