DATA PROTECTION POLICY

Who We Are

Intelligent Outsourcing is a Business Process Outsourcing company (BPO) based in the UK and the Philippines concentrating on Accountancy and IT solutions. Intelligent Outsourcing is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all legal obligations.

Purpose of this Policy

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. This policy requires staff to ensure that the management team be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

The purposes for which personal data may be used by us: HR, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business and improving our services.

Personal data means 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.

Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

'Data Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

'Data Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'Processing' means any 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Information Commissioner's Office (ICO) is the national body responsible for data protection.

Aims

This policy applies to all staff, who must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Intelligent Outsourcing shall comply with the principles of data protection as set out in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles. The principles are:

Lawful, fair and transparent. Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

Limited for its purpose. Data can only be collected for a specific purpose.

Data minimisation. Any data collected must be necessary and not excessive for its purpose.

Accurate. The data we hold must be accurate and kept up to date.

Retention. We cannot store data longer than necessary.

Integrity and confidentiality. The data we hold must be kept safe and secure.

Accountability

We must ensure accountability and transparency in all our use of personal data. Each member of staff is responsible for keeping a written record of data processing activities. This must be kept up to date and must be approved by the management team.

To demonstrate compliance with data protection laws, you are responsible for understanding your responsibilities to ensure the following data protection obligations are met:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including: Data minimisation, transparency, allowing individuals to monitor processing and creating and improving security and enhanced privacy procedures on an ongoing basis

Procedures

Fair and lawful processing: We must process personal data fairly and lawfully in accordance with individuals' rights. This means that we should not process personal data unless the individual whose details we are processing has consented to this happening. Data subjects have the right to have any data unlawfully processed erased.

How we establish a lawful basis for processing data: It is the responsibility of the management team to check the lawful basis for any data you are working with and to ensure all your actions comply with the lawful basis. At least one of the following conditions must apply with regards to personal data:

- **Consent:** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Contract:** The processing is necessary to fulfil or prepare a contract for the individual.
- **Legal obligation:** We have a legal obligation to process the data (excluding a contract).
- **Vital interests:** Processing the data is necessary to protect a person's life or in a medical situation.
- **Public function:** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Legitimate interest:** The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Intelligent Outsourcing is classified as a data processor. We must maintain our appropriate registration with the Information Commissioner's Office in order to continue lawfully processing data. As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. As a data processor we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches.

Responsibilities

Our responsibilities include:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Your responsibilities:

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified

- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

The management team will:

- Keep the Managing Director updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Arrange data protection training and advice for all staff members and those included in this policy
- Answer questions on data protection from staff and other stakeholders
- Respond to individuals such as clients and employees who wish to know which data is being held on them by us
- Check and approve third parties that handle the company's data
- Address data protection statements from clients, target audiences, or media outlets
- Ensure all marketing initiatives adhere to data protection laws and this policy.
- Ensure all systems, services, software and equipment meet acceptable security standards
- Check and scan security hardware and software regularly to ensure it is functioning properly
- Research third-party services, such as cloud services the company is considering using to store or process data

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform us immediately.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. All staff use a password management system to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The management team must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- You must not transfer personal data abroad without express permission of the management team.

- All possible technical measures must be put in place to keep data secure

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

Right to be informed

- Providing a privacy notice which is concise, transparent, intelligible and easily accessible and written in clear and plain language.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the MANAGEMENT TEAM.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Right to Erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and /or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The Right to Object

Individuals have the right to object to their data being used on grounds relating to their own situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

Third Parties

As a data processor we must have written contracts in place with any third parties that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Terms and Conditions

Our terms and conditions must comply with the standards set out by the ICO. Our terms and conditions must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

Criminal Offence Data

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the MANAGEMENT TEAM prior to carrying out a criminal record check.

Audits, Monitoring and Training

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the management team and normal procedures.

Monitoring

Everyone must observe this policy. The management team has overall responsibility for this policy. Intelligent Outsourcing will keep this policy under review and amend or change it as required. You must notify the management team of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

Reporting Breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Intelligent Outsourcing has a legal obligation to report any data breaches to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify a breach or is found to have known or suspected a breach has occurred, but has not followed the correct reporting procedures, will be liable to disciplinary action.

Please see the Data Reporting Procedure form as an Appendix to this policy.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the management team.

Created April 2018

DATA BREACH REPORTING PROCEDURE

Report of an Information Security Incident or Data Breach

Members of staff discovering incidents must report an information security incident or personal data breach immediately to the management team. Please use this form to provide details of the incident. For more information, please refer to the Data Protection Policy.

We may revise our Acceptable Use Policy at any time by posting the updated version of the policy to our website. You are expected to check this policy from time to time to take notice of any changes we make, as they are legally binding on you.

Person reporting the incident				
Date of incident				
Description of incident:				
Is Personal Data involved?	**Yes**		**No**	
Categories of personal data (e.g. name, address, Banner ID, etc.)				
Categories of data subject (e.g. internal records, client database etc.)				
Number of data subjects involved (if known)				
Any initial action taken in response to incident				

Created April 2018