Policy number: HC16
Re-regulation :
11,17,18

Data Protection Policy

Introduction

SweetTree Home Care Services Ltd gathers and uses certain information about individuals. Individuals include our clients and their family members, employees, suppliers, other care providers and any other people SweetTree Home Care Services Ltd has a relationship with or may need to contact.

Key Issues

This Data Protection Policy ensures SweetTree Home Care Services Ltd:

- Complies with data protection law;
- Protects the rights of all members of the SweetTree Team and Clients;
- Is open about how data is stored and processed;
- Protects itself from the risks of a data breach
- Track and Trace

Data Protection Laws

General Data Protection Regulation (GDPR)

The GDPR is the new framework for data protection laws and it replaces the previous 1995 Data Protection Directive, which current UK law is based upon.

The legislation is designed to "harmonise" data privacy laws across the European Union as well as give greater protection and rights to individuals.

It's provisions in the UK is covered by a new Data Protection Bill which became law on 25th May 2018 and will continue post Brexit.

The scope of the GDPR covers personal and sensitive personal data.

Personal Data

Any information that can be used to directly or indirectly identify a person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Policy number: HC16
Re-regulation :
11,17,18

Key Issues (continued)

Sensitive Personal Data

Encompasses genetic data (which SweetTree Home Care does not hold), information about religious and political views, sexual orientation for example.

Highlights

- Individuals have easier access to the data companies hold about them;
- Fines regime in place for breaches;
- Clear responsibility for organisations to obtain the consent of individuals they collect information about.
- Requirement to document why information is being collect and processed, descriptions of information held, how long it is kept for and descriptions of technical security measures that are in place.
- How to request copy of all data

Policy Scope

This policy applies to:

- The Head office of SweetTree Home Care Services Ltd
- All branches of SweetTree Home Care Services Ltd
- All employees and volunteers of SweetTree Home Care Services Ltd
- All contractors, suppliers, and other people working on behalf of SweetTree Home Care Services Ltd

It applies to all data the company holds relating to identifiable individuals, and includes but is not restricted to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Next of kin details
- Date of birth
- Marital status
- Health related information
- Access codes
- Financial Information

Data Protection Risks

This policy helps to protect SweetTree Home Care Services Ltd from data security risks, including:

- Breach of confidentiality – for instance information being given out inappropriately.
- Failing to offer choice – for instance all individuals should be free to choose how the company uses data relating to them;

Key Issues (continued)

- Reputational Damage – for instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with SweetTree Home Care Services Ltd has responsibility for ensuring data is collected, stored and handled appropriately within the remit of their role.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Specific key areas of responsibility:

Company Directors: Ultimately responsible for ensuring that legal obligations are met.

The Privacy Officer / Data Protection Compliance Officer is responsible for:

- Keeping the Advisory Board, Compliance team and the GDPR Committee updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Ensuring the data protection training is relevant / up to date;
- Handling internal and external data protection questions;
- Dealing with requests from individuals to see data held about them (called 'subject access requests') within a month of the request being made.
- Reviewing any contracts or agreements with third parties that may handle the company's sensitive data.

The IT Manager is responsible for*:*

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Performing regular checks and scans to ensure security hardware and software is functioning properly;
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The Commercial Director is responsible for:

- Addressing any data protection queries from journalists or media outlets like newspapers;
- Where necessary, work with other employees to ensure marketing initiatives abide by data protection principles.

Policy number: HC40
Re–regulation : 11,17,18

Policy and Procedure

- The only people able to access data covered by this policy should be those who need it for their work;
- Data should not be shared informally. When access is required to confidential information, individuals can request this by submitting a Subject Access Request to the Privacy Officer;
- SweetTree Training Academy will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
    - Setting strong passwords to access the information systems, and update when prompted;
    - Personal data should not be disclosed to unauthorized people, either within the company or externally;
    - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required it should be deleted and disposed of;
    - Submit an Employee Details Amendment form to let us know of changes to name, address or bank details;
    - Employees should request help from their line manager or the Privacy Officer if they are unsure about any aspect of data protection;
    - Use SweetTree.com emails only when sending information;
    - Be wary of emails that may not be genuine;
    - Only forward SweetTree.com emails to family members /third parties if explicit consent has been given;
    - Don't disclose information over the phone without verifying who you are talking to;
    - Never save files directly to personal laptops or other mobile devices like tablets or smartphones;
    - Never use external file storage / transfer hardware;
    - Never divert sweettree.co.uk or sweettree.com to any external email;
    - Always use the SweetTree.com email address when communicating with office staff / other Support Workers;
    - Notify the Office Team if any information you are given relating to a client is found to be out of date;
    - Lock PC screens when away from your desk;
    - Contact Support Workers via their SweetTree.com email address only;
    - Update information in PeoplePlanner relating to a client or funder if it is found to be out of date, for example phone number, address;
    - Log out of operational systems before leaving your desk if office based;
    - Don't download 'free' software from the internet;
    - Never give keys to SweetTree or partner buildings for other people to use;
    - Notify the IT Manager immediately if a member of staff is leaving the company so access to all systems can be removed and keys, phone, etc. recovered.

Policy and Procedure (continued)

Information Security Management

- SweetTree Home Care Services have a service level agreement with IT company ITLAB, they are responsible for the information security management.
- The IT manager monitors security of computer systems, manages phone systems, and remote access into the secure network.
- SweetTree's main server is held in the main SweetTree Office. It is secured in a locked air-conditioned room – accessible only by IT manager.
- The server is secured by BIT Defender and Mimecast which filters all information in and out of the company server. These securities are managed and monitored by ITLAB and the IT manager. A back up of the server using Symantec Backup, is completed daily and tapes held off site for security and safety.
- All servers and computers containing data are protected by approved security software and a firewall. (BIT Defender)
- All computers are scanned weekly by the IT manager on site and monitored, and all username and password protected. All user access is on an individual security level basis. Secure folders with security access are maintained for some information on the server held by senior managers.
- SweetTree has two internet lines to ensure a failsafe connection – and an emergency contingency plan in place with 24-hour cover. (Please refer to the Emergency Contingency Plans for more detail).
- Laptops and all mobile devices are password protected
- The SweetTree Wi-Fi connection is secured and can only be accessed via a secure password.
- Virtual Private Network connections are secured by username and password. All on – call personnel have a VPN connection to prevent printed documentation travelling from office to home.
- All confidential waste is disposed of securely in a locked confidential waste bin – managed by a service level agreement with Restore - Datashred and taken off site for shredding.

Data Storage

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a desk / printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

Policy and Procedure (continued)

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (such as backup tapes), these should be kept locked away securely.
- Data should only be stored on designated drives and services, and should only be uploaded to an approved cloud computing service platform.
- Servers containing personal data should be situated in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- No software to be downloaded unless authorized by IT Manager.

Data Use

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Use computer screen shields when working constantly with personal data e.g. Payroll.
- Personal data should not be shared informally. It should never be sent to a personal email address UNLESS consent has been given to do so by a family member.
- Client information that is required by an employee, to be able to carry out their tasks should only be sent to their SweetTree.com email address.
- Data must be encrypted before being transferred electronically. The IT Manager can facilitate this to send data to authorized external contacts such as Auditors.
- Personal data should never be transferred outside the European Economic Area.
- Employees should not save copies of personal data to their own computers or company laptop hard drives.

Data Accuracy

The law requires SweetTree Home Care Services Ltd to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Employees should not create any unnecessary additional data files.
- Employees should take every opportunity to ensure data is updated.
- SweetTree Home Care Services Ltd will have a clear and easy process for individuals to update the information held relating to them.
- Data should be updated as inaccuracies are discovered.
- It is the communication manager's responsibility to ensure marketing databases are checked against Hygiene and Data Quality suppression files on an ongoing basis"

Policy and Procedure (continued)

Subject Access Requests (SAR)

All individuals who are the subject of personal data held by SweetTree Home Care Services Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts SweetTree Home Care Services Ltd requesting information specific to them, this is called a Subject Access Request (SAR). These must be responded to within one month of receipt, and are free of charge.

The Privacy Officer must always verify the identity of anyone making a SAR before handing over any information. Clients with sensory or other disabilities must be given appropriate help and support from an independent source as required.

Right to Erasure

The right to erasure states that in certain circumstances, an individual can submit a request to have personal information erased to prevent further processing of that data. The right to erasure applies when:

- The personal data is no longer necessary or relevant in relation to the purpose for which it was originally collected.
- The individual specifically withdraws consent to processing (and if there is no other justification or legitimate interest for continued processing).
- Personal data has been unlawfully processed, in breach of the GDPR.
- The data must be erased in order to comply with legal obligations (for example, the deletion of certain data after a set period of time).

If one of the above conditions applies under this right to erasure, SweetTree Home Care Services Ltd has an obligation to delete and remove the data 'without undue delay' and specifically within a month unless specific circumstances apply.

In instances where personal data has been shared with other third parties or made available in the public domain, the GDPR states that 'all reasonable steps' must be taken to inform other outlets of the request for erasure and require them to comply with deletion or removal.

The exceptions to the right to erasure and reasons to refuse to comply include:

- The right of freedom of expression and information
- Compliance with legal obligations or official authorities

Policy and Procedure (continued)

- Public health reasons or the performance of a public interest task
- If needed for the exercise or defence of legal claims

In some cases, the restriction of personal data may be more applicable, and this could be used an alternative option to erasure or in circumstances where data must be held in limbo pending legal challenges.

Note: there is a distinct difference between personal data and client data. Individuals can only request their own data to be erased.

The request should be sent to info@sweettree.co.uk and should give an indication of the individuals link to SweetTree be it client, funder, employee, job applicant etc. So that SweetTree can reduce the spread of information to the wrong departments.

Disclosing data for other reasons

In certain circumstances, external bodies request data from SweetTree Home Care Services Ltd, which the company is legally required to comply with. Examples of this are:

- Office of National Statistics
- HMRC
- Department of Work and Pensions
- Care Quality Commission
- Government Equalities Office
- UK Visas and Immigration / Home Office
- The Police
- Safeguarding authorities
- Track and Trace (Covid-19)

In these circumstances SweetTree Home Care Services Ltd will disclose the requested data. However, the Privacy Officer will ensure the request is legitimate, seeking assistance from the Directors / legal advisers where necessary.

We are also required to carry out Criminal Record checks as part of the terms of employment. The Disclosure and Barring Service (DBS) has a Code of practice regarding correct handling, which is adhered to. SweetTree Home Care Services Ltd are authorized to receive disclosure information, and it is a criminal offence to pass this information on to any other person or organisation.

References that are sent from SweetTree are sent in confidence to the attention of the addressee only.

Policy and Procedure (continued)

How long data is held for

Data	Held for:
Client Records	7 years after the date the service provision ceased (Adults) 25 years after the date the service provision ceased (Children)
CVs of unsuccessful Applicants for Jobs	3 months
Employee files	7 years after the date employment ceased
Accounting transactions	7 years
Criminal Record Disclosure information	DBS certificates are keptp for 6 months and destroyed after. For compliance purposes a DBS approval form is kept on file which contains the individual's name, date of birth, type of check carried out, certificate number and whether the check return any result (Clear or Unlcear)

Data Breach

If a data breach occurs, please notify the Privacy Officer immediately. Please refer to the Data Breach Procedure for definitions on what constitutes a data breach. Depending on the nature of the data breach there may also be a requirement to notify the Care Quality Commission. In these instances, please notify the Registered Manager.

Providing Information

SweetTree Home Care Services Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

How the data is being used.
How to exercise their rights.

The company has a privacy policy, setting out how data relating to individuals is used by the company. This is available on request, and a version of this statement is also available on the website.
Employees are required to read and acknowledge understanding of the Employee Data Consent Form.
Clients are required to read and sign the Client Data Consent Form.

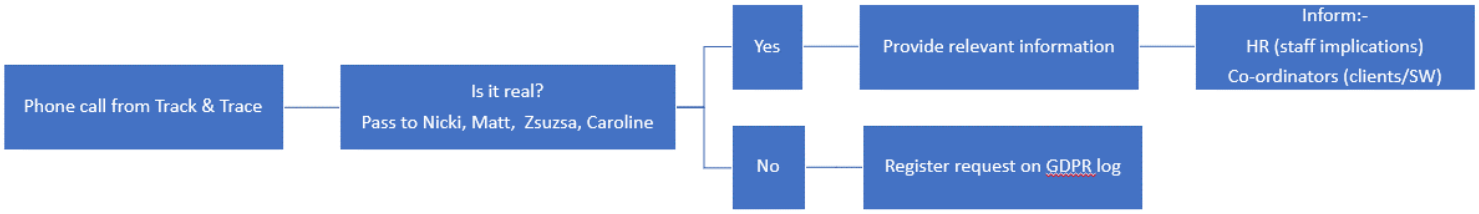
Clients or employees who have a complaint about the way that the organisation keeps files about them, or who are refused access to files that they believe they should have access to, should be referred to the Data Protection Information Commissioner.

Policy number: HC40
Re–regulation : 11,17,18

UK Government Track and Trace

Due to Covid-19 the UK Government has implemented track and trace. SweetTree is obliged if contacted by the Track and Trace team to provide the required basic information and no more anything else would be against GDPR.

The procedure and information is as follows:



All calls should direct staff to the following website:

https://contact-tracing.phe.gov.uk/

The only relevant information is as follows:

Track and Trace may only ask SweetTree for the following information and this is if SweetTree place is involved in a coronavirus outbreak and there is a risk that staff may have been in close contact of someone infected with the virus.
1.full name
2.contact telephone number, if available
3.email address, if available

This is direct from (https://contact-tracing.phe.gov.uk/help/privacy-notice)

Additional Information

Eugdpr.org - EU GDPR website
ICO.org.uk – Information Commissioner's Office website.
SweetTree Home Care registration number Z1197199

Supporting Procedures

Right To Erasure Procedure

Data Breach Procedure

Subject Access Request (SAR) Procedure