Privacy and Personal Data Protection Policy

Document:	Privacy and Personal Data Protection Policy
Document Number:	FCL/ISMS/L2/DEP
Version:	1.0
Document Date:	14th April 2025
Prepared By:	Amey Kakde
Reviewed By:	Aniruddha Hublikar
Approved By:	Dr. Rahul Patil
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Date of Change	Version No.
1	Initial Release	14th April 2025	1.0

Review History

Sl. No.	Reviewed by	Date of Review	Version No.
1	Aniruddha Hublikar	14.04.25	1.0

Areas of the standard addressed

The following areas of the ISO/IEC 27001 standard are addressed by this document:

- A.5 Organizational controls
  - A.5.1 Policies for information security
  - A.5.34 Privacy and protection of PII

Contents

Tables

1 Introduction

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

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

In collecting and using this data, the organization 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 Fluid Controls Limited. is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Fluid Controls Limited systems.

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 Access Policy*
- *Social Media Policy*
- *Information Security Incident Response Procedure*
- *Information Security Roles, Responsibilities and Authorities*

2 Privacy and personal data protection policy

2.1 The General Data Protection Regulation

The global requirement data & privacy and safety is one of the most significant pieces of legislation affecting the way that [Fluid Control Ltd] carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the data & privacy and safety global requirement which is designed to protect the personal data of citizens of any part globe. It is Fluid Control Ltd policy to ensure that our compliance with the and data & privacy and safety other relevant legislation is clear and demonstrable at all times.

2.2 Definitions

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."*

2.3 Principles relating to processing of personal data

There are several fundamental principles upon which the global requirement 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').

In addition, the controller shall be responsible for, and be able to demonstrate compliance with all of these principles ('accountability').

[Fluid Controls Limited] must ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems. The operation of an information security management system (ISMS) that conforms to the ISO/IEC 27001 international standard is a key part of that commitment.

2.4 Rights of the individual

The data subject also has rights under the Data & PII. 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 [Fluid Controls Limited] that allow the required action to be taken within the timescales stated.

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

2.5 Consent

Unless it is necessary for a reason allowable in the global requirement, consent must be obtained from a data subject to collect and process their data. In case of children below the age of 18 parental consent must be obtained. Transparent information about our usage of their 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 definitely within one month.

2.6 Privacy by design

[Fluid Controls Ltd] 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.

2.7 Transfer of personal data

Transfers of personal data outside the global territory must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the global requirement. This depends partly on the global requirements 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.

2.8 Data protection officer

A defined role of (Appointed Company secretary acting as DPO) Data Protection Officer (DPO) is required under the global requirement 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 Legal Advisor/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, Fluid Controls Ltd]requires a Data Protection Officer to be appointed.

2.9 Breach notification

It is Fluid Controls Ltd. 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 global requirements 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 our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Under the global requirement, 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.

Note : Refer Annex : A

2.10 Addressing compliance to the Global requirement

The following actions are undertaken to ensure that [Fluid Controls Limited] complies at all times with the accountability principle of the:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organization
- 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:
    - Fluid Controls Limited 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.

Annex : A

Aspect	**GDPR (EU)**	**DPDP Act (India, 2023)**	**FIPPs (General Principles)**
Scope	Applies to personal data (online and offline) of EU residents, extraterritorial application	Applies to digital personal data of Indian residents, also extraterritorial, excludes purely offline data	Broad principles applying to personal data and privacy generally
Data Categories	Distinguishes sensitive data (health, biometrics, etc.) with enhanced protections	No special categories; uniform treatment of all personal data	Emphasizes protection of sensitive data and fairness
Data Subject Rights	Extensive rights including access, correction, erasure, portability, objection, automated decision-making	Similar rights but excludes portability, objection to automated decision-making, and right to restrict processing	Emphasizes individual control, notice, and consent
Lawful Basis for Processing	Multiple bases: consent, contractual necessity, legitimate interests, legal obligation, public interest	Primarily consent-based, with limited exceptions (state functions, legal compliance)	Requires notice and consent where appropriate
Consent Management	Defined strict consent requirements; opt-in, granular	Introduces Consent Managers, as intermediaries to facilitate consent	Emphasizes informed and voluntary consent

Breach Notification	Mandatory risk-based notification within 72 hours to authorities and affected data subjects if high risk	Universal notification to Data Protection Board and affected data principals, irrespective of risk level	Requires timely breach notification and response
Cross-Border Data Transfer	Strict requirements; adequacy decisions, standard contractual clauses, binding corporate rules	Central government regulates permitted countries; less prescriptive mechanisms	Principles support data sovereignty and safeguards
Regulatory Authority	Independent supervisory authorities in each EU country	Data Protection Board of India appointed by central government; concerns on independence	Emphasizes oversight and enforcement authority
Penalties	Up to 4% global turnover or 20M fines	Up to, 250 crore (25 M) per breach; broad enforcement powers	Encourages accountability through sanctions
Government Exemptions	Limited, subject to necessity and proportionality	Broad exemptions for sovereignty, public order, law enforcement	Variably addressed; emphasizes lawful processing