

ESTATE INSURANCE GROUP

Data Protection Policy

1. Purpose

- 1.1 The Data Protection Act 1998 (“the Act”) has two principal purposes:
- 1) To regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals, of those personal data; and
 - 2) To provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.
- 1.2 The cornerstones of the Act are the eight data protection principles, which prescribe:
- 1) Guidelines on the information life-cycle (creation/acquisition; holding; processing; querying, amending, editing; disclosure or transfer to third parties; and destruction (“the life-cycle”);
 - 2) The purpose for which data are gathered and held; and
 - 3) Enshrine rights for data subjects.

The Act applies to EIG, the Data Controller for the purposes of the Act, and to anyone who holds personal information in a structured way so that retrieval is easy. The Company is fully committed to abiding, not only by the letter, but also by the spirit of the Act, and, in particular, is committed to the observation, wherever possible, of the highest standard of conduct mandated by the Act. This policy has been written to acquaint staff with their duties under the Act and to set out the standards expected by the Company in relation to processing of personal data and safeguarding individuals’ rights and freedoms.

2. Staff Duties

Employees of the Company are expected to:

- 1) Acquaint themselves with, and abide by, the Data Protection Principles;
- 2) Read and understand this policy document;
- 3) Understand how to conform to the standard expected at any stage in the life-cycle;
- 4) Understand how to conform to the standard expected in relation to safeguarding data subjects’ rights (e.g. the right to inspect personal data) under the Act;
- 5) Understand what is meant by “sensitive personal data”, and know how to handle such data; and
- 6) Contact the Data Protection Officer if in any doubt, and not to jeopardise individuals’ rights or risk a contravention of the Act.

3. The Data Protection Principles

The Data Protection Principles, in summary, are:

- 1) Personal data shall be processed fairly and lawfully.
- 2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- 3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- 4) Personal data shall be accurate and, where necessary, kept up to date.
- 5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- 6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
- 7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Best-Practice guidelines for the life-cycle process

4.1 Holding/safeguarding/disposal of personal data (see Principles 4,5 and 7)

Data should not be held for longer than is necessary. The Company's records management policies should be consulted for guidance on what is necessary for each kind of data.

Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken.

4.2 Processing of personal data (see Principles 1,2)

In this particular context, "processing" is used in the narrow sense of editing, amending or querying data. In the context of the Act as a whole, 'processing' is very widely defined to include acquisition, passive holding, disclosure and deletion.

Personal data must not be processed except for the purpose(s) for which they were obtained or for a similar, analogous purpose. If the new purpose is very different, the data subject's consent must be obtained.

4.2.1 Disclosures

The Company's policy is to exercise its discretion under the Act to protect the confidentiality of those whose personal data it holds.

4.2.2 Transfers

Personal data should not be transferred outside the Company, and in particular not to a country outside the EEA.

- 1) Except with the data subject's consent; or
- 2) Unless that country's data protection laws provide an adequate level of protection; or
- 3) Adequate safeguards have been put in place in consultation with the Data Protection officer; or

- 4) In consultation with the Data Protection Officer, it is established that other derogations apply.

4.3 Destruction of personal data (see Principles 5 and 7)

Personal data must not be held for longer than necessary; and when such data have been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

5. **Data subjects' rights of access**

The Company is fully committed to facilitating access by data subjects to their personal data, while bearing in mind the need to protect other individuals' rights of privacy.

All data subjects will be expected to fill in a Subject Access request form, obtainable from the ICO web-site.

The fee for a subject access request is £10. All subject access requests are to be forwarded to the Data Protection Officer or Director, if they have not already been addressed to him.

6. **Review**

This policy will be reviewed periodically to take account of changes in the law and guidance issued by the Information Commissioner.

7. **Data protection contacts**

For general enquires about the Company's Data Protection Policy and for formal subject access requests under the Act:

Jeremy Stephen - Director

8. **Disciplinary consequences of this policy**

Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA in contravention of paragraph 4.4.2 above) or any other breach of section 55 of the Data Protection Act 1998 by staff will be treated seriously by the Company and may lead to disciplinary action.