FIRST OPTION
safety consultants

GDPR & DATA PROTECTION POLICY

1. GDPR and Data Protection Policy

This sub-policy specifies the controls that need to be applied to the storage, processing and dissemination of Personal Information that is accessed, stored or processed by the company to ensure that First Option complies with and can demonstrate compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

1.1. **Data Officer**

The Chief Operating Officer will act as the Data Officer whose contact details are published on the company's website. They will:

1.1.1. Report directly to the Senior Management Team and be involved properly and in a timely manner in all issues which relate to the protection of Personal Information;

1.1.2. Have the full support of Senior Management in performing their tasks.

1.1.3. Be provided with all resources necessary to carry out the tasks required by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

1.1.4. be provided with all the resources necessary to maintain their expert knowledge;

1.1.5. have unlimited access to Personal Information processing operations.

1.1.6. not be dismissed or penalised by the Senior Management for performing tasks and duties required of them by the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

1.1.7. Not undertake any other tasks and duties that result in a conflict of interest.

1.1.8. It is the responsibility of the Data Officer to:

1.1.8.1. Inform and advise Senior Management, users and any suppliers who undertake processing of Personal Information on behalf of First Option, of their obligations in regard to this policy and the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

1.1.8.2. Monitor First Option's compliance with this policy, the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

1.1.8.3. Ensure all employees have appropriate training with regards to processing of Personal Information.

1.1.8.4. Act as a contact point for the Information Commissioner's Office on issues relating to the processing of Personal Information.

1.2. **Application of the Personal Information protection principles**

The following principles must be applied and compliance with them demonstrated in relation to all Personal Information that is accessed, stored or processed by employees, and employees or suppliers, while they are accessing or processing First Option's information assets and any Personal Information that First Option is the Controller of or processing on behalf of another Controller:

1.2.1. Personal information shall be processed lawfully, fairly and in a transparent manner.

1.2.2. Personal information shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.

1.2.3. Any Personal Information collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

1.2.4. Any Personal information processed shall be accurate, kept up to date (where necessary) and every reasonable step taken to ensure that Personal Information that is inaccurate with regards to the purposes for which it is processed is erased or rectified without delay.

1.2.5. Personal information shall not be kept in a form that permits identification of Information Subjects for longer than is necessary for purposes for the which the personal information is processed (Personal Information may be put Beyond Use where deletion is not reasonably feasible).

1.2.6. Appropriate technical and company measures shall be taken to ensure appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

1.2.7. All processes and operations that involve the processing of Personal Information must be designed to ensure that these principles can be achieved and are applied.

1.3. **Registration with the Information Commissioner**

It is the responsibility of the Chief Operating Officer to ensure that the appropriate registration is maintained with the Information Commissioner.

1.4. **Personal Information Processing Register**

It is the responsibility of the Managing Director to ensure that a **Personal Information Processing Register** is maintained that contains information on:

1.4.1. All Personal Information that First Option is the Controller of regardless of whether it is processed by First Option or by a Processor engaged by First Option.

1.4.2. All Personal Information that First Option is a Processor of on behalf a Controller or other Processor.

1.4.3. The types of Information Subjects that the Personal Information relates to, the limit of the information collected and the source that it is obtained from.

1.4.4. The reason the processing is undertaken and the legal grounds for doing so.

1.4.5. The types of processing employed, and the methods and technologies used.

1.4.6. The details of any Processers used (where First Option is the Controller) or direct Sub-Processors used (where First Option is the Processor).

1.4.7. The country or region where the Personal Information is processed and stored;

1.4.8. All recipients of the Personal Information.

1.4.9. The period for which the Personal Information is retained and the justification for doing so.

1.4.10. Whether any Automated Processing is undertaken.

1.4.11. Whether the Personal Information falls into a Special Category and if so the processing justification offered by Article 9 of the General Data Protection Regulation (EU 2016/679) that applies.

1.4.12. Whether the Personal Information is transferred in any way outside of the EU and if so the countries/territories/companies it is transferred to.

1.5. **Consent to process Personal Information**

Where First Option is a Controller of Personal Information and it undertakes processing of Personal Information requiring the consent of the Information Subject, a record of the consent must be obtained from the Information Subjects.

1.6. **Processing of Personal Information obtained from an Information Subject or from third parties**

1.6.1. Where First Option has collected personal data directly from an Information Subject or from a third party (i.e. not directly from the Information Subjects it relates to), they must be provided with a **Privacy Notice** that contains at least the following information who consent to the processing of their Personal information of the name and contact details of First Option's Data Protection Officer.

1.6.2. The scope and legal justification of processing that will be undertaken with the information they provide.

1.6.3. Where the legal justification for processing the Personal Information is the Controller's legitimate interest, details of the legitimate interest.

1.6.4. Where the legal justification for Processing the Personal Information is that the Information Subject has consented to the processing, the existence of a right to withdraw consent at any time, without affecting the lawfulness of the processing carried out prior to the withdrawal.

1.6.5. The categories of recipients who will have access to their Personal Information;

1.6.6. The time period for which their information will be stored or the criteria that will be applied to determine the time period.

1.6.7. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

1.6.8. Any planned transfers of their information to a third country or international company and information on the safeguards being applied and the means by which the Information Subject can obtain a copy of them or where they are available.

1.6.9. Whether any automated decision-making will be applied to their information and if so, the logic that will be applied and the envisaged consequences for them.

1.6.10. Whether First Option is a joint Controller of the information and if so and overview of the agreement in place with other joint Controllers.

1.6.11. Their rights to:

1.6.11.1.1. Request access to their information.

1.6.11.1.2. Request corrections be made to their information.

1.6.11.1.3. Request their information be deleted.

1.6.11.1.4. Request that processing of their information is restricted.

1.6.11.1.5. Request their information be transferred to another Controller.

1.6.11.1.6. Lodge a complaint with the Information Commissioner.

1.6.11.1.7. The means by which they can notify First Option to exercise one or more of these rights.

1.7. **Accessing, processing and storage of Personal Information**

The Chief Operating Officer must ensure that appropriate physical and technical controls are in place to:

1.7.1. Protect the confidentiality, integrity and availability of all Personal Information.

1.7.2. Prevent unlawful processing of Personal Information.

1.7.3. Personal information should be accessed, processed and stored only to:

1.7.3.1.1. Fulfil the needs of clients/customers.

1.7.3.1.2. Comply with legal requirements.

1.7.3.1.3. Enable the effective implementation of the company's ISMS.

1.7.3.1.4. Personal information should be accessed, processed and stored in accordance with this policy, and the Information Classification, Labelling and Handling Rules.

1.8. **Requests by Information Subjects to exercise their rights and freedoms**

For all Personal Information that First Option is the Controller of:

1.8.1. All requests by Information Subjects whose Personal Information is processed by First Option, to exercise their rights and freedoms under the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) will be managed in accordance with ICO Procedures.

1.8.2. Any information that needs to be provided to Information Subjects who submit requests will be provided in a concise, transparent, intelligent and easily accessible form, using clear and plain language.

1.8.3. Any information requested by Information Subjects in the relation to any of their Personal Information processed by First Option that First Option is legally obliged to provide, will be provided free of charge unless the request if manifestly unfounded or excessive, in which case First Option may change a reasonable fee for providing the information of refuse to act on the request.

1.8.4. Where the request covers the deletion of information that has been made public then First Option will take all reasonable steps possible to inform other Controllers who are processing the information to delete any copy of the information that they hold or any links they have to the information.

1.9. **Transferring Personal Information**

1.9.1. Any transfer of personal information to a third party must be carried out under a written agreement, setting out the scope and limits of the sharing and in accordance with the Information Classification, Labelling and Handling Rules.

1.9.2. In the event that First Option needs to transfer Personal Information to a non-EU country or an international company then:

1.9.2.1.1. Relevant Privacy Notices needs to be updated to reflect this.

1.9.2.1.2. The Information Subjects affected must be informed before the transfer takes place and provided with information regarding the safeguards that First Option will ensure are in place.

1.10. **Compliance and Controls Assessments**

Assessments will be made at regular intervals to ensure that:

1.10.1. All controls employed to protect Personal Information is controlled or processed by First Option are maintained and effective.

1.10.2. First Option complies with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679).

1.10.3. A schedule of audits will be completed as detailed in the **Internal Audit Plan**.

1.11. **Arrangements with Joint Controllers**

Where First Option is a joint Controller of any Personal Information then a Joint Controller Agreement (or an equivalent agreement) will be implemented with any joint Controllers.

1.12. **Arrangements with Controllers**

Where First Option undertakes processing on behalf of a Controller

1.12.1. A Personal Data Processing Contract will be (or an equivalent agreement) will be implemented with any Processors.

1.12.2. No processing of information provided by the Controller will be undertaken without an explicit instruction from them.

1.13. **Arrangements with Processors**

Where First Option uses a supplier to undertake processing on its behalf:

1.13.1. A Personal Data Processing Contract will be (or an equivalent agreement) will be implemented with any Processors.

1.13.2. Before changing supplier or taking on a new supplier, any applicable Controllers will be notified in writing of the change and provided with an opportunity to object to the change.

1.13.3. A Personal Information Processor Assessment will be completed to assess whether they can provide sufficient guarantees to implement appropriate control measures that will ensure the processing they undertake complies with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679) and protects the rights and freedoms on the Information Subjects whose information they process on behalf of First Option.

1.13.4. An audit of a supplier's compliance with the Data Protection Act 2018 and the General Data Protection Regulation (EU 2016/679 will be undertaken where:

1.13.4.1.1. The information obtained from a **Personal Information Processor Assessment** raises doubts as to the adequacy of the guarantees provided by a Processor, or

1.13.4.1.2. The supplier is undertaking High Risk Processing, or

1.13.4.1.3. An information security incident occurs that has a significant impact on the confidentiality or integrity or availability of any Persona Information and following an investigation of the root cause of the incident, the controls and processes employed by the supplier are identified as having been a contributing factor.

1.14. **High Risk Processing**

1.14.1. A data impact assessment must be completed for any High Risk Processing of Personal Information that First Option is a Controller of before any such processing is started.

1.14.2. If a data impact assessment indicates that the processing would result in a high risk to the rights and freedoms of the Information Subjects whose Personal Information is being processed, the Chief Operating Officer must consult with the Information Commissioner's office before any processing is started.

1.15. **Personal Information Breaches**

1.15.1. In the event of a Security Incident that compromises the confidentiality, integrity or availability of any Personal Information actions shall be taken and records maintained in accordance with the **ICO Procedures**