



Data Protection Policy

1. Introduction

The Institute of Industrial Engineers & Safety Management Systems (IIESMS) is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) and other relevant data protection laws. This policy outlines how we collect, use, store, and protect personal data.

2. Purpose

The purpose of this policy is to ensure that IIESMS complies with data protection laws, protects the rights of individuals, and provides a clear framework for the lawful processing of personal data.

3. Scope

This policy applies to all employees, members, contractors, and other parties who process personal data on behalf of IIESMS.

4. Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Data Subject:** The individual whose personal data is being processed.
- **Data Controller:** The entity that determines the purposes and means of processing personal data.
- **Data Processor:** The entity that processes personal data on behalf of the data controller.
- **Processing:** Any operation performed on personal data, including collection, storage, use, and destruction.

5. Data Protection Principles

IIESMS adheres to the following data protection principles:

1. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner.

2. **Purpose Limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data Minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date.
5. **Storage Limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.
6. **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

6. Data Subject Rights

Data subjects have the following rights:

- **Right to Access:** The right to obtain confirmation as to whether personal data is being processed and access to the data.
- **Right to Rectification:** The right to have inaccurate personal data corrected.
- **Right to Erasure:** The right to have personal data erased in certain circumstances.
- **Right to Restriction:** The right to restrict the processing of personal data in certain circumstances.
- **Right to Data Portability:** The right to receive personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller.
- **Right to Object:** The right to object to the processing of personal data in certain circumstances.
- **Rights Related to Automated Decision Making:** The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects the individual.

7. Lawful Basis for Processing

IIESMS processes personal data based on one or more of the following legal bases:

- **Consent:** The data subject has given explicit consent for the processing.
- **Contract:** The processing is necessary for the performance of a contract with the data subject.
- **Legal Obligation:** The processing is necessary for compliance with a legal obligation.



- **Legitimate Interests:** The processing is necessary for the legitimate interests of IIESMS or a third party, provided these interests are not overridden by the rights of the data subject.

8. Data Security

IIESMS implements appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, disclosure, or destruction. This includes:

- Access controls to restrict access to personal data.
- Encryption of sensitive data.
- Regular security assessments and audits.
- Staff training on data protection principles and practices.

9. Data Breaches

In the event of a data breach, IIESMS will promptly assess the risk to data subjects and report significant breaches to the relevant supervisory authority within 72 hours. Affected individuals will be informed if the breach is likely to result in a high risk to their rights and freedoms.

10. Data Protection Officer

IIESMS has appointed a Data Protection Officer (DPO) responsible for overseeing data protection strategy and implementation. The DPO can be contacted at: **Email:** [DPO Email Address]

Phone: [DPO Phone Number]

11. Review and Updates

This policy will be reviewed regularly and updated as necessary to ensure continued compliance with data protection laws and best practices.

12. Contact

For questions or concerns about this Data Protection Policy, please contact: the **Institute of Industrial Engineers & Safety Management Systems (IIESMS)**

Email: info@iiesms.ie

Phone: +353 (0)51 311134