DATA PROTECTION /
PRIVACY POLICY

GUIDING PRINCIPLE

Any individual about whom you keep personal data electronically or manually is entitled to a copy of the data you are keeping about them upon making an access request. Lee Insurance Brokers acts as both a Data Controller and Data Processor. You should not disclose any information about an individual to a third party unless you are satisfied that you have that individual's consent.

1. Purpose of Data Protection

The *Data Protection Act 1988* and the *Data Protection (Amendment) Act 2003* govern the processing of all personal data. The purpose of these Acts is to safeguard the privacy rights of individuals regarding the processing of their personal data by those who control such data. In particular, it provides for the collection and use of data in a responsible way, while providing against unwanted or harmful data use.

2. Purpose of Policy

The purpose of this policy is to set out the arrangements that apply to the management of data protection and to affirm our commitment to protect the privacy rights of individuals in accordance with legislation. This policy sets out the many areas of our work in which data protection issues arise and outlines best practice in dealing with these issues.

3. Definitions - Data Protection Acts

The following definitions have been adapted from Section 1 of the Data Protection Acts:

- ***Data:*** means automated and manual data. Automated data means any information on computer, or information recorded with the intention that it be processed by computer. Manual data means information that is recorded as part of a relevant filing system or with the intention that the data form part of a system. Examples of sensitive data which we hold include, names, addresses, bank details, PPS numbers, dates of birth, bank account details/statements, financial audit reports, financial/grant payment schedules, tender documents etc.

- ***Data controller:*** means a body that, either alone or with others, controls the content and use of personal data

- ***Data processor:*** means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment

- ***Data subject:*** means an individual who is the subject of personal data

- ***Personal data:*** means data relating to a living individual who is or can be identified either

from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

- ***Processing:*** means performing any operation/sets of operations on the data, whether or not by automatic means, including:

    - obtaining, recording or keeping the information
    - collecting, recording, organizing, storing, altering or adapting the information or data
    - retrieving, consulting or using the information or data
    - disclosing the information or data by transmitting, disseminating or otherwise making them available
    - aligning, combining, blocking, erasing or destroying the information or data.

- ***Relevant filing system:*** means any set of information relating to individuals (to the extent that while not computerized) which is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

- ***Sensitive personal data:*** means personal data which relates to specific categories defined as:
    - racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
    - trade union membership
    - the physical or mental health or condition or sexual life of the data subject
    - the commission or alleged commission of any offence by the data subject
    - any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

4. Data Protection Principle

As a Data Controller, Lee Insurance Brokers must comply with the eight principles of Data Protection as set out in the Data Protection Acts and administer our legal responsibilities in accordance with these stated principles as follows:

1) obtain and process information fairly
2) keep data only for one or more specified, explicit and lawful purposes
3) use and disclose data only in ways compatible with these purposes
4) keep data safe and secure
5) keep data accurate, complete and, where necessary, up-to-date
6) ensure that data is adequate, relevant and not excessive
7) retain data for no longer than is necessary for its purpose or purposes
8) give a copy of their personal data to an individual, on request, and correct the data or, in certain cases as defined in the Data Protection Acts, block or erase the data where that individual so requests. Depending on the business and who the Data Controller is.

5 Application of the rules of data protection

In order to ensure that Lee Insurance Brokers complies with these principles, the following procedures must be observed at all times.

5.1 Obtaining and processing personal data

- personal data is obtained fairly if the data subject is aware of the purpose for which Lee Insurance Brokers is collecting the data, of the categories of person/organization to whom the data may be disclosed, of non-obligatory or optional answers in forms, of the right of access to the data and of the right of rectification of the data
- obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data is necessary for fulfilling that purpose and ensure data is used only for that purpose
- it follows that use of Lee Insurance Brokers data processing facilities in capturing and storing personal data for purposes, which are not related to the functions of Lee Insurance Brokers must not take place
- inform data subjects of what personal information is held by Lee Insurance Brokers, what it will be used for and to whom it may be disclosed
- obtain written consent when processing sensitive data and retain a copy of the consent. It should be noted that consent cannot be inferred from a non-response in the case of sensitive (see definition in Section 3 above) data.

5.2 Disclosing personal data

- personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data is being kept. Special attention should be paid to the protection of sensitive personal data, the disclosure of which would normally require explicit consent
- except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, do not disclose to any third party any personal data without the consent of the data subject.
- verbal consent does *not* suffice in the case of sensitive personal data. Written consent must be obtained unless there is a statutory obligation to disclose, or the information is released, for example to the Gardaí, for the prevention of crime and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interests of the data subject
- personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfill administrative functions. Be satisfied of the need to disclose
- personal data should not be disclosed outside of the EEA unless written consent has been obtained, unless disclosure is required for the performance of a contract, to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

5.3 Permitted disclosures of personal data

The Data Protection Acts provide for disclosures, where data is:

- authorized for safeguarding the security of the State
- required for the purpose of preventing, detecting or investigating offences apprehending or prosecuting offenders, or assessing moneys due to the

State
- required to protect the international relations of the State

- required urgently to prevent damage to health or serious loss/damage to property
- required under law
- required for legal advice or legal proceedings
- disclosed to, at the request of or with the consent of the data subject.

5.4 Securing personal data

Lee Insurance Brokers must protect personal data from unauthorized access when in use and in storage and it must also be protected from inadvertent destruction, amendment or corruption.

- personal electronic data should be subject to stringent controls, passwords, encryption, access logs, backup, etc.
- screens, printouts, documents, and files showing personal data should not be visible to unauthorized persons.
- personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited or restricted access.
- subject to in-house retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has Expired and contractual obligations upheld.
- when upgrading or changing PC, the hard drive should be wiped by an appropriate ICT staff member or returned to funder as required.
- special care must be taken where laptops, PC's and mobile storage devices such as USB Keys containing personal data are used outside of Lee Insurance Broker's office.

5.5 Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data is accurate, complete and kept up-to-date. Review and audit procedures should be developed to monitor that this is being achieved.

5.6 Retention of personal data

Data should not be kept for longer than is necessary for the purpose for which it was collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose. Personal information should only be held for periods specified in the Lee Insurance Brokers Records Retention Policy.

5.7 Disposal of personal data

Personal data should be disposed of when it is no longer needed for the effective functioning of Lee Insurance Brokers. The method of disposal should be appropriate to the sensitivity of the data, such as shredding in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken when PC's are transferred from one person to another or outside Lee Insurance Brokers or are being disposed of.

5.8 Rights of data subjects

Right of access
The Act provides for the right of access by the data subject to his or her personal information. Data subjects must be made aware of how to gain access to their personal data. A data subject is entitled to be made aware of his or her right of access and to the means by which to access the data. A data subject is entitled to the following on written application within forty days, or sixty in the case of examination data:

- a copy of their personal data;
- the purpose of processing the data;
- the persons to whom the Lee Insurance Brokers discloses the data;
- an explanation of the logic used in any automated decision-making;
- copy of recorded opinions about him or her, unless given in confidence

- A maximum fee of €6,35

- may be charged for access to their personal information.

5.9 Restriction of rights of access

This right of access is restricted where the data is:

- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- subject to legal professional privilege
- kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects
- back-up data.

5.10 Provision of access to third parties

A data subject is entitled to access his or her own personal data only. The personal information of a data subject including contact details, must not be disclosed to a third party without the consent of the individual concerned. An agreement may be made to forward a communication to a data subject on behalf of a third party, but no information should be disclosed about the data subject. In the case of research surveys where there is an agreement to forward documentation to data subjects, a notice should be included to the effect that no personal information has been released.

5.11 Limitations on the use of personal data for research
Where research is being carried out either by staff or outside consultants involved in collecting personal data (especially sensitive personal data) they are bound by the requirements of the Act. Initially, they must ensure that data is obtained and processed fairly. It is essential that the necessary consent from data subjects is obtained. Whenever possible, personal data should be rendered anonymous. The Act requires that personal data shall be kept only for

one or more specified, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those.

5.12 Right of rectification or erasure

Data subjects have a right to have personal data rectified or, blocked from being processed or erased where the data controller has contravened the Act. In order to comply with this right of access, rectification or erasure, it must be ensured that personal data can be located and collated quickly and efficiently by:

- ensuring personal data is in a format that is easy to locate and collate
- verifying that the access request and the personal data released refer to the same individual
- knowing exactly what data is held on individuals, and by whom
- holding personal data in a secure central location.

5.13 Responsibilities of data subjects

All staff and other data subjects should be informed of how to keep their personal data up to date. All staff and other data subjects are responsible for:

- checking that any information they provide to Lee Insurance Brokers is accurate and up to date
- informing Lee Insurance Brokers of any changes of information that they have provided, such as changes of address
- checking the information Lee Insurance Brokers sends out from time to time, giving details of information kept and processed
- informing Lee Insurance Brokers of any errors or changes (Lee Insurance Brokers cannot be held responsible for any errors unless previously informed).

5.14 Departmental Responsibility

Chief Privacy Officer

- Patrick Lee
- Administration – Ann-Marie Roe

6. Further information

These guidelines are intended as a general introduction and are not an authoritative interpretation of the law. Extensive information is available from the Data Protection Commissioner's website, www.dataprotection.ie, or from the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois.

7. Review

This policy has been developed in consultation with staff and it will be reviewed periodically to ensure it remains up-to-date and consistent with developments in good employment practice. All Lee Insurance Brokers staff are welcome to contribute their experiences and opinions as part of this and staff will be notified of any revisions that are made.