DATA PROTECTION POLICY

This Policy

This document outlines GearedApp LTD's committed and approach to data protection, for the purpose of withholding best practice and ensuring the safety of our clients, staff and other individuals.

All activities are carried out in line with relevant UK and EU legislation. This includes, but is not limited to the Data Protection Act 1998 (DPA), the EU Data Protection Directive 95/46/EC, and the forthcoming EU General Data Protection Regulation ("GDPR").

Data Protection Principals

The eight data protection principals are as follows:

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.

Our commitment

We are committed to:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff who handle personal data, so that they can act confidently and consistently
- Notify the Information Commissioner voluntarily, even if this is not required

Staff Responsibilities

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Directors and Senior management have a responsibility to review and develop data protection policies, implement procedures and ensure notification and briefing to the board and the ICO.

Security

Set measures are in place to ensure that security is withheld at GearedApp. These include, but are not limited to:

- The use of secure and encrypted services where personal data is involved
- Password protection for all equipment and hardware
- Clear desk, paperless policy

To ensure business continuity, data is backed all stored securely on cloud-based services.

Outsourcing and Suppliers

GearedApp ensures an adequate level of protection for any personal data processed by others on its behalf or transferred outside the European Economic Area. When determining whether to use an external provider, GearedApp requires proof of their adherence to Data Protection Legislation both in the UK and EU.

Data recording and storage

Accuracy

GearedApp ensures that the personal data it holds is of sufficient quality to make decisions about individuals. Data is not collected without a legitimate business reason and collects only the minimum required to meet the purposes for which it is needed and which are specified in the privacy notice. All personal data held is accurate and, where necessary, kept up-to-date.

Retention

GearedApp ensures that personal data is not kept for longer than is necessary. We carry out checks to identify which records or data sets are held, and when they should be deleted or anonymised. Senior management are accountable for checking this data regularly. Data is disposed of securely.

Subject access requests

All subjects have the right to request access to their data. It is the responsibility of senior management to ensure that requests are handled within the statutory mandated timescale.

Access requests should be made in writing. All GearedApp staff are required to inform senior management of any access request so that it can be responded to in a timely manner, without delay. The identity of the subject will be verified before supplying data.

Privacy impact assessments

GearedApp assesses all projects and initiatives during the initial planning and scoping phases, and we ensure that privacy and data protection are at the centre of all of our decisions. In certain situations, as is mandated by the General Data Protection Regulation (GDPR), we may also conduct comprehensive Privacy Impact Assessments (PIA) to evaluate and mitigate against any risks to data protection. This is used throughout the development and implementation of a project to identify and reduce privacy risks. Throughout this process we will:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

Transparency

Personal data is not processed in any manner that is "incompatible" with it's specified purpose. We are committed to providing transparency as to how and why personal data is processed, and use the following methods to explain our processes:

- Website
- Email and e-newsletters
- Staff handbook
- Meetings with our customers

Direct Marketing

We require consent in advance of any direct marketing via our e-newsletters, and any other direct marketing we conduct. We record the date and method of providing such consent. It is the responsibility of senior management to ensure these lists are up to date and that consent has been received from all individuals.

We do not share contact details with any external organisations and these details are used only to provide company news to our contacts.

Individuals can opt out of receiving e-newsletters or communication with us at any time.

Staff training & responsibilities

All staff receive an initial induction in which they will be informed of their data protection responsibilities. Staff who have access to personal data will receive specific training relating to this.

There will be ongoing opportunities to discuss the issue of data protection during weekly team meetings and monthly one to ones with senior management.