AURAretrofit
hello@auraretrofit.co.uk • 02392 252 171 • www.AuraRetrofit.co.uk
Bridgwater House, Unit 2 Haywards Business Centre,
New Lane, Havant, Hampshire PO9 2NL
Home Heating and Energy Solutions

# Fair Processing Notice (Employee Data) Policy

**ICO Registration Reference: Z2466237**

During the course of our activities we, Aura Retrofit Limited, will process personal data (which may be held on paper, electronically, or otherwise) about our staff and we recognise the need to treat it in an appropriate and lawful manner, in accordance with the United Kingdom General Data Protection Regulations (UK GDPR). The purpose of this notice is to make you aware of how we will handle your personal data.

This notice does not form part of any employee's contract of employment, and we may amend it at any time.

## Data protection principles

We will comply with the six data protection principles in the UK GDPR, which say that personal data must be:

- Processed fairly and lawfully.
- Collected for specified, explicit and legitimate purposes and processed in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate and kept up to date.
- Not kept longer than necessary for the purpose.
- Processed in a manner that ensures appropriate security of the data.

"Personal data" means recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you. "Processing" means doing anything with the data, such as storing, accessing, disclosing, destroying or using the data in any way.

## Fair and lawful processing

We will usually only process your personal data where the processing is necessary to comply with our legal obligations, for the protection of your vital interests, for our legitimate interests or the legitimate interests of others. The full list of conditions is set out in the UK GDPR.

We will only process "special categories of data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, genetic data and data about sexual orientation where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the UK GDPR.

## How we are likely to use your personal data

We will process data about staff for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits in connection with your employment.

We may process sensitive categories of data relating to staff including, as appropriate:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

- the employee's gender, sexual orientation, racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- in order to comply with legal requirements and obligations to third parties.

**Processing for limited purposes**

We will only process your personal data for the specific purpose or purposes notified to you or for any other purposes specifically permitted by the UK GDPR.

**Adequate, relevant and non-excessive processing**

Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

**Accurate data**

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data, we hold about you.

**Data retention**

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

**Processing in line with your rights**

You have the right to:

- Request access to any personal data we hold about you.
- Prevent the processing of your data for direct-marketing purposes.
- Ask to have inaccurate data held about you amended.
- Ask to have data deleted where there is no good reason for us to continue processing it.
- Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else.
- Object to any decision that significantly affects you being taken solely by a computer or other automated process.

**Data security**

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

**Providing information to third parties**

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the six data protection principles.

**Data Privacy Impact Assessments (DPIAs)**

The Company, as a Data Controller, must conduct DPIAs should they propose a specific type of processing or processing which is likely to result in a high risk to individuals' interests.

Company personnel should conduct a DPIA (and discuss your findings with the Data Protection Lead) when implementing major system or business change programs involving the processing of personal data including the following:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated processing including profiling and/or automated decision-making;
- large scale processing of sensitive data; and
- large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

**Subject access requests**

If you wish to know what personal data we hold about you, you must make the request in writing. All such written requests should be forwarded to the Data Protection Officer.

**Organisational Measures**

The Company has undertaken, and will continue to undertake the following measures to ensure that we comply with our obligations under the GDPR and in particular the security principal of the GDPR:

- Regular data mapping and risk assessments of all types of personal data we obtain, hold or record in line with our Privacy Standard;
- Nominate an individual (as set out in this policy) who will have overall responsibility for information security;
- Provide training to all members of staff on data protection and the procedures they must follow in line with Company procedure (including the correct use of our Information Technology and Computer Systems);
- Annual reviews of this Information Security Policy to ensure that it is compliant and the Company's measures are maintained;
- Personal data collated and stored (in line with our Privacy Standard and Data Retention Policies) will be backed up on a nightly basis (depending upon the type of personal data) to ensure that it can be easily recovered if there was a security breach, incident which resulted in data being lost, altered or destroyed;

- Data Retention Policies set out how long personal data will be stored and when it will be erased in line with data protection principals and to ensure data is not kept longer than the lawful reason for processing as identified in our Privacy Notices;
- Any third party who acts as a data processor on behalf of the Company (as data controller) will be audited and appropriate terms in compliance with the GDPR will be agreed in writing;
- Procedure to change personal details is available and all staff are aware of the Company's process.

This list is not exhaustive and will be continually reviewed as part of the review of this policy.

**Technical Measures**

The Company has undertaken, and will continue to undertake the following measures to ensure that we comply with our obligations under the GDPR and in particular the security principal of the GDPR:

- All hard copy personal data is kept in lockable storage devices (access is limited to personnel who have the authority to access such personal data);
- Storage of electronic personal data is protected with approved security measures such as encryption, password-protected documents etc;
- The Company uses reputable companies and ensures they are compliant with data protection regulation to store and back up personal data such as Cowley IT, to assist with the recovery of data following any incident;
- The Company uses CCTV on site (please see the company's CCTV policy);
- The Company is aware and has measures in place to ensure its cyber security is monitored and compliant with guidelines in place this includes the use of WordFence and VIPRE (an anti-virus system);
- The Company's website is hosted by a company who is compliant and registered with ISO27001;
- All data is wiped from all electronic devices (including computers, phones, tracking devices etc) by a third party (currently Cowley IT or Aerial Telephones). The Company ensures that the nominated third party is compliant with GDPR;
- Paper waste is disposed on site by use of shredding machines and we operate a clear desk procedure meaning all notes must be shredded on a daily basis;
- Any visitors to the Company premises are accompanied by a nominated manager will be responsible for the visitor during the duration of their attendance on site;
- All IT and electronic equipment is stored securely on site. Should any company personnel remove electronic equipment from Company premises, they must seek managerial approval and comply with company procedure. Engineer and surveyor tablets are password-protected and signed for;
- The Company has and will undergo any relevant DPIAs (see below) on new systems which could be rolled out for the processing of data or other changes to our systems to ensure there is a process in place should the Company make the decision to implement a major change or our systems

The Company performs regular tests of the measures in place to assess and evaluate the effectiveness of our procedures and systems in place. All testing is recorded and will form part of ongoing data mapping and risk assessment processes.

**Data Mapping and Risk Assessments**

The Company carries out a data mapping and risk assessment of the principal information and personal data we process and hold on a quarterly basis. The data mapping process is recorded and maintained to show the main categories of information we hold in relation to our customers, the business and our members of staff. Such a process also indicates what security measures are taken to protect the personal data we process, use and maintain together with any risks identified.

In general terms the types of documents to be held in our information systems (either electronic or hard copy) are:

- Customer documents
- Staff documents (contracts of employment, personnel records etc)
- Business documents (examples – finance agreements, company documents etc)
- Others (third party agreements)

The safe disposal of any information and personal data collated as part of the data mapping process will be in line with this policy.

**Breaches of data protection principles**

If you consider that the data protection principles have not been followed in respect of personal data about yourself or others, you should raise the matter with your line manager. Any breach of the UK GDPR will be taken seriously and may result in disciplinary action.