Bespoke Supportive Tenancies Ltd

GDPR Policy

Version: 01

Review

Date of this review	Date of last review	Policy author(s)	Compliance Manager	Next review date
April 2020	N/A	Denise Jolley	N/A	April 2022

Details of amendments

Version	Date	Update/ amendment detail	Resulting from

Approved by

Executive Team	April 2021
Board	N/A

1. INTRODUCTION

1.1 This policy sets out the organisations commitment to meeting and upholding the principles of General Data Protection Regulations (GDPR).

2. PURPOSE

2.1 The purpose of this document is to ensure that all employees are clear on the steps that will be taken by the organisation in terms of meetings its obligations under the General Data Protection Regulations (GDPR).

3. SCOPE

3.1 This policy applies to those individuals that are directly employed by the organisation and for whom the organisation has legal responsibility.

This policy also applies to contractors or workers who are undertaking temporary work or work experience on behalf of the organisation either on the organisations premises or on behalf of the organisation in a remote working capacity.

4. KEY PRINCIPLES

4.1 BeST is committed to the protection of all personal and sensitive data for which it holds responsibility as a Data Controller and the processing of such data in line with data protection principles and the General Data Protection Regulations (GDPR).

The requirements of this policy are mandatory for all employees of the organisation and any third party contracted to providing services on behalf of the organisation.

4.2 Data Controller

BeST is a Data Controller for the purposes of GDPR. A Data Controller is a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

4.3 Processing

The organisation understands that processing 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, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

4.4 Lawful Basis for Processing Data

The organisation will comply with the six lawful bases for processing data, which are as follows:

- Consent – the individual has given clear consent for their personal data to be processed for a specific purpose.
- Contract – the processing is necessary for entering into a contract with an individual or the individual has asked for specific steps to be taken before entering into the contract.
- Legal obligation – the processing is necessary in order to comply with the law (not including contractual obligations).
- Vital interests – the processing is necessary to protect someone's life.
- Public task – the processing is necessary for the performance of a task in the public interest and the task or function has a clear basis in law.
- Legitimate interests – the processing is necessary for the individuals legitimate interests or the legitimate interests of a third party. Unless there is a good reason for protecting the individuals personal data which overrides those legitimate interests.

The organisation recognises that no single basis is better or more important than the others. Also, which basis is the most appropriate to use will depend on the purpose for processing and the relationship with the individual. The organisation will ensure that:

- The lawful basis for processing will be determined before starting to process the data and will be documented.
- Care is taken to choose the correct lawful basis for processing as it understands that the lawful basis cannot be changed to a different lawful basis at a later date without good reason, and in particular as relates to Consent.
- In terms of processing Special Category Data, it will comply with the requirement to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- It will comply with the requirement to identify both a lawful basis for general processing and an additional condition for processing criminal conviction data or data about offences.

4.5 Principles for Processing

The organisation will comply with all principles for processing, which are as follows:

Lawfulness, fairness and transparency – this is the most important principle and relates to total transparency for all data subjects. When collecting data, the organisation will be clear about why it is being collected and how it is going to be used. If the data subject requests further information regarding the processing of their data, then the organisation will provide this is in a timely manner.

Purpose Limitation – the organisation will have a specific and legitimate reason for collecting and processing personal information. The data will only be used for the designated purpose and will not be reprocessed for any other use, unless the data subject has provided their explicit consent to do so.

Data Minimisation – any data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. In view of this, the organisation will only store the minimum amount of data required for its purpose. It will not hold more data than is necessary.

Accuracy – the personal data collected will be accurate, fit for purpose and up to date. In view of this, the organisation will regularly review information held about individuals and delete or amend inaccurate information accordingly.

Storage Limitation – once the personal data is no longer needed for the purposes for which it was collected, the organisation will delete or destroy the data unless there are other grounds for retaining it. To ensure compliance, the organisation has in place a review process to manage the cleansing of databases.

Integrity and Confidentiality – the organisation will ensure that all the appropriate measures are in place to secure the personal data it holds. This includes protection from internal threats such as unauthorised use, accidental loss or damage, as well as external threats such as phishing, malware or theft.

Accountability – the organisation will take responsibility for the data it holds and will demonstrate compliance with the other principles. It will evidence the steps that it has taken to demonstrate compliance, which will include:

- Evaluating current practices
- Creating a personal data inventory
- Obtaining appropriate consent
- Carrying out data protection impact assessments

4.6 Data Subject Rights

A data subject is any living individual whose personal data is collected, held or processed by an organisation.

The organisation will comply with all rights pertaining to data subjects as follows:

- The right to be informed – the organisation will tell individuals what data is being collected, how it is being used, how long it will be kept for and whether it will be shared with any third parties. This information will be communicated concisely and in plain language.

- The right of access – the organisation will provide a copy of any personal data they hold concerning an individual within one month of the request being received, although exceptions will be made for requests that are manifestly unfounded, repetitive or excessive.

- The right to rectification – the organisation will update any information that it holds that is inaccurate or incomplete within one month of a request being received, although exceptions will be made for requests that are manifestly unfounded, repetitive or excessive.

- The right to erasure – if requested, the organisation will erase the data of individuals in the event that the data is no longer necessary, the data was unlawfully processed or it no longer meets the lawful ground for which it was collected. This includes where the individual withdraws consent.

- The right to restrict processing – as an alternative to erasing the data, the organisation will limit the way it uses personal data if the individual requests this.

- The right to data portability – the organisation will honour an individuals right to obtain and reuse their personal data for their own purposes across different services. This right applies to personal data that the individual has provided to the organisation by way of a contract or consent.

- The right to object – the organisation will honour an individuals right to object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest or exercise of official authority. It will stop processing information unless it is able to demonstrate compelling legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual or if the processing is for the establishment or exercise of defence of legal claims.

4.7 Personal Data

Personal data includes information relating to natural persons who:

- Can be identified or who are identifiable, directly from the information in question;

  Or

- Who can be indirectly identified from that information in combination with other information.

Identifiers include ID numbers, location data, physical, psychological, genetic and mental factors and may include (but is not limited to):

- Name
- Date of Birth
- Postcode
- Address
- National Insurance Number
- Photographs/Digital Images
- NHS Number
- Passport Number
- Online Identifiers/Location Data such as MAC, IP Addresses and Mobile ID's

4.8 Special Category Data

Special Category Data is defined by the GDPR as:

- Personal data that reveals racial or ethnic origin
- Personal data that reveals political opinions
- Personal data that reveals religious or philosophical beliefs
- Personal data that reveals trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health
- Data concerning a persons sex life
- Data concerning a persons sexual orientation

4.9 Special Category Data Processing

With regards to the processing of any Special Category Data, the organisation will ensure that its processing is lawful, fair and transparent and complies with the principles and requirements of GDPR in relation to this data.

In addition to identifying a lawful basis for processing, it will only process Special Category Data if it is able to meet one of the specific conditions in Article 9 of the GDPR. It will consider the purposes of processing and identify which of the conditions are relevant on a case by case basis.

If the basis for processing requires a basis in UK law, the organisation will meet the additional conditions set out in the Data Protection Act 2018.

The organisation will undertake a Data Protection Impact Assessment (DPIA) for any type of processing that is likely to be high risk.

The organisation will keep records, documenting the categories of data for every incident of Special Category Data processing.

4.10 Article 9 Special Conditions

Article 9 of the GDPR relates to the following:

- Explicit consent (a)
- Employment, social security and social protection (if authorised by law) (b)
- Vital interests (c)
- Not-for-profit bodies (d)
- Made public by the data subject (e)
- Legal claims or judicial acts (f)
- Reasons of substantial public interest (with a basis in law) (g)
- Health or social care (with a basis in law) (h)
- Public health (with a basis in law) (i)
- Archiving, research and statistics (with a basis in law) (j)

If relying on conditions (b), (h), (i) or (j), the organisation will meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the Data Protection Act 2018.

If relying on the substantial public interest condition in Article 9(2)(g), the organisation will also meet one of the 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the Data Protection Act 2018.

The organisation will identify which of the conditions most closely reflects its purpose after carefully considering the detailed provisions of each condition to ensure that it can demonstrate that the condition applies.

The organisation will take steps to demonstrate that any specific processing is 'necessary for reasons of substantial public interest" on a case by case basis.

5. RESPONSIBILITIES

5.1 Executive Team – The Executive Team has overall responsibility for ensuring that BeST continuously adheres to best practice in every aspect of the GDPR.

5.2 Heads of Department – Heads of Department are responsible for ensuring that that the requirements of this policy are implemented at operational level.

They are also responsible for:

- Notifying the HR Department of any potential data breach within their teams with immediate effect.
- Working with the HR Department in investigating any potential data breach.
- Prioritising their attendance at any meetings connected with this process and maintaining confidentiality.

5.3 Employees – Employees are responsible for seeking clarification from their manager if they are unsure how the policy should be interpreted.

They are also responsible for:

- Raising any concerns that they have about any practices they have witnessed or experienced which are contrary to this policy.
- Participating in any training that is provided relating to GDPR or any aspect of this policy.

5.4 Human Resources – Human Resources are responsible for providing guidance to managers and employees on the interpretation and implementation of this policy.

They are also responsible for the following:

- Providing confidential support and advice to managers and employees on aspects of data processing, security, governance and privacy.
- Ensuring that this policy is updated in line with any legislative changes.

6. REPORTING AND MONITORING

6.1 The Record of Processing Activity (RoPA) will establish what data is processed within the organisation, through what activities and how it is stored.

6.2 Data breaches will be reported to the ICO and data subjects, if appropriate, in accordance with legislation.

6.3 Data processing agreements will be signed with any third parties that process personal data on the organisations behalf.

7. DEFINITIONS

7.1 BeST – Bespoke Supportive Tenancies Ltd.

8. EQUALITY AND DIVERSITY

8.1 BeST is committed to mainstreaming equality and diversity throughout all its activities as well as meeting the general and specific duties imposed on it through the legislation. Please refer to BeST's Equality and Diversity Policy to read the Policy details in full.