FarrSight Solutions Limited
Data Protection Policy

This Policy was prepared by the Data Protection Officer, Angela Brown on 7 March 2018.

The Policy was approved by the Managing Director, Stephen Farrar on 13 March 2018.

The effective date of this Policy is 13 March 2018.

The next review date will be 13 March 2021.

Introduction

FarrSight Solutions Limited ("the company") needs to gather and use certain information about individuals.

These can include clients, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures the company:

- complies with data protection law and follows good practice;
- protects the rights of staff, clients and partners;
- is open about how it stores and processes individuals' data; and
- protects itself from the risks of a data breach.

Types of data

This policy applies to all data held relating to identifiable individuals, even if that information technically falls outside of the data protection laws. This can include:
Personal Data: Name, Address, Telephone number, Date of birth, National Insurance number, Identification references, Service history, Salaries, Benefit details, Bank details; and
Sensitive Data: Gender, State of health and sexual orientation.

Policy statement

This policy ensures that the data requested and held for the processing purposes of legal obligation under Article 6(c) or legitimate interest under Article 6(f), adheres to the principles relating to processing of personal data under Article 5 by being:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- 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 ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 ('storage limitation'); and

- 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 ('integrity and confidentiality').

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The GDPR provides the following rights for individuals:
- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision making and profiling.

An individual can ask to review the personal information held and can request the data be changed or deleted. Subject to such information no longer being necessary for the purpose for which it was originally collected or processed. This can be arranged by contacting the Data Protection Officer at FarrSight Solutions Limited, Cotton House, 12-18 Queen Street, Manchester, M2 5HS.

There will usually be a small administration fee in relation to any requests for access to personal information.

Data protection risks

This policy helps to protect the company from data security risks including:
- breaches of confidentiality – information being given out inappropriately;
- failing to offer choice – all individuals should be free to choose how the company uses date relating to them; and
- damage to reputation – the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

The responsibilities of the Data Protection Officer include:
- briefing the company on Data Protection responsibilities;
- reviewing Data Protection and related policies;
- advising other staff on tricky Data Protection issues;
- ensuring that Data protection induction and training takes place;
- notification to the ICO;
- handling individuals access request; and
- approving unusual or controversial disclosures of personal data.

General staff responsibilities

Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
- strong passwords (a random mixture of lower and upper case letters, numbers and other characters) to be used;
- personal data (including sensitive data) should not be disclosed to unauthorised people, either within the company or externally;
- secure email platform to be used, whenever processing personal data (including sensitive data);
- data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of; and
- employees should request help from the Data Protection Officer if they are unsure about any aspect of data protection.

Data storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- when not required, the paper or files should be kept in a locked location;
- employees should ensure paper and printouts are not left where unauthorised people could see them;
- paper should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- if data is stored on removable media (DVD/USB), these should be kept locked away securely when not being used;
- data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing server;
- servers containing personal data should be sited in a secure location away from general office space;
- data should be backed up frequently;
- data should never be saved directly to mobile devices, that do not have adequate security; and
- all servers and computers containing data should be protected by approved security software and a firewall.

The company aims to ensure that individuals are aware that their data is being processed, and that they understand how their data is being used and how to exercise their rights. In addition to this Data Protection Policy the company also has a Privacy Policy setting out how data relating to individuals is used by the company. Both of these documents (in this or later versions), are available on the website www.farrsight.com.