IRIS Service Delivery UK Limited

Data Protection Policy

IRIS-HR-PO-019

Owner:	HR Manager
Author:	HR Officer
Issue:	1.0
Date distributed:	17 Jan 21
Due for review on:	17 Jan 23

Table of Contents

1 Introduction

Iris Service Delivery UK Limited is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations and in particular the General Data Protection Regulations (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018.

Iris controls personal data about our employees, contractors, clients, suppliers and other individuals for a variety of business purposes. Iris only processes data to fulfil contractual obligations or to comply with the law.

This policy sets out how Iris manages personal data and the rights of the individual (known in the GDPR Regulations as the Natural Person) so that personnel understand the rules governing their use of the personal data to which they have access in the course of their work.

2 Definitions

2.1 Business Purposes

The purposes for which personal data may be used by Iris include but are not limited to:

- Personnel
- Administrative
- Financial
- Regulatory
- Payroll, and
- Business development purposes.

2.2 Personal Data

Personal data is information that relates to an identified or identifiable individual.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

2.3 Data Controller

Data Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.
If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

2.4 Data Processor

Processors act on behalf of, and only on the instructions of, the relevant controller.

3 Scope

This policy applies to all Iris personnel, who must be familiar with this policy and comply with its terms.

This policy supplements other policies including the Information Security Policy, IT and Data User Policy and the Communications and Use of Equipment Policy. Iris may supplement or amend this policy by additional policies and guidelines from time to time.

4 Responsibilities

4.1 General

- Analysing and documenting the type of personal data Iris holds
- 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

4.2 Data Protection Officer

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all personnel and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- The DPO may appoint suitable deputies to fulfil their responsibilities as and when required.

4.3 IT Contractors

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

- Researching third-party services, such as cloud services the company is considering using to store or process data

5 The principles

Iris Service Delivery UK Limited shall comply with GDPR, which sets out seven key principles which lie at the heart of the general data protection regime.
GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals (lawfulness, fairness and transparency);

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (purpose limitation);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);

d) 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 (accuracy);

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (storage limitation);

f) 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);

g) the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability).

6 Lawful basis for processing data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Our commitment to this process demonstrates that Iris have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

Iris will ensure that individuals whose data is being processed is informed of the lawful basis for processing their data. This applies whether Iris have collected the data directly from the individual, or from another source.

7 Special categories of personal data

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. It includes, but is limited to, information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health

- sexual orientation
- criminal record

In all cases where Iris process special categories of personal data, Iris will require the data subject's explicit consent to do this unless exceptional circumstances apply or Iris are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If Iris do not have a lawful basis for processing special categories of data that processing activity must cease.

8 Rights of individuals

Individuals have rights to their data and Iris Service Delivery UK Limited will respect and comply with to the best of our ability. Iris will ensure individuals can exercise their rights in the following ways:

8.1 Right to be informed

Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children. Keeping a record of how Iris use personal data to demonstrate compliance with the need for accountability and transparency.

8.2 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

8.3 Right to rectification

Iris 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 DPO.

8.4 Right to erasure

Iris must delete or remove an individual's data if requested and there is no compelling reason for its continued processing. This will be done no later than one month after receiving the request.

8.5 Right to restrict processing

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

8.6 Right to data portability

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

8.7 Right to object

Iris must respect the right of an individual to object to:

- data processing based on legitimate interest or the performance of a public interest task
- direct marketing, including profiling
- processing their data for scientific and historical research and statistics.

8.8 Rights in relation to automated decision making and profiling

Iris 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.

9 Audits, monitoring and training

9.1 Data audits

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 DPO and normal procedures

9.2 Monitoring

All Iris personnel must observe this policy. The DPO has overall responsibility for this policy. Iris Service Delivery UK Limited will keep this policy under review and amend or change it as required. Individuals must comply with this policy fully and at all times and must notify the DPO of any breaches of this policy.

9.3 Training

Iris will provide adequate training on provisions of data protection law specific to their role. Individuals shall complete all training as requested. If the individual moves role or responsibilities, they are responsible for requesting, via the DPO, new data protection training relevant to the new role or responsibilities.

10 Reporting breaches

The procedure for the reporting and investigation of breaches is set out in the Information Security Policy and is to be adhered to following any incident.

A register of such incidents is maintained.

11 Failure to comply with this and associated policies

Iris Service Delivery UK Limited take compliance with this policy very seriously and failure to comply puts both Iris and the individual at risk. Therefore failure to comply with any requirement may lead to disciplinary action under Iris's procedures which may result in dismissal or termination of contract.

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

12 Monitoring and review

The effectiveness of this policy will be continually monitored, and content amended to reflect changes in working practices and legislation.

This document will be review if there is a significant change in legislation, equipment, buildings, staff, and technology or if an incident occurs.

13 Documented Information

13.1 Referenced Document

All documented information produced as a result of following this procedure is maintained IAW IRIS-QA-PR-001 Control of Documents and Documented Information

Document Reference No.	Title
IRIS-QA-MA-001	Quality Manual
IRIS-QA-PR-001	Control of Documents and Documented Information

Table 1 Referenced Documents

13.2 Document Change History

Issue No.	Details of Change	Date	Name
1.0	New Version	17 Jan 21	Sumeeta Hallan

Table 2 Document Change History

13.3 Terminology

Terms	Description

Table 3 Terminology