# Data Protection Policy

*Incorporating*

*Brian Johnston & Co (Insurance Brokers) Limited*

*Linkfield Accident Management Limited*

# Data Protection

The Company has adopted the following Policy in relation to the collection, storage and processing of personal information.

**Scope**

Acceptance of and adherence to this Policy forms part of every employee's contract of employment.

**Principles**

The Company will comply with all applicable requirements of current data protection legislation including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation ((EU) 2016/679) (GDPR) in force from time to time and any applicable national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then any replacement legislation in the UK to the DPA and the GDPR.

This Policy applies to all personal data held by the Company. The term Data Subject is used in respect of any individual for whom the Company holds personal data on.

The Policy should be read in conjunction with the Company's Privacy Policy. The Company has separate privacy policies for customers, employee, and job applicants.

The Company has taken steps to protect the security of personal data in accordance with its Data Security Policy and will train staff about their data protection responsibilities as part of the induction process. The Company will only hold data for as long as necessary for the purposes for which we collected it.

The Company is a 'Data Controller' for the purposes of personal data. This means that we determine the purpose and means of the processing of personal data.

This Policy explains how the Company will hold and process personal information. It explains the rights of data subjects. Data subjects is the term given to the individuals for who the Company holds personal data.

**Data Protection Principles**

In order to operate effectively and fulfil its legal obligations, the Company needs to collect, maintain and use certain personal information about current, past and prospective employees, customers, suppliers and other individuals with whom it has dealings.

The Company is committed to the 8 principles of data protection as detailed in the DPA. These principles require that personal information must:

1. be fairly and lawfully processed and not processed unless specific conditions are met;
2. be obtained for one or more specified, lawful purposes and not processed in any manner incompatible with those purposes;
3. be adequate, relevant and not excessive for those purposes;
4. be accurate and, where necessary, kept up to date;
5. not be kept for longer than is necessary;
6. be processed in accordance with the data subject's rights under the DPA;
7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage;

8. not be transferred to countries outside the European Economic Area (EEA) unless the country or territory ensures adequate protection for the rights and freedoms of the data subjects.

**Data Protection Principles under GDPR**

The Company uphold and adheres to the data protection principles as set out in Article 5 of the GDPR:

Personal information must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. accurate and, kept up to date; with every reasonable step taken to ensure that personal data that is inaccurate, is erased or rectified without delay;

5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

6. 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, using appropriate technical or organisational measures.

**Personal Data**

Personal Data refers to any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

**Sensitive Personal Data**

Sensitive Personal Data are types of personal data consisting of information as to:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic or biometric data;
- health;
- sex life and sexual orientation;
- criminal convictions and offences.

The Company may hold and use any of these special categories of personal data, as detailed in the Privacy Notice, in accordance with the law.

**Individual Rights**

Under the GDPR Data Subjects have rights in relation to how the Company uses their personal information. They are:

- **Right to be informed** - Data Subjects have a right to receive clear and easy to understand information on what personal information the Company has, why it is held and who the Company share it with;
- **Right of access** - Data Subjects have the right of access to their personal information. If a Data Subject wishes to receive a copy of the personal information the Company holds, the Data Subject may make a data subject access request (DSAR);
- **Right to request that Data Subjects personal information be rectified -** If Data Subject's personal information is inaccurate or incomplete, the Data Subject can request that it is corrected;
- **Right to request erasure -** Data Subjects can ask for the personal information the Company holds on them to be deleted or removed if there is not a compelling reason for the Company to continue to hold it;

**Note: The Company's website includes a form to enable Data Subjects to request erasure.**

- **Right to restrict processing -** Data Subjects can ask that the Company blocks or suppresses the processing of their personal information for certain reasons. This means that the Company is still permitted to keep the information but must ensure it is not used in future for those reasons Data Subjects have restricted;
- **Right to data portability -** Data Subjects can ask for a copy of their personal information for their own purposes to use across different services. In certain circumstances, Data Subjects may move, copy or transfer the personal information held to another Company in a safe and secure way. For example, if a Data Subjects were moving their information from one back-office system to another provider;
- **Right to object -** Data Subjects can object to the Company processing their personal information where it is based on legitimate interests (including profiling), for direct marketing (including profiling) and if the Company was using that data for scientific/historical research and statistics.

**Processing Personal Data**

In order to comply with the law, the Company will:

- always ensure there is a lawful reason for the collection, processing and sharing of personal data;
- observe fully all conditions regarding the fair collection and use of personal information;
- meet its legal obligations to specify the purpose for which information is used;
- collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with legal obligations;
- ensure the quality of the personal information used;
- apply strict checks to determine the length of time personal information is held;
- ensure that individuals about whom information is held are able to exercise their rights under the DPA and GDPR, including the right to be informed that processing is taking place, the right of access to their own personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase incorrect information;
- take appropriate technical and organisational security measures to safeguard personal information;

- ensure that personal information is not transferred outside the EEA without suitable safeguards.

**Lawful Basis for Processing**

The Company will always have a lawful basis for the processing of personal data. The GDPR sets out six available lawful bases for processing. These are:

1. Consent;
2. Contract;
3. Legal obligation;
4. Vital interests;
5. Public task;
6. Legitimate interests.

The GDPR allows EU member states limited provisions for how it applies in their country. The provisions adopted by the UK Governments are set out in the DPA. Section 20 of the Act details the provision with regards insurance.

Section 20 allows a firm to process personal data when processing involves insurance. The term insurance contact applies to:

- Advising on, arranging, underwriting or administering an insurance contract;
- Administering a claim under an insurance contract; or
- Exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

Processing can reasonably be carried out without the consent of the data subject only where:

- The controller cannot reasonably be expected to obtain the consent of the data subject; and
- The controller is not aware of the data subject withholding consent.

Data will be processed under the provisions set out under Section 20 of the DPA, through consent, legal obligations or legitimate interests. The Company's Privacy Statement provides further information.

**Personal Data Breaches**

The Company will report certain types of personal data breach to the Information Commissioner's Office. The Company will do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Company will inform those individuals without undue delay.

The Company has in place robust breach detection, investigation and internal reporting procedures.

The Company keep a record of any personal data breaches, regardless of whether or not the breach is notifiable.

**Accountability and Governance**

- Accountability is one of the data protection principles - it makes the Company responsible for complying with the GDPR and requires it to be able to demonstrate compliance;
- The Company has in place appropriate technical and organisational measures to meet the requirements of accountability such as adopting a Data Security Policy;
- Data Protection is integral to the Company's philosophy and all new systems are designed with data protection at their core;
- The Company is Cyber Essentials certified;

- Appropriate written contracts are place with organisations that process personal data on the Company's behalf;
- The Company maintains documentation of its processing activities;
- The Company has implemented appropriate security measures including third party penetration testing;
- The Company will record and, where necessary, report personal data breaches to the Information Commissioner's Office;
- The Company carries out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- The Company has appointed its HR & Compliance Officer as the Data Protection Officer;
- As an Insurance Broker, the Company will adhere where possible to templates and guidance issued by the British Insurance Brokers Association;
- The Company understands that Data Protection obligations are ongoing, and processes and procedures are reviewed and updated as and where required.

**Responsibilities**

Whilst the Chief Executive Officer has ultimate responsibility for compliance of this Policy, each Director is also accountable to this Policy. The Board has appointed the HR & Compliance Officer as the Data Protection Officer (DPO), supported by the Business Systems Analyst (BSA), to be responsible for developing and encouraging good information handling practice amongst all employees of the Company. The Board will work with the DPO and BSA to ensure the success of this Policy.

Employees whose role involves the collection, maintenance and processing of personal information about other employees, customers, suppliers or any other individuals with whom the Company has dealings are responsible for following the Company's rules and procedures on good data protection practice as notified from time to time by their Line Manager.

**Data Security Policy**

The Company has in place a Data Security Policy (DSP) to protect the Company, its staff, clients and the public from information security threats, whether internal or external, deliberate or accidental. Information, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected. Confidentiality, integrity and availability of information are essential to maintain legal compliance. The DSP Policy statement has been created to:

- Safeguard the personal information of all clients;
- Safeguard the business information of all corporate clients;
- Protect the business interests of the Company;
- Comply with the DPA and GDPR.

All staff will receive training on the DPA, GDPR, and the DSP. Employees are subject to monitoring, auditing and performance reviews to ensure compliance in the handling of Personal Data.