Sustain UK Ltd

2A Albert Rd
Harborne, Birmingham
West Midlands, B17 0AN

Tel: 0121 428 2221
Fax: 0121 210 7799
info@sustainuk.org

Privacy & Confidentiality Policy/Procedures (incl Data Protection & GDPR)

1. Overview

Sustain (UK) Limited ("Sustain") acknowledges that in properly carrying out its duties, its employees will have access to information that is personal and often also highly confidential regarding both the Company, Staff member colleagues and also Tenants.

Furthermore, the law concerning personal information has been updated by the Data Protection Act 2018 and the EU General Data Protection Regulations (EU Regulation 2016/679) (the "GDPR").

This policy applies to current and former staff of Sustain, including workers, volunteers, apprentices, consultants, [as well as those on work experience].

Sustain will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from Ian MacGregor. We will only hold data for as long as necessary for the purposes for which we collected it.

This policy explains how Sustain will hold and process information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of, the Company.

This policy does not form part of the employment contract and may be updated it at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2. Data Protection Principles

Personal data must be processed in accordance with the following "Data Protection Principles." It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;

- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

Sustain are responsible for ensuring and demonstrating compliance with these principles.

3. Definitions

3.1 What does Confidentiality entail?

Confidentiality refers to any information (written or verbal) about an individual, which must not be shared without that person's permission and must only be recorded/stored in designated and in an appropriately secure manner and not used improperly. This includes anything discussed with Staff or Tenants during their respective support sessions.

3.2 What does Privacy entail?

Every data controller (Sustain) must issue a Privacy Notice to all individuals that they hold personal data for. This must show the purposes of the processing of Personal data.

GDPR also requires that we have identified and published a 'valid lawful basis' in order to process personal data' – Sustain has considered this and our view is shown at para 3.4 below.

3.3 What is Personal Data?

Personal data has been defined as 'any information relating to a person who can then be directly or indirectly identified, including by use of a reference as an identifier'. Personal data therefore covers obvious information such as name, contact details, NI no's, Next of Kin, but it also covers less obvious information such as unique identification numbers. Personal Data does not include anonymised data from which an individual cannot be identified.

The Personal Data collected on all individuals (i.e. Tenants, Staff, Non-Executive Directors) associated with sustain, is detailed in individual Privacy Notices. The Privacy notices are shared with all new starters and are also available from HR.

This policy applies to all personal data whether it is stored electronically, on paper, or in/on other materials.

Personal Data might be provided to Sustain by you, or by someone else (such as a former employer, your doctor, or a credit reference agency), or

it could be created by Sustain. It could be provided or created during the recruitment process or during the course of the employment contract (or contract for services) or after it has ended. It could be created by our manager or other colleagues.

3.4 What are 'Special Categories' of Personal Data?

"Special categories" of Personal Data are types of personal data consisting of information about:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic or biometric data;
- health; and
- sex life and sexual orientation.

Sustain may hold and use any of these special categories of personal data in accordance with the law.

Sustain may also hold and use personal data relating to criminal allegations, offences, proceedings and convictions.

3.5 What are the lawful bases for processing?

Under the GDPR, Sustain must always have a valid lawful basis in order to process Personal Data, and there are six available lawful bases on which to rely.

At least one of these must apply whenever personal data is processed. Sustain has considered this and detailed below (in italics) how Sustain interprets each of the relevant legal bases:

a. **Consent**: the individual has given clear consent for us to process their personal data for a specific purpose – this is ascertained via the signed consent notice attached to every individual's Privacy Notice.

b. **Contract**: the processing is necessary for contracts / agreements we have with the individuals, for example, agreements to provide accommodation and support.

c. **Legal obligation**: the processing is necessary for Sustain to comply with common law or a statutory obligation, for example, Housing Benefit Regulation.

d. **Vital interests**: the processing is necessary to protect someone's life. Safeguarding of individuals (for example, Tenants, Staff and any visitors) is of paramount importance to Sustain.

e. **Public task**: the processing is necessary for the performance of a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Sustain does not believe that this lawful basis applies when processing Personal Data.

f. **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Following a 'Legitimate Interest Assignment', Sustain has assessed that 'Next of Kin' (NOK) details as being such a legitimate interest.

To summarise, we believe that the Personal Data collected is needed for Sustain to perform the service of providing vulnerable people with accommodation and support. Consent has been obtained via signed Privacy Notices.

3.6 When we may process Personal Data

Sustain may process Personal Data in various situations, for example:

a) Tenants:

- Providing and managing support.
- Personalising and tailoring services as agreed with the individual.
- Communicating with individuals.
- Evidencing to our Commissioners and Regulators.
- For the safety of the Tenants, Staff and general public.

With the permission and/or where permitted by law, we may also use the personal data for internal marketing purposes, which may include contacting the individuals by email and telephone and post with information about Sustains services or news updates.

We will however not send any unlawful marketing or spam. We will always work to fully protect individual's rights and comply with our obligations under the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

We do not use the automated system for carrying out any kinds of decision making or profiling.

b) Sustain staff, including workers, volunteers, apprentices, consultants, as well as those on work experience

Sustain has to process personal data in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement).

Examples include:

- to decide whether to employ (or engage) and individual.
- to decide how much to pay, and the other terms of the contract.
- to check the legal right to work for Sustain.
- to carry out the contract between us including, where relevant, its termination.
- to deliver training and review performance.
- to decide on promotion.
- to decide how to manage performance, absence or conduct.
- to carry out a disciplinary or grievance investigation or procedure.
- to determine whether Sustain needs to make reasonable adjustments to the workplace or individual roles because of a disability.
- to monitor diversity and equal opportunities.
- to monitor and protect the security (including network security) of Sustain, its staff, tenants and others.
- to monitor and protect the health and safety.
- to make relevant payments to pension and other benefits in accordance with the individual contract of employment.
- to pay tax and National Insurance.
- to provide a reference upon request from another employer.
  [to pay trade union subscriptions.]
- to monitor compliance with Sustain policies and Sustain's contractual obligations.
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect Sustain.
- to answer questions from insurers in respect of any insurance policies which relate to Sustain staff.
- to run the Sustain business and plan for the future.
- for the prevention and detection of fraud or other criminal offences.
- to defend Sustain in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure.
- for any other reason which Sustain may notify of from time to time.

Sustain might process special categories of Personal Data, in particular, Sustain will use information in relation to:

- race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities.
- sickness absence, health and medical conditions to monitor absence, assess fitness for work, to pay benefits, to comply with legal obligations under employment law including to make reasonable adjustments and to look after health and safety.
- trade union membership to pay any subscriptions and to comply with legal obligations in respect of trade union members.

4. Summary Procedures

4.1 Duties & Responsibilities:

All staff are required to sign a confidentiality statement before their employment commences and should also receive training as part of their induction on the principle elements of the Sustain's confidentiality policy and the basic principles of the Data Protection Act/GDPR and the implications that this will have on their work.

Every employee has a duty of confidentiality to Tenants and a duty to support professional ethical standards of confidentiality. Everyone within Sustain and covered by Sustain contracts must be aware of the importance of confidentiality. All Staff need to be aware of their responsibilities for safeguarding Tenants confidentiality and keeping information secure.

4.2 Record keeping/Storage:

a) Care must be taken to ensure that any markings on the external page of a file/lever arch file, is not made visible to any visitor to the accommodation or office.

b) All Staff records should be kept in a secure area (secure rooms/filing cabinets) in the Company's Head Office

c) Records relating to Tenants (eg Support Plans/Personal Files etc) should again be kept in a secure area (secure rooms/filing cabinets) in the Home Providers Head Office or the accommodation location. All records must always be locked away when not being used and when in use must not be able to be viewed by anyone other than the data subject or an authorised officer.

d) The filing cabinet/secure area must be locked at all times when not being used by a Staff member. No Tenant's records should be taken off the designated premises. When Tenant files are needed, Staff should get them from the secure area, not leave them unattended and return them immediately following their use.

e) In office locations, care must be taken not to display on walls/noticeboards etc, any personal information which could identify Tenant details

f) No computer screens (or other display screens) showing Tenant personal data (including even names) must be visible to visitors to the office or in the office from a 'counter area'.

g) With regard to confidentiality, all Tenants have the right to receive their confidential post un-opened. This is in accordance with the Data Protection Act and Human Rights legislation.

h) Personal information regarding staff members should also be kept in the strictest of confidence and accessed only by management. No Staff records must leave the premises at any time.

i) Any personal data which is no longer needed must be disposed of securely (in accordance with 'Data Retention Policy' periods). This means that paper and other physical records should be thoroughly shredded, and disposal arrangements made with a company that has achieved BS EN 15713:2009

j) Personal data held on computers etc that are sold on or donated – it is no longer acceptable to just re-format hard disk drives. As there are tools now readily available which can recover data from formatted disks. It is therefore important that organisations contract with a company which guarantees full data as being irrecoverable.

k) Personal data will only be stored in the UK. This means that it will be fully protected under the GDPR

l) Staff must comply with the requirements of this policy. Non-compliance with this policy may result in disciplinary action being taken, which may amount to gross misconduct leading to dismissal.

m) There are however exceptions to our Privacy & Confidentiality policy. If we think that a person is at serious risk or we are given information about a crime, then we may have to pass this onto other people. We would normally tell the individual before we do this and will provide reasons in writing for our action.

5. How long will we keep the Personal Data?

We will not keep personal data for any longer than is necessary in light of the reason(s) for which it was first collected and also in line with guidance

from our insurers and/or if there is an ongoing query from a statutory body (eg HM Revenues) or an ongoing legal claim/court proceeding.

For further information on data retention, please see the separate Data Retention Policy displayed on the sustain web site www.sustainuk.org

6. How do we share the Personal Data collected?

We will not share any personal data with any third parties other than where we have obtained a 'Data Sharing Agreement'. We require those people and companies to keep Personal Data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process data for the lawful purpose for which it has been shared and in accordance with instructions from Sustain.

In some limited circumstances, we may be legally required to share certain personal data, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority. In these instances, we will always endeavour to inform the individual concerned.

Sustain does not send your personal data outside the European Economic Area. If this changes, Sustain will notify those affected. Sustain will also explain the protections that are in place to protect the security of the data.

7. Individual rights

Every person has the following rights with regard to Personal Data:

a) **The right to be informed** about the collection and use of their personal data. This Privacy and Confidentiality Policy & Practice (freely available on the Sustain web pages and referred to in documentation provided to Tenants & Staff) should tell an individual everything they need to know, but if people have any further questions, they should approach the person in the organisations who has responsibility for Data Protection.

b) **The right to access personal data** that is held concerning themselves.

c) **The right to have personal data rectified** if any of the personal data held by us is inaccurate or incomplete.

d) **The right of erasure**, the right to ask us to delete or otherwise dispose of any aspect of an individual's personal data that we have.

e) **The right to restrict** (i.e. prevent) the processing of personal data.

f) **The right to object** to us using an individual's personal data for a particular purpose or purposes.

g) **The right to data portability**, if someone has provided personal data to us directly, then we are using it with their consent for the performance of a task which has been explained to them. The individual can then ask us for a copy of that personal data to re-use when e.g., they move to another job (i.e., Staff) or to another supported accommodation provider (Tenants).

h) **Right to be made aware** when the data held is used for automated decision-making and profiling. However, Sustain would point out that we currently **do not** intend to use personal data in this way

Individuals should contact Sustain's Data Protection Officer, Ian MacGregor at ian@sustainuk.org in any of the above situations.

Further information about an individual's rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If an individual has any cause for complaint about our use of their personal data, they have the right to lodge a complaint with the Information Commissioner's Office. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has more information on your rights and our obligations.

Sustain is registered with the Information Commissioners Office (ICO) registration number ZA037625.

8. How can individuals access their Personal Data?

If any individual wants to know what personal data is held about them, they can made a Subject Access Request (SAR).

This request must be made in writing to Sustain's Data Protection Officer, Ian MacGregor at ian@sustainuk.org. If you receive a SAR during the course of your employment with Sustain, the SAR should be forwarded immediately to the Data Protection Officer who will coordinate a response.

To make a SAR in relation to your own personal data, you should write to the Data Protection Officer. Sustain must respond within one month unless

the request is complex or numerous in which case the period in which we must respond can be extended by up to two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, Sustain may charge a reasonable administrative fee or refuse to respond to your request. Sustain normally work on the basis that any request which will take more than a day to deal with is likely to be manifestly excessive, and in those circumstances believe a reasonable charge is one working day's salary.