1. Definitions

Throughout this policy, the following definitions apply:

Company Name: First Integrated Solutions Ltd
Company Personnel: All employees, contractors, agency workers, consultants and directors
Data Controller: the person or organisation that determines when, why and how to process personal data
Data Protection Act 2018: The Data Protection Act 2018, as amended from time to time
Data Subject: An identified or identifiable individual about whom we hold personal data
Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity
Data Protection Officer (DPO): Phil Cameron, Operations & Compliance Director
General Data Protection Regulation (GDPR): the EU General Data Protection Regulation
Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers
Personal Data Breach: The loss or unauthorised access, disclosure or acquisition of personal data
Privacy Guidelines: The Company Privacy/GDPR and Data Protection Act 2018 related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, as amended from time to time. These are available from the Human Resources Department.
Privacy Notices: separate notices setting out information that may be provided to you that details why we collect information about you and what we do with it
Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, as amended from time to time. These are available from the Human Resources Department.
Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. Introduction

The organisation is fully committed to prepare for and, after 25th May 2018, to comply with the General Data Protection Regulation (GDPR). The GDPR applies to all organisations that process data relating to their employees, as well as others, including customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed.

This Data Protection Policy applies to all Company Personnel. You must read, understand and comply with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines, including any amendments. Any employee who is found to have breached this Data Protection Policy may be subject to disciplinary action up to and including summary dismissal.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. It is a critical responsibility that we take seriously at all times.

Whilst employees are required to comply with the terms of this Data Protection Policy, it does not form part of their employment contract.
Please contact Human Resources with any questions about the operation of this Data Protection Policy or if you have any concerns that this Data Protection Policy is not being or has not been followed.

4. Policy

First Integrated is committed to ensuring these principles are followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the organisation will:

- Observe fully the conditions regarding the fair collection and use of information including giving consent
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information only to the extend that it is needed to fulfil our operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the information is held for no longer than is necessary
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- Take appropriate technical and organisational security measures to safeguard personal information
- Publicise and abide by individuals' right to appeal or complain to the supervisory authority (The Information Commissioner's Office ICO) in the event that agreement cannot be reached in a dispute regarding data protection
- Ensure that personal information is not transferred abroad without suitable safeguards

This policy does not form part of the formal contract of employment for staff but is a condition of employment that staff will abide by the policies made by First Integrated. Any failure to follow the Data Protection Policy may lead to disciplinary proceedings.

The designated Data Controllers Phil Cameron, Operation & Compliance Director and Nicola Tocher, HR Coordinator, will deal with day-to-day matters. Any member of staff or other individual who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with one of the above-named persons.

5. Types of Data we hold

Employee Personal data is kept in personnel files or within the Company's HR systems. The type of data held by the Company includes but is not limited to the following:

- name, address, phone numbers - for individual and next of kin

- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details
- driving records

Relevant individuals should refer to the company's Privacy Policy for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

6. Personal Data Protection Principles

6.1. Lawfulness and Fairness

To this end, the organisation endorses fully and adhered to the six principles of data protection as set out in Article 5 of the GDPR.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals
2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which its processed
4. Data must be 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
5. Data must be 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
6. Data must be 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

6.2. Consent

In some circumstances consent maybe required. Consent should be freely given, specific and informed. It may also be withdrawn at any time.

6.3. Transparency

Information in relation to how and why we collect data will be provided through appropriate Privacy Policies.

External Personal Data of Clients or Supplier, both Current and potential, shall be retained for the purpose of promoting or developing the Company. This data shall be limited to relevant business associated information; all such data shall be securely stored within the Company Data systems. Access to such information shall be limited to FIS personnel in the execution of their job function related to customer care and business promotion/development. Data which has expired or no longer holds relevance to the business shall be removed and permanently deleted from the respective data managements systems.

6.4. Purpose Limitation

Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further processed in any manner incompatible with those purposes. We will not Process Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed and has consented where necessary.

6.5. Data Minimisation

Personal Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When Personal Data is no longer needed, it is deleted or anonymised in accordance with the Company's data retention guidelines.

6.6. Accuracy

We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

6.7. Storage Limitation

Personal Data will be kept in an identifiable form for no longer than is necessary for the purposes for which the data is processed.

7. Security Integrity and Confidentiality

Personal Data will be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction as set out in our Information Technology Policy. Where you work remotely, whether at home or at client sites, or Process Personal Data on personal devices, you must follow all policies in relation to this.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

8. Reporting a Personal Data Breach

The GDPR and Data Protection Act 2018 requires Data Controllers to notify any Personal Data

Breach to the applicable regulator and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so within 72 hours.

If you know or suspect that a Personal Data Breach has occurred, you should contact Phil Cameron, Operations & Compliance Director or Nicola Tocher, HR Coordinator immediately.

9. Transfer Limitation

Where it appears necessary to transfer Personal Data outside of the UK, you must first contact Phil Cameron, Operations & Compliance Director or Nicola Tocher, HR Coordinator for guidance on how this can be achieved within the scope of the GDPR and Data Protection Act 2018.

10. Company Procedures

The Company has appointed Phil Cameron, Operations & Compliance Director and Nicola Tocher, HR Coordinator with a specific responsibility for protecting the personal data of individuals in respect of processing and controlling the data. If you wish further information in relation to the steps taken please contact either or the above noted.

11. Data Subjects Rights and Requests

Data Subjects have certain rights when it comes to how we handle their Personal Data.

These include rights to: withdraw consent to Processing; receive certain information about the Data Controller's Processing activities; request access to the Personal Data that we hold; ask us to erase Personal Data if it is no longer required for the purpose for which it was collected or Processed; to rectify inaccurate data; to complete incomplete data; restrict Processing in specific circumstances; challenge Processing which has been justified on the basis of our legitimate interests or in the public interest; prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else; be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; make a complaint to the supervisory authority.

You must immediately forward any Data Subject request you make or receive to Nicola Tocher, HR Coordinator and comply with the Company's Data Subject response process**.**

12. Accountability

We implement appropriate technical and organisational measures to ensure compliance with data protection principles. Our policies and procedures are one way in which we demonstrate our compliance with the GDPR and Data Protection Act 2018.

13. Record Keeping

Where required by the GDPR and Data Protection Act 2018 we will keep full and accurate records of all our data Processing activities. In addition, we will keep records of Data Subjects' consents and procedures for obtaining consents, in accordance with the Company's record keeping guidelines.

14. Training and Audit

We require all Company Personnel to read and understand the Data Protection Policy when they are inducted. In addition, you will be required to undergo training appropriate to your role to enable you to comply with the GDPR and Data Protection Act 2018.

15. Sharing Personal Data

We will only share Personal Data with third parties where certain safeguards and contractual arrangements have been put in place.

We only share the Personal Data we hold with third parties, including but not limited to our service providers such as benefits providers, payroll providers and professional advisors if:

a) We have a lawful basis for doing so;
b) Sharing the Personal Data complies with the Privacy Notices provided to the Data Subject and, if applicable, consent has been obtained; and
c) The third party has agreed to comply with the required data security policies and procedures and put adequate security measures in place.

We may share the Personal Data we hold with another employee, agent or representative of our group which includes our subsidiaries and our ultimate holding company along with its subsidiaries if the recipient has a job-related need to know the information.

16. Changes to this Data Protection Policy

We reserve the right to change this Data Protection Policy at any time without notice to you.
This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates

End

Phil Cameron
Operations & Compliance Director

17/05/2018