integritysupportsolutions

Privacy Policy

Document Control				
Version	**Date**	**Reason**	**Owner**	**Reviewer**
0.1	04/06/2018	Initial draft	Tony Couch	Rob Graham
1.0	16/07/2018	Issued to Client		

Table of Contents

1.0 Introduction 3
2.0 The Data Protection Principles 3
3.0 Rights of Data Subjects 3
4.0 Personal Data 4
4.1 Sensitive personal data 4
5.0 Processing Personal Data 5
6.0 Legal basis for processing personal data 5
7.0 Data Protection Procedures 6
8.0 Organisational Measures 6
9.0 Access by Data Subjects 7
9.1 Subject Access Request (SAR) 8
10.0 Retention of Data 8
11.0 Notification to the Information Commissioner's Office 8
12.0 Contacting Integrity Support Solutions Group 9
13.0 Integrity Support Solutions Group Pledge 9

1.0 Introduction

This document sets out the obligations of Integrity Support Solutions Group ("the Company") with regard to Privacy, Data Protection, the rights of Data Subjects and the people with whom it works in respect of their personal data under the European Union General Data Protection Regulation ("the Act").

This Policy shall set out the principles and procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company.

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully.

2.0 The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out the principles with which any party handling personal data must comply.

All personal data must be: -

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

We aim to ensure all personal data is protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and

Will not be transferred to a country or territory outside of 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.

3.0 Rights of Data Subjects

Under the Act, data subjects have the following rights: -

- The right to be informed that their personal data is being processed
- The right to access any of their personal data held by the Company within 0ne month of making a request
- The right to prevent the processing of their personal data in limited circumstances
- The right to rectification if any personal data held is inaccurate

- The right to erasure of personal data if it is no longer necessary for it to be processed (the right to be forgotten)
- The right to restrict processing under certain circumstances
- The right to data portability where personal data is processed by electronic means
- The right to object to the processing of personal data
- Rights in relation to automated decision making

We will adopt the principle of "data protection by design" as a standard approach to the collection, recording, processing, sharing, and controlled destruction of personal data and ensure that the rights of individuals are paramount at all times.

4.0 Personal Data

Personal data is defined by the Act as: -

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.1 Sensitive personal data

The Act also defines "sensitive personal data" as personal data relating to

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the data protection principles; the Policy and our Privacy Notice(s) are made available to clients and on our website here.

5.0 Processing Personal Data

All personal data held and processed by the Company is collected to ensure that the Company can facilitate efficient transactions with third parties including, but not limited to, its customers, partners, associates and affiliates and efficiently manage its employees, contractors, suppliers, agents and consultants. Personal data shall also be used by the Company in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within the Company. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

The Company shall ensure that: -

- All personal data collected and processed for and on behalf of the Company by any party is collected and processed fairly and lawfully
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)
- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed
- No personal data is held for any longer than necessary in light of the stated purpose(s)
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data
- All personal data is transferred using secure means, electronically or otherwise
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory
- All data subjects can exercise their rights set out above in Section 3 and more fully in the Act

6.0 Legal basis for processing personal data

Records will be kept of all personal data processed by The Company. The legal basis for processing that personal data will be identified as one of the categories as specified in the Act. Processing will only be legal if one of the following conditions is met: -

- Data subject gives clear **consent** for one or more specific purposes.
- Processing is necessary to meet **contractual** obligations entered into by the data subject.
- Processing is necessary to comply with **legal obligations** of the controller.
- Processing is necessary to protect the **vital interests** of the data subject.

- Processing is necessary for tasks in the **public interest** or exercise of authority vested in the controller.
- Processing is for the purposes of **legitimate interests** pursued by the controller.

7.0 Data Protection Procedures

The Company shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company comply with the following when processing and / or transmitting personal data: -

- All emails containing sensitive personal data must be encrypted
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar
- All electronic copies of personal data should be stored securely using passwords, suitable data encryption, secure and effective back up
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which could be easily guessed or otherwise compromised.

8.0 Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data: -

- A designated officer (“the Designated Officer”) within the Company shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.
- All employees, contractors, agents, consultants, suppliers, partners or other parties working on behalf of the Company are made fully aware of both their individual responsibilities and the Company’s responsibilities under the Act and shall be furnished with a copy of this Policy.

- All employees, contractors, agents, consultants, suppliers, partners or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, suppliers, partners or other parties working on behalf of the Company handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those employees, contractors, agents, consultants, suppliers, partners or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, suppliers, partners or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, supplier, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, suppliers, partners or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Act.
- Where any contractor, agent, consultant, supplier, partner or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

9.0 Access by Data Subjects

A data subject may make a subject access request ("SAR") at any time to request a copy information which the Company holds about them, specifically: -

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that is provided in a privacy notice (see our privacy notice here).

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the accuracy of the data and lawfulness of the processing.

9.1 Subject Access Request (SAR)

Upon receipt of a SAR the Company shall have a maximum period of one month within which to respond. The following information will be provided to the data subject: -

- Whether or not the Company holds any personal data on the data subject
- A copy of any personal data held on the data subject
- Details of what that personal data is used for
- Details of any third-party organisations that personal data is passed to
- An explanation and/or key to any technical terminology or codes
- Copy(ies) of any consent(s) having been given

10.0 Retention of Data

It is our intent to retain personal data for no longer than is absolutely necessary, at which time it will be safely deleted and/or destroyed.

All companies are obliged by law to retain certain information for specified minimum periods e.g. financial records must be kept for 7 years. We will comply with prescribed legislation.

If we have received consent from you we will continue to hold your data for the term of validity of that consent.

For all other personal data our standard retention period is 3 years or longer for legitimate business reasons.

11.0 Notification to the Information Commissioner's Office

As a data controller, the Company is required to notify the Information Commissioner's Office that it is processing personal data. The Company is registered in the register of data controllers.

Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office.

12.0 Contacting Integrity Support Solutions Group

If you have any questions about how we use your personal data that are not answered here, or if you want to exercise your rights regarding your personal data, please contact us by any of the following means:

- phone us on: - 01782 341827
- e-mail us at: - info@ssuk.eu or
- Integrity Support Solutions Group Ltd., Unit 1 Holm Ind. Est., Moffat, DG10 9JU

You have the right to lodge a complaint with the Information Commissioner's Office. Further information, including contact details, is available at https://ico.org.uk.

13.0 Integrity Support Solutions Group Pledge

Integrity Support Solutions Group Ltd is committed to complying with data protection legislation and good practice including: -

- processing personal information only where this is strictly necessary for legitimate organisational purposes
- collecting only the minimum personal information required for these purposes and not processing excessive personal information
- providing clear information to individuals about how their personal information will be used and by whom
- only processing relevant and adequate personal information;
- processing personal information fairly and lawfully
- maintaining an inventory of the categories of personal information processed by us
- keeping personal information accurate and, where necessary, up to date
- retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
- respecting individuals' rights in relation to their personal information, including their right of subject access
- keeping all personal information secure
- only transferring personal information outside the EU in circumstances where it can be adequately protected
- the application of the various exemptions allowable by data protection legislation
- developing and implementing a Personal Information Management System (PIMS) to enable the policy to be implemented.