Privacy and Personal Data Protection Policy

DOCUMENT CLASSIFICATION	Protected
DOCUMENT REF	ISMS-DOC-A18-5
VERSION	3
DATED	20/7/23
DOCUMENT AUTHOR	Eddie Blass
DOCUMENT OWNER	Eddie Blass, CEO

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	25/4/22	Eddie Blass	Initial document
2	13/10/23	Lyn Bosanquet	Changes to reflect local environment
3	20/7/23	Lyn Bosanquet	Update to incorporate Academy

Distribution

NAME	TITLE
All staff	All staff, all students and all members of the Inventorium community

Approval

NAME	POSITION	SIGNATURE	DATE
Eddie Blass	CEO	E Blass	25/4/22
Eddie Blass	CEO	E Blass	29/11/22
Eddie Blass	CEO	E Blass	20/7/23

Contents

Tables

1. Introduction

In its everyday business operations Inventorium makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Customers / students
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, Inventorium is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Inventorium takes to ensure that it complies with it.

Please note this policy describes applicable legislation in the European Union. This is currently the highest standard around the world and hence has been adopted here.

The following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Records Retention and Protection Policy*
- *Acceptable Use policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *Information Security Incident Response Procedure*
- *Information Security Roles, Responsibilities and Authorities*

2. Scope

This policy applies to all systems, people and processes that contribute to the business operations and information systems of Inventorium, Inventorium RTO and Inventorium Academy, including directors, employees, suppliers and other third parties who have access to Inventorium systems.

3. Definitions

There are a total of 26 definitions listed within Article 4 – Definitions of the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined 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."*

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."*

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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*

4. Policy Statement

4.1 The General Data Protection Regulation

The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of legislation affecting the way that Inventorium carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is Inventorium's policy to ensure that our compliance with the GDPR and other relevant legislation is always clear and demonstrable.

4.2 Principles relating to processing of personal data

There are several fundamental principles upon which the GDPR is based.

These dictate that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

4. Accurate and, where necessary, kept up to date ('accuracy')
5. 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 ('storage limitation').
6. 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').

The Information Security Manager is responsible for and be able to demonstrate compliance with these principles ('accountability').

Inventorium ensure it complies with these principles in relation to all data collection, management and processing it undertakes. The operation of the information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

4.3 Rights of the individual

The data subject also has rights under the GDPR. These consist of:

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

Each of these rights must be supported by appropriate procedures within Inventorium that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in Table 1.

DATA SUBJECT REQUEST	TIMESCALE
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 1: Timescales for data subject requests

4.4 Consent

Unless it is necessary for a reason allowable in the GDPR, consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 (Note – this age may be lower in individual EU member states) parental consent must be obtained. Transparent information about the usage of personal data must be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject, then this information must be provided within a reasonable period after the data are obtained and within one month.

4.5 Privacy by design

Inventorium has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy (also known as data protection) impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation will be considered where applicable and appropriate.

4.6 Transfer of personal data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

It may be necessary for specific contractual terms to be used to cover international transfers. Where possible, these should be based upon standard contractual clauses (SCCs) made available by the relevant authority.

Intra-group international data transfers may be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

4.7 Data protection officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Inventorium does not require a Data Protection Officer to be appointed.

4.8 Breach notification

It is Inventorium's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with Inventorium's *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under the GDPR the relevant supervisory authority has the power to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

4.9 Addressing compliance to the GDPR

The following actions are undertaken to ensure that Inventorium always complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the information security management system.

4.10 Inventorium's obligations as a cloud service provider

In addition to holding personal data on our own account, Inventorium also stores and processes the personal data of our cloud customers. In doing so, there are several additional obligations that must be fulfilled to allow Inventorium customers to stay within the law. The policy in this area is informed by ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors which, as well as recommending specific enhancements to ISO/IEC 27001 controls, also provides the following policy guidance:

- Inventorium must provide its customers with the facilities to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII
- Inventorium must only use the cloud customer's PII for their purposes, not Inventorium's purposes
- The customer must be informed if Inventorium is required by law to disclose any customer data, unless Inventorium is prohibited from doing so
- Details of disclosures must be recorded
- Inventorium must inform its customers if it uses sub-contractors to process their PII
- Inventorium must inform its customers if their PII is subject to unauthorised access
- It must be clear in which country or countries the customer's PII is stored

Additional recommendations stated in ISO/IEC 27018 are also included in the relevant policies and procedures within the ISMS.