INSIGHT FIRST LTD

GDPR Policy

Contents

.....

1. Aims

Insight First Ltd aims to ensure that all data collected about staff, clients, client associated customers and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office.

It also takes into account the expected provisions of the General Data Protection Regulation, which is new legislation due to come into force in 2018.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller (Managing Director)	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor or Data protection officer	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Insight First Ltd processes personal information relating to clients and client associated customers and delegates the responsibility of data controller to the Managing Director.

Insight First Ltd is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- 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
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The Managing Director has overall responsibility for ensuring that the company complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the Managing Director, who will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the company of any changes to their personal data, such as a change of address.

7. Privacy/fair processing notice

7.1 Clients and Client Associated Customers

This data includes, but is not restricted to:

- Contact details
- Data Client Associated Customers, such as special diet requests/profiles

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them should refer to sections 8 of this policy.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at our customers. The purpose of processing this data is to assist in the running of the company, including to:

- Enable individuals to be paid
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies.

Any staff member wishing to see a copy of information about them that the company should contact the Managing Director..

8. Subject access requests

Under the Data Protection Act 1998, clients have a right to request access to information the company holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- Name
- A correspondence address
- A contact number and email address
- Details about the information requested

Subject access requests will be provided within 30 working days. The table below summaries the charges that apply.

Number of pages of information to be supplied	Maximum fee (£)
1-19	5.00
20-50	10.00

9. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office desks, on staff room tables or pinned to noticeboards where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access company computers, laptops and other electronic devices. Staffs are reminded to change their passwords at regular intervals.
- Staff, who store personal information on their personal devices are expected to follow the same security procedures for company-owned equipment

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

12. Training

Our staff are provided with data protection training.

Data protection will also form part of continuing professional development, where changes to legislation or the company processes make it necessary.

13. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018.

We will review working practices when this new legislation takes effect and provide training to members of staff where appropriate

14. Monitoring arrangements

The Managing Director is responsible for monitoring and reviewing this policy.

The Managing Director checks that the company complies with this policy by, among other things, reviewing company records twice yearly.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

.