

Data Protection Policy

Objective

The purpose of this Policy is to ensure compliance with the Data Protection Act 2018 and to ensure that InstaGroup discharges all of its legal obligations in this respect.

Scope

This Policy applies to all activities for which InstaGroup is the data controller and data processor and to all InstaGroup staff (including permanent, temporary and contract staff). The term 'personal data' is defined as 'information that relates to a living individual who can be identified from the data'.

This Policy also applies to members of the InstaGroup Snug Network who are responsible for any aspect of the processing of personal data using InstaGroup's Green Deal SMART Assessment Software either through the hosted Property Hub or Apple iPads.

Responsibilities

This Data Protection Policy has been approved by, and has the full support of, the Directors who are ultimately responsible for compliance with data protection legislation.

The Directors will appoint a Data Protection Officer who has direct responsibility for maintaining this Policy and providing advice and guidance on its implementation. The Data Protection Officer can be contacted at compliance@instagroup.co.uk.

All managers will be responsible for implementing this Policy within their areas of responsibility.

All staff will be provided with education and training and will be expected to comply with data protection legislation and adhere to InstaGroup's policies and procedures.

Each company that is a member of the InstaGroup Snug Network will appoint a Data Protection Officer who has responsibility for the implementation of this Policy within their company and for ensuring that the member company's policies and procedures are aligned with this Policy, for all work undertaken for InstaGroup Limited.

Policy Statement

It is the policy of InstaGroup that:

- Personal data shall be processed fairly and lawfully
- Personal data shall only be obtained for specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive to the purpose(s) for which they are processed
- Personal data shall be kept accurate and up to date
- Personal data shall not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of the data subjects

- Personal data shall be protected from unauthorised and unlawful processing and against accidental loss or destruction or damage by appropriate technical and organisational controls
- Personal Data must not be copied or saved to personal PCs/personal portable devices
- Personal data shall not be transferred to a country or territory outside the EEA unless an adequate level of protection of the rights and freedoms of the data subject(s) can be guaranteed

Further policies and procedures may be produced to support this Policy.

Principles

The following principles shall be complied with throughout InstaGroup and the InstaGroup Snug Network.

- 1. Lawfulness, Fairness and Transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
- 2. Purpose Limitation** - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- 3. Data Minimisation** - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 4. Accuracy** - Personal Data shall be accurate and, where necessary kept up to date.
- 5. Storage Limitation** - Personal data shall be kept in a form, which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed.
- 6. Integrity & Confidentiality** - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.
- 7. Accountability principle** - We must demonstrate that the six Data Protection Principles are met for all personal data for which it is responsible.

Every person associated with Insta who processes or uses any personal data must abide by these Principles at all times. In order to ensure that this happens, we have developed this Data Protection Policy.

Personal Data Quality

- All forms used to collect personal data shall only ask for information which is relevant to the purpose of the form, including those forms processed electronically
- Staff have the opportunity to confirm the accuracy of personal data held by HR by updating the HR Toolkit.
- Changes in personal data relating to data subjects must be promptly and accurately updated on the appropriate system(s)

Subject access

Where an individual makes a request relating to any of the rights listed above, we will consider each such request in accordance with all applicable Data Protection laws and regulations. No

administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

Data Subjects shall have the right to require us to correct or supplement erroneous, misleading, outdated, or incomplete personal data. If we cannot respond fully to the request within 30 days, the DPO shall provide the following information to the Data Subject or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date. Details of any requested information or modifications which will not be provided to the
- Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the appropriate individual who the Data Subject should contact for follow up.

Personal data retention

- Personal data shall not be retained for longer than is required for the purpose for which it was collected.
- Staff will review customer information whenever accessed then remove and securely destroy any information which is beyond its retention period.
- Instagroup will require all data processors to formally agree that personal data will not be retained for longer than the purpose for which they are processing it.

Staff awareness

- Data protection training will be included in the staff induction process
- All new staff will receive data protection training relevant to their role as soon as possible following commencement of their employment.
- All staff will receive data protection training periodically.
- Guidance material will be available to all staff who process personal data.

Governance

This Policy will be reviewed regularly, at least on an annual basis, by the Data Protection Officer. Any changes will be passed to the Directors for approval.