Data Protection Policy

Directorate: Resources
Date of Issue: May 2018
Version: V5

live • grow • thrive • together

1. Introduction

The General Data Protection Regulation (GDPR) 2018 replaces the EU Data Protection Directive and supersedes the laws of EU Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

2. Aim / Purpose of the Policy

The aim of this policy is to ensure that Salix Homes is compliant with the General Data Protection Regulations (GDPR) and the Data Protection Bill 2018. This policy also supports Salix Homes' aim in demonstrating commitment to Data Protection legislation.

This policy outlines the responsibilities of Salix Homes and its employees in respect of the collection, use and disclosure of data and the rights of the customer to have access to personal data concerning them.

3. Policy

1. Definitions

1.1. **Data** means information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, i.e. highly structured readily accessible paper filing system;

(d) does not fall within (a), (b) or (c) above but forms part of an accessible record; or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

1.2. **Data Controller** means a person who (either alone, jointly or in common with other persons) determines the purposes for, and the manner in which, any personal data is processed. A Data Controller may also act jointly with another organisation to process personal data.

1.3. **Data Processor**, in relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

1.4. **Data Security Breaches**, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data.

1.5. **Data Subject** means an individual who is the subject of personal data.

1.6. **Data Subject Rights**. Data Subjects have rights in relation to their personal data under the GDPR. Those rights include:

(a) the right to be informed;
(b) the right of access;
(c) the right to rectification;
(d) the right to erasure;
(e) the right to restrict processing;
(f) the right to data portability;
(g) the right to object; and
(h) rights in relation to automated decision making and profiling.

1.7. **Personal data** means information which:

(a) relates to a living individual who can be identified from the data, or

(b) from the data and other information which is in the possession of, or

(c) is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

1.8. **Privacy and Data Protection Legislation**, includes all applicable laws and regulations relating to the processing of personal data and privacy, as follows (not necessarily exhaustive):

(a) the Data Protection Act 1998;
(b) the Data Protection Directive;
(c) the Electronic Communications Data Protection Directive;
(d) the Privacy and Electronic Communications Regulations 2003;
(e) the Human Rights Act 1998;
(f) the European Convention on Human Rights;
(g) the General Data Protection Regulation (GDPR); and
(h) the Data Protection Bill

1.9. **Processing,** in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data

1.10. **Special Category Personal Data,** for the purpose of this Agreement includes, but is not limited to:

- political opinions;
- religious beliefs or other beliefs of a similar nature;
- ethnicity;
- trade union details;
- medical records; or
- sexual preferences.

1.11. **Supervisory Authority**. The GDPR states that each EU member must have their own Supervisory Authority in place to govern Data Protection within its own boundaries. The Information Commissioners Office (ICO) governs Data Protection for the UK.

Compliance & Assurance

2. Salix Homes is registered with the ICO and seeks to renew this registration on an annual basis. The

ICO will be notified of any changes in the way in which Salix Homes processes personal data within 28 days of the changes taking place.

3. To show accountability and compliance with the GDPR and Data Protection Bill 2018, Salix Homes keeps all processing activities within our Information Asset Register (IAR). The IAR records the following information against all data assets:

- The source of the data;
- What the data is used for;
- What the data consists of;
- Details of the information asset owner;
- The volume of that specific data asset;
- Details of personal and/or special category data contained within the data asset;
- Who has access to the data asset internally;
- Who the data asset is shared with externally;
- Confirmation of data sharing/processing agreements if applicable;
- Format of the data asset;
- Where the data asset is stored electronically and/or physically;
- Details of the retention period of the data asset and the deletion schedules that are in place;
- The data classification scheme for the data asset;
- Details of the primary processing purpose for the data asset and any other processing purposes;
- Details of what consent is in place to process the data asset; and
- Details of the risk assessment for the data asset.

4. All Salix Homes employees are provided with Data Protection training through various channels. All employees are held appropriately accountable for Data Protection.

Incident Reporting & Management

5. Salix Homes will maintain an Incident Reporting & Management Procedure, which instructs all employees what process to follow in the event of a data breach.

6. Salix Homes will ensure that all breaches are recorded within the breach register and that each breach will be thoroughly investigated in accordance with the Incident Reporting & Management Procedure.

7. Salix Homes will ensure that any breaches, which may affect an individual's rights and freedoms, will be reported to the ICO within 72 hours of becoming aware of the breach.

Record Management

8. The Records Management Procedure provides guidelines on how the business will collect, store, process and retain personal information. In accordance with the Records Management Procedure and its appendix, the Retention Schedule, Salix Homes will:

- Ensure that all personal and special category data is processed under the appropriate legal basis.

- Ensure that all documents are stored in accordance with the Records Management Procedure.

- Ensure that all information is only held for the amount of time detailed within the Retention Schedule, is not kept longer than is necessary and within statutory guidance.

Privacy / Confidentiality

9. The Privacy Statement on the Salix Homes website details how we collect, store, process and retain customer information.

10. The Privacy Statement will be reviewed on an annual basis to ensure it remains relevant and will be updated with any relevant legislative and/or regulatory changes as and when they occur.

11. The Employee Privacy Statement included in each employee contract details how we collect, store, process and retain employee information.

Data Sharing

12. Salix Homes will ensure that a Data Sharing / Processing Agreement is in place for all information that is shared with other organisations.

13. The Data Sharing Procedure and the IT Security framework set out guidelines on the process to follow when sharing information.

14. Salix Homes will ensure that all data shared outside of the business will be transferred in a secure, safe method and will only share information that is necessary for the purpose.

15. Salix Homes commits to informing all customers and employees on the organisation we share their information with. A full description of the types of organisations we share information with can be found in the Privacy Statement located on our website.

16. The Data Sharing Procedure sets out guidelines on the process to follow when sharing information, including tools to use to further protect our customer and employee data.

Individual Rights

17. Salix Homes will ensure that all customers and employees are aware of their individual rights and how to submit an Individual Rights Request. This information can be found in the Privacy Statement on our website.

18. Individual Rights include, but are not limited to:

a. The right to be informed.
b. The right of access.
c. The right to rectification.
d. The right to erasure.
e. The right to restrict processing.
f. The right to data portability.

g. The right to object.
h. Rights in relation to automated decision making and profiling.

19. Salix Homes will exercise any relevant exemptions, permitted by the GDPR, where necessary, which include:

a. national security;
b. defence;
c. public security;
d. the prevention, investigation, detection or prosecution of criminal offences;
e. other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
f. the protection of judicial independence and proceedings;
g. breaches of ethics in regulated professions;
h. monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defense, other important public interests or crime/ethics prevention;
i. the protection of the individual, or the rights and freedoms of others; or
j. the enforcement of civil law matters.

20. The Individual Rights Procedure sets out guidelines on the process to follow when a customer or employee submits an Individual Rights Request.

Data Protection Audits

21. Salix Homes will conduct Data Protection Audits to ensure compliance with the GDPR and the Data Protection Bill 2018.

22. Salix Homes conducts Data Protection Audits to:

a. raise awareness of Data Protection amongst employees;
b. to demonstrate Salix Homes' commitment to, and recognition of, the importance of Data Protection;
c. to ensure all Data Protection policies and practices are adhered to;
d. to identify any potential Data Protection risks we may have been previously unaware of; and
e. to identify any potential training gaps.

23. Salix Homes will endeavour to perform Data Protection Audits each quarter.

Data Protection Impact Assessments (DPIAs)

24. Data Protection Impact Assessments (DPIAs) will be carried out for all new activities using personal information prior to work commencing.

25. All completed DPIAs will be summarised and added to the Salix Homes website.

26. Any DPIA that results in a high residual risk, after all possible mitigations, but which can be objectively justified by the Senior Management Team, will be discussed with the ICO for further advice.

CCTV

27. Salix Homes has CCTV in operation in communal areas of all tower blocks and sheltered accommodations for the prevention and detection of crime. The appropriate notices are present in all areas with CCTV cameras.

28. The CCTV Procedure sets out guidelines on:

a. installing CCTV cameras;
b. the retention period of the footage; and
c. the process of sharing the footage with individuals and other agencies.

Security of Data

29. Salix Homes will ensure that all customer and employee data is held on secure systems and software that restricts access to only those who are required to process the information.

30. Salix Homes requests that all software providers sign up to our IT Security Standards, to demonstrate compliance with the GDPR and the Data Protection Bill 2018.

31. The IT Security Policy stipulates the high level of security that Salix Homes provides for all customer and employee data.

32. The Acceptable Use Procedure sets out guidelines on how those with access to data use Salix Homes' systems and software.

Direct Marketing

33. Salix Homes will use direct marketing to keep all customers updated on community events, to provide information relating to each neighbourhood and to provide offers to all of our customers. We use the following methods to provide these types of information to our customers:

- newsletters;
- e-newsletters;
- magazines;
- texts
- e-mail; and
- phone calls.

34. Salix Homes will provide our community based information under the legal basis of "Legitimate Interests", as we believe that our customers will be interested to hear about offers, events and information relating to their neighbourhoods. All customers are able to opt out of receiving information at any time and further information can be found in our Privacy Statement on the Salix Homes website.

35. The Privacy Statement on the Salix Homes website details all the direct marketing methods that we use and the legal basis we use to process the information.

Training

36. Salix Homes will provide mandatory training to all employees on the importance of Data Protection. Any training gaps that are identified, will be discussed with the appropriate Senior Management team member and additional training will be delivered where necessary.

37. Salix Homes will conduct regular Data Protection awareness campaigns to ensure that Data Protection is continuously at the forefront of everything we do.

4. Service Standards & Performance Measures

Contracts
Salix Homes will ensure that the appropriate Data Protection clauses are included in all procurement contracts which result in the sharing of personal data. Where this is not possible, we ensure that appropriate data sharing/processing agreements are in place

Data Breaches
Salix Homes will ensure that any breach of personal data, that may affect an individual's rights and freedoms, is reported to the ICO within 72 hours of Salix Homes becoming aware of the breach wherever possible.

Salix Homes will investigate and keep a record of all breaches, near misses and compliance concerns reported to the Data Protection Officer and use any appropriate lessons learned to continuously improve.

Data Protection Audits
Salix Homes will ensure that regular Data Protection Audits are completed throughout the business.

Data Protection Impact Assessments (DPIAs)
Salix Homes will ensure that a DPIA is undertaken for all new activities involving the use of personal data**.**

Individual Rights Requests
Salix Homes will endeavour to ensure that 100% of individual rights requests are complied with within one calendar month.

Salix Homes will also endeavour to ensure that 100% of complaints relating to individual rights requests are responded to within 21 calendar days.

Training and Awareness
Salix Homes will ensure that all new employees complete training on GDPR and the Data Protection Bill.

Salix Homes will also ensure that annual refresher training on Data Protection, and related responsibilities, takes place for all employees where appropriate.

5. Risks

Risk of reputational damage – Responsible: Service Directors
Failure to effectively manage compliance with the GDPR and the Data Protection Bill 2018 could result in Salix Homes experiencing reputational damage.

Risk of limited customer intelligence – Responsible: Service Directors
Failure to effectively process and share customer information could result in customers refusing to share personal information with the organisation, which could result in less well informed decisions being

made.

Risk of Information Commissioner intervention – Responsible: Executive Director of Resources / Data Protection Officer
Failure to adhere to the GDPR and Data Protection Bill 2018 could result in the Information Commissioner taking action to change the behaviour of the organisation and the individuals that collect, use and store personal information. In addition to the monetary action detailed in the risk below, the ICO could also pursue a criminal prosecution, non-criminal enforcement and/or an audit.

Risk of Financial penalty – Responsible: Executive Director of Resources / Data Protection Officer
Failure to comply with the GDPR and Data Protection Bill 2018 could result in financial penalties being imposed upon Salix Homes. At present available fines can be up to 2% of our global turnover for minor breaches and up to 4% of our global turnover for major breaches.

Each of these risks can be mitigated by ensuring that the correct policies, procedures and documentation are/is in place and utilised and that all employees are well trained in their responsibilities under the GDPR and Data Protection Bill 2018 and are appropriately supervised.

6. Related Procedures & Documents

Policies/Procedures:

1. IT Security Policy
2. Acceptable Use Procedure
3. CCTV Procedure
4. Confidentiality Procedure
5. Data Sharing Procedure
6. Incident Reporting & Management Procedure
7. Individual Rights Procedure
8. Privacy Procedure
9. Record Management Procedure

Directly linked documents:

i. Data Protection Audit Schedule & Forms
ii. Data Protection Impact Assessment (DPIA) Toolkit & Form
iii. Data Sharing/Processing Form
iv. Incident Reporting Form (Make available online)
v. Individual Rights Request Form (Make available online)
vi. Information Asset Register
vii. Privacy Statement
viii. Retention Schedule
ix. Employee Privacy Statement

Other linked documents:

- Compliance Register
- Data Classification Scheme
- Information Governance Group ToR
- Leaver Form
- New Starter Form
- Procurement Framework
- Risk Register

7. Responsibilities

The application of this policy is the responsibility of all Salix Homes employees and any person handling data on behalf of the organisation, including consultants, volunteers, contractors and suppliers.

In particular, the Data Protection Officer has overall responsibility for ensuring compliance with all Data Protection legislation and shall ensure that:

i. Salix Homes is registered as a Data Controller.
ii. Individuals processing personal information understand that they are responsible for complying with the Data Protection principles.
iii. Individuals processing personal information are appropriately trained to do so.
iv. Individuals processing personal information are appropriately supervised.
v. Individuals are aware of the process to follow if they have any queries when handling personal information.
vi. Enquiries about handing personal information are dealt with promptly and courteously.

8. Related Legislation

(a) the Data Protection Act 1998;
(b) the Data Protection Directive;
(c) the Electronic Communications Data Protection Directive;
(d) the Privacy and Electronic Communications Regulations 2003;
(e) the Human Rights Act 1998;
(f) the European Convention on Human Rights;
(g) the General Data Protection Regulation (GDPR); and
(h) the Data Protection Bill