

Data Protection Policy

Overview:	The Data Protection Policy sets out how the Regenda Group complies with the General Data Protection Regulation 2018 and signposts to relevant Guidance Notes for managing personal data.
Approved by:	Executive Team
Date approved:	23 April 2018
Next review date:	01 April 2021
Champion:	Director of Business Assurance
Lead:	Governance & Risk Manager
Version:	V2.0
Scope:	All Group organisations

Contents

1.	Introduction/ policy statement	3
2.	Scope and exemptions	3
3.	Definitions	3
4.	Data Protection Principles	4
4.1	Lawfulness, fairness and transparency	5
4.2	Purpose limitation	5
4.3	Data minimisation	5
4.4	Accuracy	5
4.5	Storage limitations	6
4.6	Integrity and confidentiality	6
5.	Conditions for consent to processing personal data	6
6.	Restrictions of processing	6
7.	Rights of the data subject	7
7.1	The right to be informed	7
7.2	The right of access	7
7.3	The right to rectification	7
7.4	The right to erasure	7
7.5	The right to restrict processing	8
7.6	The right to data portability	8
7.7	The right to object	8
7.8	Rights in relation to automated decision making and profiling	8
8.	Regenda’s responsibilities as the data controller	9
8.1	Internal Data Protection Policies, Processes and Training	9
8.2	Data Protection by design and by default	9
8.3	Data Processors	9
8.4	Records of processing activities	9
8.5	Security	10
8.6	Notification of a personal data breach to the Information Commissioner’s Office and communication to the data subject	10
8.7	Data Protection Impact Assessment	10
8.8	Transferring data outside of the European Union	10
8.9	Data Protection Officer	10
9.	Associated documents	10
9.1	Associated legislation, regulation and guidance	10
9.2	Associated Group documents/ guidance/ PIs	11
10.	Development and implementation	11
11.	Equality, diversity and human rights	11
12.	Monitoring and reporting	11

1. Introduction/ policy statement

The General Data Protection Regulation 2018 (GDPR) sets out rules for processing personal information. The Regulation applies to personal information that the Regenda Group holds about its customers and employees. The Regulation states that those who record and use personal information must ensure that it is handled properly and in accordance with GDPR. Therefore the Regenda Group are required to ensure that all personal data is managed in accordance with the following principles:

- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitations
- Integrity and confidentiality

The Regenda Group, as data controller is required to demonstrate that it complies with the six data protection principles detailed above.

The Regenda Group is registered with the Information Commissioner's Office (ICO) as a Data Controller under the General Data Protection Regulation 2018 and recognises that all individuals have a right to have their personal information collected, processed and shared in line with GDPR and that all information is kept safe and secure.

2. Scope and exemptions

The Regenda Group is made up of Regenda Homes and its wholly-owned subsidiaries.

This policy applies to all organisations that are part of the Regenda Group and all staff employed within those organisations (including permanent, temporary or contract staff).

3. Definitions

Group: shall mean all Group organisations.

Data Subject: shall mean any living individual who is the subject of personal data. Examples include but are not limited to customers, residents, including prospective/former residents, people who use and/or enquire about our services, visitors to our website, board/committee members, job applicants, current and former employees.

Personal Data: shall mean information about a living individual who can be identified from that information. It also includes any expression of opinion or view about an individual or their circumstances. Examples of personal data include but

are not limited to name, address, housing history, economic status, allowance, benefits and grants, support services received.

Special Category Data: shall mean data that is classed as more sensitive in relation to the fundamental rights and freedoms of the data subject. Examples of sensitive personal data include but are not limited to racial or ethnic origin, political opinions, religious or other beliefs, genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing personal data: the processing of personal data includes collecting, recording, storing and sharing.

Privacy Notice: a statement providing information about what to expect when the Regenda Group collects and processes personal data.

Authority to act: If someone wants a third party (for example, relative or friend) to act on their behalf, they need to complete an Authorisation form.

Data Controller: An individual or organisation who decides how personal data is processed and why it is needed.

Data Processor: means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Officer (DPO): Data Protection Officers are responsible for overseeing data protection and ensuring compliance with General Data Protection Regulation requirements.

Information Commissioner's Office (ICO): the independent supervisory body responsible for regulating General Data Protection Regulation. The ICO's remit is to promote good practice, provide information to individuals and organisations and to take enforcement action where there has been a breach in General Data Protection Regulation.

Subject Access Request: If we hold personal information about someone, they have the right to request access to this information. This is a Subject Access Request.

The Privacy and Electronic Communications Regulations (PECR) 2003: Direct marketing guidance with a focus on calls and texts to individuals, which complements General Data Protection Regulation.

4. Data Protection Principles

Accountability and Governance

The processing of personal data is carried out in accordance with the six data protection principles and the Regenda Group has appropriate governance arrangements in place to demonstrate compliance.

4.1 Lawfulness, fairness and transparency

The data that the Regenda Group collects is processed lawfully, fairly and in a transparent manner.

The Group ensures that before any personal data is processed at least one of the following applies:

- The processing is necessary for the performance of a contract to which the data subject is a party or in order to enter into a contract (i.e. tenancy agreement or lease);
- The data subject has given consent to the processing of the personal data for one or more specific purpose;
- Processing is necessary for compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or for public interest.

To ensure transparency the Regenda Group provides information to all data subjects about what to expect when the Regenda Group collects and processes personal information. The Regenda Group provides privacy information to individuals at the time of collection and has full privacy notices on all of its websites.

4.2 Purpose limitation

The Regenda Group only collects personal data for specific, explicit and legitimate purposes. We do not further process data for other reasons than the fulfilment of the contract or for the purpose in which the data was collected.

4.3 Data minimisation

The Regenda Group limits personal data collection, storage and usage to what is adequate, relevant and absolutely necessary for carrying out the purpose for which the data is processed.

All information processed by the Regenda Group is detailed in the Information Asset Register and further guidance is available within the Data Management Guidance Note.

4.4 Accuracy

The Regenda Group aims to ensure that all personal data is accurate and where necessary kept up to date. Day to day responsibility for data quality rests with all staff and guidance is provided to staff in the Data Management Guidance Note.

4.5 Storage limitations

All records containing personal data are stored in a format which allows identification of the data subject and personal data is not kept for longer than necessary in line with the Group's data retention guidelines.

4.6 Integrity and confidentiality

Appropriate security measures are in place to prevent against unauthorised or unlawful processing, accidental loss, destruction or damage to personal data.

The Group undertakes robust security checks with all customers and data processors before personal data is shared and access to personal data is limited to relevant job roles.

To ensure the security of data, all staff receive compulsory data protection and security training.

5. Conditions for consent to processing personal data

Where the processing of personal data is based on consent, the Regenda Group will clearly record consent and advise the data subject of their right to withdraw their consent at any time.

The Regenda Group processes special categories of personal data, including; racial and ethnic origin, religious beliefs, sexual orientation and data concerning health or medical conditions. Explicit consent is sought from the data subject prior to the processing of special categories of data.

When processing the data of children under the age of 16, consent is obtained from whoever holds parental responsibility for the child.

Children have the same rights as adults over their personal data, these include the right to access their personal data; to request rectification; to object to processing and to have their personal data erased.

6. Restrictions of processing

There are circumstances when obligations under the GDPR become exempt, and the Regenda Group will share personal data to safeguard:

- National security;
- Defence;
- Public security;
- Prevention, investigation, detection or prosecution of criminal offences;

- Other important public interests, in particular economic or financial interests including budgetary and taxation matters, public health and security;
- The protection of judicial independence and proceedings;
- Breaches of ethics in regulated professions;
- Monitoring, inspection or regulatory functions connected to the exercise of official or authority regarding security, defence, other important public interests or crime/ethics prevention;
- The protection of the individual, or the rights and freedoms of others; or
- The enforcement of civil law matters.

7. Rights of the data subject

GDPR provides the following rights for individuals;

7.1 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. The Regenda Group provides clear and transparent privacy information to individuals at the point of collection.

7.2 The right of access

Individuals have the right to access their personal data.

The Regenda Group has a Data Sharing and Subject Access Request Process contained within the Data Management Guidance Note that allows individuals access to their personal data.

7.3 The right to rectification

Individuals are entitled to have personal data rectified if it inaccurate or incomplete.

The Regenda Group aims to ensure that all personal data is accurate and kept up to date and has a Data Management Guidance Note in place that provides staff with the necessary guidance to rectify and update inaccurate data.

7.4 The right to erasure

The right to erasure is also known as 'the right to be forgotten'. This right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. The Regenda Group will erase and prevent further processing in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data has been erased in order to comply with a legal obligation.

Further guidance for staff is contained within the Data Management Guidance Note.

7.5 The right to restrict processing

Individuals have the right to restrict the processing of their personal data. When processing is restricted, the data controller is permitted to store the personal data but not further process it.

Further guidance for staff is contained within the Data Management Guidance Note.

7.6 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily in a safe and secure way, without hindrance to usability.

Further guidance for staff is contained within the Data Management Guidance NoteF.

7.7 The right to object

Individuals have the right to object to processing of personal data, including direct marketing and profiling.

The Regenda Group will only continue to process personal data if it can demonstrate legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

The Regenda Group will, however, stop processing personal data for direct marketing and profiling purposes as soon as an objection is received.

The Regenda Group's privacy notices inform individuals of their right to object.

7.8 Rights in relation to automated decision making and profiling

Individuals have the right not to be subject to a decision based solely on automated processing.

The Regenda Group does not make decisions on staff or customers based wholly on automated means, unless the decision is necessary for entering into or managing a contract.

8. Regenda's responsibilities as the data controller

The Regenda Group demonstrates compliance with the GDPR by implementing the following;

8.1 Internal Data Protection Policies, Processes and Training

The Regenda Group has:

- Data Protection policies and Guidance Notes in place that are regularly reviewed and updated;
- Compulsory data protection training for all staff;
- Regular data protection awareness campaigns;
- Data champions across the Group;
- An internal data protection audit plan;
- An annual data protection compliance statement and report to Board.

8.2 Data Protection by design and by default

The Regenda Group implements appropriate technical and organisational measures to ensure that data protection and privacy is considered for all initiatives that involve the processing of personal data to ensure compliance and good practice. This includes:

- Data minimisation;
- Pseudonymisation and encryption;
- Transparency;
- Allowing individuals to monitor processing; and
- Creating and improving security features on an ongoing basis.

8.3 Data Processors

The Regenda Group has data sharing agreements in place with all data processors and all data processors are required to provide sufficient guarantees that the requirements of the GDPR will be met and the rights of the data subjects protected.

8.4 Records of processing activities

The Regenda Group has an Information Asset Register that documents all of the Group's data processing activities, the purpose of processing, data sharing and retention.

8.5 Security

The Regenda Group has appropriate security measures in place to protect personal data and prevent against unauthorised or unlawful processing, accidental loss, destruction or damage to personal data.

8.6 Notification of a personal data breach to the Information Commissioner's Office and communication to the data subject

A robust data protection breach reporting process is detailed in the Data Management Guidance Note, which ensures that any personal data breaches are reporting to the Information Commissioner's Office within 72 hours.

This Guidance Note also ensures that the data subject is informed of the breach if it affects their rights and freedoms.

8.7 Data Protection Impact Assessment

A data protection impact assessment (DPIA) process is detailed in the Data Management Guidance Note, which helps to identify and minimise the data protection risks associated with:

- Processing that is likely to result in a high risk to the interests of the data subject;
- Projects which require the processing of personal data.

8.8 Transferring data outside of the European Union

The Regenda Group currently uses data processors who store personal data outside of the European Union. The Regenda Group has data sharing agreements in place with these data processors and carry out robust checks to ensure that adequate levels of protection are in place to protect the rights and freedoms of the data subject in relation to the processing of the personal data.

8.9 Data Protection Officer

The Regenda Group has appointed a Data Protection Officer (DPO) to assist in the monitoring of internal compliance, provide advice on the Group's data protection obligations and act as a point of contact for data subjects and the Information Commissioner's Office.

9. Associated documents

9.1 Associated legislation, regulation and guidance

General Data Protection Regulation 2018

The Privacy and Electronic Communications Regulations (PECR)

9.2 Associated Group documents/ guidance/ PIs

The following policies, Guidance Notes and documents should be used in conjunction with this policy:

- Data Management Guidance Note
- Information Asset Register
- Privacy Notices on websites
- Data Sharing Agreement
- Authorisation Form
- Information Security Policy
- Mobile Device Policy
- Staff Handbook
- Safeguarding Policy
- Dealing with Unacceptable Behaviour Policy

10. Development and implementation

This policy has been developed to comply with General Data Protection Regulation and will be implemented through awareness for customers and staff via the Group's websites and newsletters.

11. Equality, diversity and human rights

This policy has been developed to protect all individuals' fundamental rights and freedoms and is necessary and proportionate.

12. Monitoring and reporting

Compliance with this policy will be monitored through a robust internal audit plan and annual report and compliance statement presented to Group's Board.