Data Protection Policy

Purpose

The purpose of this policy is to ensure that ISS Labour Ltd (ISSL) and its staff (meaning permanent, fixed term, and temporary staff, any third party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with ISSL), conduct their business practices in a manner compliant with the Data Protection Act 2018 ("DPA") and the General Data Protection Regulations (GDPR 2018) and its principles to ensure that all personal data is secure, accurate and up-to-date at all times.

Scope

This policy applies to all members of the organisation and those contracted to work on behalf of ISSL and is to be followed at all times. Its aim is to protect the rights of individuals and applies to all personal and sensitive information that is used, stored, and transmitted either electronically or via paper-based methods.

Objectives

The objective of this policy is to protect the rights of individuals with regards to the personal information known and held about them by ISSL in the course of business and ensure that every business practice, task and process carried out by ISSL, is compliant with each principle of the DPA 2018 and the GDPR 2018.

ISSL aim to ensure that staff are trained and aware of the guiding principles behind Data Protection of personal data, namely, to ensure;

- **Confidentiality** – That personal data will be handled with due regard to its sensitivity and appropriate security measures put in place to maintain its confidentiality
- **Integrity** – That the personal data which is held by ISSL is up to date, accurate and can be relied upon.
- **Availability** – That the personal data will be available to the data subject when they require the information.

This policy is therefore in place to ensure regulatory and legal compliance at all times with regards to handling and processing personal data.

Data Protection Policy Statement

ISSL is classed as a Data Controller/Data Processor under the current DPA 2018, however ISSL recognises that under the GDPR 2018 our obligations to ensure appropriate controls are in place irrespective of classification is of critical importance.

This policy confirms our commitment to protect the privacy of personal data of our customers, clients, employees, and other interested parties.

Basic Principles Regarding Personal Data Processing

The GDPR sets out a set of six guiding principles, which outline the responsibilities for organisations handling personal data. Article 5(2) of the GDPR states that *the controller shall be responsible for, and be able to demonstrate, compliance*. This is known as the 'Principle of Accountability'. The remaining principles state that personal data must be;

a) **Lawfulness, Fairness and Transparency -** Processed lawfully, fairly and in a transparent manner in relation to the data subject.

b) **Purpose Limitation -** Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

UNCONTROLLED IF PRINTED

Data Minimisation - Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Accuracy - Accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

Storage Period Limitation - Be kept for no longer than is necessary for the purposes for which the personal data is processed.

Integrity and Confidentiality - 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').

Data Processing

Transmitting Personal Data - Where personal data is to be transmitted (either electronically or in hard copy), staff are required to ensure that any such data is secured using appropriate measures (e.g. use of encryption, passwords for electronic transmissions or using secure couriers).

Personal data will only be transmitted in accordance with best practice and processes noted as part of the ISSL Integrated Management System (IMS).

Personal data is only transmitted to a person authorised to receive it in compliance with these Data Protection principles.

Storing Personal Data - Personal data in hard copies (e.g., paper medical records, copy passport etc) is retained only for as long as is essential to the account and/or customer, employee, or other interested party that they refer to.

Personal data in hard copy or electronic formats will be stored in accordance with best practice and in line with processes, which are part of a broader Information Security Management System (ISMS).

The management of personal data is controlled through this standard and ISSL has committed to ongoing audit and review of policies, processes and practices associated to holding information in all its form.

Breaches of Personal Data - If any breach of the DPA, GDPR or its principles occurs, staff are required to inform their line manager, who will report the details to the HSQE team to be logged and investigated, in line with ISSL's Incident Management processes.

Subject Access Request (SAR) - An individual has the right to see what personal information is being held about them by ISSL. If an individual makes a written request to us and asks for information under the Subject Access Request provisions, they are entitled to request:

- information on whether any personal data is being processed;
- what personal information is being held by ISSL
- a description of the personal data, the reason it is being processed and whether it is shared with third parties (and know who they are)
- details of the source of the data

ISSL will respond to any Subject Access Requests in line with the Subject Access Request policy

Responsibilities

ISSL recognises it has a responsibility to ensure that PII is protected using appropriate technical and operational measures and as such has implemented a security framework which focuses on both operational and technical aspects of data protection. In this regard ISSL have;

- Implemented controls to ensure that staff cannot gain access to information that is not necessary for them to carry out their job functions.

UNCONTROLLED IF PRINTED

- Put in place measures to ensure that all information held will be relevant, accurate and up-to-date and used only for the purpose for which it is required and was originally intended.
- Committed to ensure information will not be kept for longer than is necessary and will be kept secure at all times.

ISSL also recognises it is responsible for ensuring that the data subjects data 'rights' are considered when processing data.

The Rights of Access by Data Subjects

Section 3 of the GDPR states that data subjects have rights in relation to their data, including;

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

When acting as a data controller, ISSL is responsible for providing data subjects with a reasonable access mechanism to enable them to exercise these rights.

Any request or right will be referred to the Subject Access Request policy.

Definitions

To ensure ISSL understands its obligations to the protection of personal data, the following definitions apply and are based on current understanding of these terms within UK and European law, and specifically in Article 4 of the GDPR.

Personal Data - Any information relating to an identified or identifiable natural person ("Data Subject") 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.

Sensitive Personal Data - Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data (referred to as special category data under GDPR) include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller - The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor - A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing - An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of the data.

UNCONTROLLED IF PRINTED

Anonymisation - Irreversibly de-personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identifying identify that individual. The personal data processing principles do not apply to anonymised data as it is no longer personal data.

Monitoring and Review

A Privacy Standard document will be maintained and issued to any individual who may handle personal data within the business.

This policy will be reviewed at least annually for effectiveness.

Gary Beeston
Group Managing Director

UNCONTROLLED IF PRINTED