	DIGITAL MANUFACTURING IRELAND	
Document Title:	Data Protection Policy Digital Manufacturing Ireland	
Document Approvers:	**Signature**	**Department**
	Tracey Mannion	Privacy Officer
	Martina Ryan	Director of Corporate Services
Version Number:	V1.0	
Effective Date:	06Sep2023	

Contents

1. Introduction

Digital Manufacturing Ireland ("DMI") acknowledges its responsibility to comply with Data Protection practices which includes and is not limited to the requirements of the General Data Protection Regulation (EU) 2016/679 and the Data Protection Acts 1988-2018. DMI is committed to protecting Personal Data of all stakeholders which includes and is not limited to customers, suppliers, Employees, contractors, and others from whom the organisation collects Personal Data.

This policy sets out how DMI will ensure that those Employees understand their obligations in terms of processing Personal Data in their everyday ongoing business operations.
The policy will be reviewed at minimum annually to ensure alignment to appropriate risk management, operational and regulatory requirements.

European Data Protection requirements specifically refer to Personal Data collected and processed within Europe. However, DMI commits to protecting all Personal Data collected, processed, stored, and transferred including Employee and customer confidential data, regardless of country of origin.

DMI is a Data Controller and processor in accordance with the European Union General Data Protection Regulations (GDPR) and the Data Protection Act 2018 the Act which apply from 25 May 2018.

2. Purpose

The purpose of the policy is to ensure that the relevant Employees as outlined in the scope are aware of acceptable practices when dealing with Personal Data. The Privacy Policy outlines the responsibilities that DMI takes to protect the privacy of the organisation's stakeholders.

3. Scope

This policy applies to:

- Stakeholders which include Employees, contractors and any Third Parties that process Personal Data on behalf of DMI.
- Personal Data that DMI processes (collect, use, share, store or delete).
- Third parties that process Personal Data on behalf of DMI.
- Any device/IT Infrastructure that is used for the processing of Personal Data by DMI.
- All Personal Data, either new or existing, in electronic or paper form.

4. Director of Corporate Services

The Director of Corporate Services has the ultimate responsibility for overseeing compliance of the Data Protection activities. This responsibility includes:

- Approving the Data Protection Policy on an annual basis.
- Make decisions on high-risk activities/data breaches. Data Incidents.
- Appropriate resources available.

4.1 Privacy Officer

The Privacy Officer is responsible for implementing and maintaining the Data Protection Policy and other related data protection policies and procedures. Some of the responsibilities include:

- Develop and maintain the Data Protection Policy on an annual basis.
- Documenting and implementing systems and controls to collect, process and secure data in accordance with the GDPR and related legislation.

- Maintaining and updating systems of control within DMI and ensuring that all Employees adhere to the internal controls.
- Working with data owners to ensure appropriate resources are allocated to Data Protection activities.
- Responding to Data Subject access requests.
- Responding to Personal Data breaches.
- Identifying and understanding all regulations and relevant legislation that may influence DMI's Data Protection Policy.
- Providing the necessary information to relevant parties to facilitate independent reviews of Data Protection procedures.

5. General Requirements

The following Data Protection requirements apply to all instances where Personal Data is stored, transmitted, processed, or otherwise handled, regardless of geographic location.

DMI has established the following high-level principles relating to Data Protection, to comply with relevant European requirements:

Lawfulness, Fairness and Transparency
Personal Data will only be processed fairly, lawfully and in a transparent manner.

Purpose Limitation
Personal Data will be obtained only for specified, explicit, lawful, and legitimate purposes, and will not be further processed in any manner incompatible with those purposes.

Data Minimisation
Personal Data will be adequate, relevant, and limited to what is necessary, in relation to the purposes for which they are processed.

Accuracy
Personal Data will be accurate, and where necessary kept up to date.

Data Storage Limitation
Personal Data will not be kept in a form which permits the identification of a Data Subject for longer than is necessary for the purposes for which the Personal Data are processed.

Integrity and Confidentiality
Personal Data will be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:

- Prevent and / or identify unauthorised or unlawful access to, or Processing of, Personal Data.
- Prevent accidental loss or destruction of, or damage to, Personal Data.

Accountability
DMI, whether serving as a Data Controller or a Data Processor, will be responsible for, and be able to demonstrate compliance with, these key principles.

Data Subject Rights
DMI will cater for Data Subject rights requests within business, regulatory and technical means.

Privacy Governance

- DMI must ensure that there is an individual who is accountable for Data Protection within the organisation.
- Every stakeholder, as outlined in the scope must be responsible for adhering to this policy.
- DMI must ensure that their Employees are trained on relevant security and privacy obligations.
- DMI will provide Data Subjects with a Privacy notice at the point of Personal Data collection.

Personal Data Processing

DMI, as a Data Controller, will be responsible for, and must be able to demonstrate compliance with the following GDPR Requirements.

- DMI will process Personal Data in accordance with the rights of Data Subjects.
- DMI will carry out communications with Data Subjects in a concise, transparent, intelligible, and easily accessible form and using unambiguous language.
- DMI will only transfer Personal Data to another group, customer, or Third Parties outside of the European Economic Area (EEA) in accordance with this policy.

Consent

- Where processing is based on consent, DMI must demonstrate that the Data Subject has provided appropriate consent for this specific processing activity.
- Date processing consent must be specific, informed, unambiguous, freely given and provided by an affirmative action (Opt-in as opposed to Opt-out).
    - Date processing consent requests must be written clearly and easy to understand in plain language.
- DMI will ensure that consent is collected and documented lawfully, which includes:
    - Provisions for determining what disclosures must be made in order to obtain a valid consent.
    - Documentation of the date of collection.
    - Method and content of the disclosures made.
    - Validity, scope, and volition of the consents provided by the Data Subject.
- DMI will establish consent withdrawal processes and inform Data Subjects about:
    - Their right to withdraw consent at any time.
    - The process through which they can achieve this.
- Where collection of Personal Data relates to a child under the age of 18, Parental or Legal Guardian consent must be given prior to the collection.
- Personal Data will not be shared with Third Parties without informing the Data Subject concerned in advance.
- Where DMI wants to process Personal Data that was collected from the Data Subject for purposes other than the purpose it was originally intended for, DMI must seek the consent of its Data Subjects in clear and concise writing. Any such request must include the original purpose for which information was collected, and also the new, or additional, purposes. The request must also include the reason for the change in purposes.

Special Categories Personal Data Processing

DMI will not process Special Categories of Personal Data unless:

- The Data Subject has explicitly provided consent.
- It is necessary to carry out the Data Controller's obligations or exercise the Data Subject's specific rights in the field of employment, social security, and social protection law.

- Necessary processing for contract performance or contract entry.
- Necessary processing for compliance with a legal obligation to which the Controller is subject.
- It is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.

a. Data Minimisation Requirements

DMI will ensure that the concept of data minimisation is applied when collecting Personal Data, DMI will:

- Only collect what is necessary to accomplish a specified purpose.
- Identify the minimum amount of Personal Data required for a particular purpose, and then align collection volumes and associated retention to this purpose.

b. Data Use Limitation Requirements

- DMI and its Employees will only collect Personal Data for specified explicit and legitimate purposes.
- DMI will not further process Personal Data unless additional consent is obtained.
- Once Personal Data is no longer required for business and/or legal purposes, Personal Data will be securely deleted.

c. Data Accuracy and Relevance Requirements

- All Personal Data processed must be accurate, adequate, relevant, up to date and not excessive, given the purpose for which it was obtained.
- Data Subjects requests for updating inaccurate Personal Data will be addressed and amended in a timely manner.
- Personal Data must be kept for no longer than is required for the purposes for which the Personal Data is processed and in accordance with DMI's Data Retention and Destruction policy.

d. Storage Limitation & Retention

- Processes must be implemented to ensure that the purposes, methods, storage limitation and retention period of Personal Data are consistent.
- All Personal Data must be adequately protected based on the existing statutory regulations and the applicable industry principles.
- Only authorised individuals may be granted access to Personal Data.
- Electronic and hardcopies documents containing Personal Data must be kept in a secure place, where unauthorised personnel cannot access it.
- DMI will erase any Personal Data:
  - That violates Data Protection Law, Data Protection Regulations, Contractual Obligations, and Requirements of this Policy.
  - If DMI no longer requires the data.
  - If the Personal Data, no longer benefits the Data Subject in the relevant process.
- DMI will anonymise and/or pseudonymise Personal Data rather than erase if:
  - The law prohibits erasure.
  - Erasure would impair the legitimate interests of the Data Subject.
  - Erasure is not possible without disproportionate effort due to the specific type of storage.
  - Where the Data Subject has disputed the accuracy of the Personal Data, DMI disagrees with that assertion and resolution has not been reached.
- DMI must retain Personal Data for no longer than is necessary and in accordance with the Records Retention and Destruction Policy.

e. Data Destruction/Disposal

- Printed hard copies containing Personal Data must be securely shredded when it is no longer needed.
- Personal Data must be destroyed in accordance with the organisations Data Retention and Destruction policy.

f. Data Classification

- All Personal Data used by DMI must be appropriately defined and classified in accordance with the Data Classification Policy.
- Personal Data of any nature whatsoever that is not explicitly classified must, by default, be considered as "Confidential" where it is not available in the public domain.

g. Integrity and Confidentiality of Personal Data Policy

- Adequate security mechanisms designed to protect Personal Data must be used to prevent Personal Data from being stolen, misused, or abused, and to prevent data breaches.
- When implementing Personal Data security measures, DMI must consider:
  - Technological developments.
  - Implementation costs.
  - Nature of relevant Personal Data.
  - Inherent risks posed by human action/physical/natural environment to Personal Data.

h. Information Security Requirements

- DMI must use appropriate technical or organisational measures to process Personal Data in a manner that ensures appropriate security of Personal Data. This includes protection of Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised access to, or unauthorised disclosure.
- Only authorised Employees must have access to Personal Data.
- DMI and Third Parties that are processing data on behalf of DMI must ensure that the relevant security measures are applied when processing (collect, use, share, store or delete) Personal Data.
- DMI will ensure that secure mechanisms are utilised when transferring Personal Data from one location to another.
- DMI must ensure that suspected / actual Personal Data breaches are disclosed in alignment with the Incident Response process.
- Privacy by design must be incorporated in all business and technical projects concerning the processing of Personal Data.

i. Privacy by Design Requirements

DMI and its Employees aim to ensure that the impact of Data Protection and Privacy are fundamental to all business processes.

- DMI will incorporate Privacy by Design principles when designing or changing a service/project.
- Data Privacy Impact Assessments (DPIA) must be performed during key implementation phases for all projects involving the processing of Personal Data:
  - All documentation related to DPIA's must be maintained for audit purposes and to facilitate consistent management/ review procedures.
  - Departments engaged in projects, new product development or systems development of any sort (including change to existing practices), where Personal Data processing is involved, must document a DPIA.

- When the processing of Personal Data may result in a high risk to the rights and freedoms of a Data Subject, DMI is required to conduct a Data Protection Impact Assessment (DPIA) and then consult with the Privacy Officer.

- The Privacy Officer will be required to consult with the Data Protection Commissioner (DPC) in certain instances (prior to processing Personal Data where a DPIA assessment indicates that the processing would result in a high risk to a Data Subject and/or where measures cannot be taken by DMI to fully mitigate the risk.).
- When relevant, and when it does not have a negative impact on the Data Subject, Privacy settings for any of DMI technology and platforms that interact with, or process Personal Data about Data Subjects will be set to the most private by default.

j. Third Party Transfer Requirements

DMI will transfer Personal Data to a Third Party outside of the EEA where any of the following apply:

- The Data Subject has given explicit Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract between the Data Subject and DMI, or the implementation of pre-contractual measures taken in response to a request by a Data Subject.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between DMI and a Third Party.
- The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims.
- The transfer is required by law.
- The transfer is necessary to protect the Data Subject's vital interests.
- The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.
- The Privacy Officer must assess whether any of the above exceptions apply prior to any Personal Data transfer and must record the determination in writing.
- In cases where there is a requirement to transfer Personal Data to a Third Party the Data Subject should be notified prior to providing information to DMI by way of a Privacy Notice.

k. Third Parties Relationships Policy

- Where DMI makes use of a Third-Party supplier to process Personal Data on its behalf, DMI must ensure that the processor has adequate measures to safeguard Personal Data.
- DMI must contractually require the Third Party to provide the same level of protection that DMI applies in order to effectively protect Personal Data.
- The Third-Party supplier or business partner must only process Personal Data to carry out its contractual obligations towards DMI, or upon the instructions of DMI, and not for any other purposes.
- If DMI processes Personal Data jointly with an independent Third Party, DMI must explicitly specify its respective responsibilities of themselves and the Third Party in the relevant contract or any other legal binding document.
- The Third Party must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.

l. Data Subject Rights Requirements

- The Privacy Officer will maintain appropriate processes and procedures to address Data Subjects rights when exercised under GDPR and relevant EU Member State Data Protection requirements.
- Any information provided to a Data Subject in response to a request must be:

- Concise, Transparent, and Intelligible.
- In an easily accessible form, using clear and plain language.
- Free unless proven to be excessive (administration fee chargeable in this case).
- Provided in a timely manner.
- Departments must notify the Privacy Officer immediately when in receipt of a Data Subject access request and must provide the Privacy Officer with all necessary support to allow a response in accordance with regulatory timelines.

m. Record of Processing Activities (ROPA)

- DMI must implement and maintain a written record of processing activity under its responsibility. Two separate records of processing activities should be developed, one for where DMI operates as a Data Controller, and the other for where DMI operates as a Data Processor.
- Maintaining records of processing activities enables DMI to demonstrate compliance with Data Protection laws. DMI must keep records of their processing activities which at a minimum, should include the following information: the collection, storage, use, transfer, protection, deletion of Personal Data, the purposes for which the data is being processed, data categories processed, and details of the technical and organisational measures taken to protect the data.
- DMI will ensure that the ROPA's are regularly reviewed and updated.

n. Personal Data Breach Management

- Information security and privacy incidents and events must be reported immediately through the appropriate channels.
- All Employees have an obligation to report actual or potential Data Protection compliance failures. This allows DMI to:
  - Investigate the failure and take remedial steps if necessary.
  - Maintain a register of compliance failures.
  - Notify the applicable Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.
- When DMI learns of a suspected or actual Data breach, an internal investigation must be performed, and the appropriate remedial measures must be taken in a timely manner.
- DMI Privacy Officer must notify the Supervisory Authorities of breaches related to Personal Data unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. This notification must be done without undue delay and, where feasible, no later than 72 hours (that is, three calendar days) after the organisation has become aware of the breach.
- DMI is required to notify Data Subjects of data breaches and if the breach is likely to result in a high risk to their rights and freedoms. This notification must be done without undue delay.

o. Training

- All Employees will receive training on Data Protection, as completion of training is compulsory.
- New joiners will receive Data Protection training as part of the induction process.
- Further Data Protection training will be provided at least every year or whenever there is a substantial change in the law or to the policy and procedure.
- DMI must ensure that Employees undergo the relevant Privacy and Information Security training on an annual basis.
- DMI will maintain Employee GDPR training completion records.

6. Policy Compliance

a. Compliance

Breaches of this policy may result in non-compliance by DMI with the relevant Data Protection Legislation which may result in fines or legal action being taken against DMI.

b. Compliance Exceptions

Any exception to the policy will be reported to the Privacy Officer in advance.

c. Non-Compliance

If a breach occurs due to reckless behaviour and a breach occurs and is knowingly not reported, the person responsible may be held accountable.

- DMI reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy.
  - Any Employee found to have violated this policy may be subject to disciplinary action.
  - Any Third-Party service provider found to have violated this policy may result in the withdrawal of DMI from that Third Party service provider and/or the cancellation of any contract(s) between DMI and the Third-Party service provider. In Addition, where a breach of this policy is committed by contractors and/or authorised Third Party commercial service providers, DMI reserves the right to remedy via the contracts in existence.
- Non-compliance will be reported to the Privacy Officer.

7. Enforcement

DMI reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. DMI Employees who breach this policy may be subject to disciplinary action as provided for in DMI disciplinary procedure. If a breach occurs due to reckless behaviour and a breach occurs and is knowingly not reported, the person responsible may be held accountable.

Where a breach of this policy is committed by contractors and/or authorised Third Party commercial service providers, DMI reserves the right to remedy via the contracts in existence.

8. Review & Update

- This policy is reviewed annually to ensure it is achieving its stated objectives.
- Moreover, ad-hoc changes and improvements will be made as and when they are identified.

9. Referenced Documents

- DMI Data Retention and Destruction policy (To be released)
- DMI Information Security Policy (To be released)
- DMI Data Classification Policy (To be released)

10. Definitions

Term	Description
Anonymised	Refer to the process of making Personal Data anonymous data. ‘Anonymise’ should be construed accordingly.

Consent	Refer to any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
Data Controller	Refers to a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data is or will be processed. A Data Controller can be the sole Data Controller or a Joint Data Controller with another person or organisation.
Data Processor	Refers to a person or organisation that holds or processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data.
Data Protection Commission	Refers to the office of the Data Protection Commission in Ireland.
Data Subject	Refers to the individual to whom Personal Data held relates, including employees, customers, suppliers.
Data Subject Request	Refers to a request from a Data Subject relating to that individual's Personal Data.
EEA (European Economic Area)	Refers to the area in which the Agreement on the EEA provides for the free movement of persons, goods, services, and capital within the European Single Market, as well as the freedom to choose residence in any country within this area.
Personal Data	Refers to any data relating to an identified or identifiable natural person (Data subject). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing	Refers to any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether 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 terms 'Process' and 'Processed' should be construed accordingly.
Pseudonymisation	Refers to the processing of Personal Data in such a manner that the Personal Data can no longer be linked to a specific Data Subject without the use of additional data, provided that such additional data is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
Personal Data Breach	Refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Restriction of Processing	Refers to marking of stored Personal Data with the aim of limiting their processing in the future.
Data Subject Access Request	Refers to a written request made to a Data Controller by a Data Subject about whom a Data Controller keeps Personal Data on computer or in a relevant filing system. Response must be provided to the Data Subject under the terms outlined by GDPR and/or local requirements.
Data Subject Rights	Refers to the rights that Data Subjects have over their Personal Data, as defined by the GDPR. Data Subject Rights allow Data Subjects to have more control over their Personal Data and how it is processed by organisations, which includes the following: ● **Right to Access:** Data Subjects will be able to request access to their data that is held by DMI. ● **Right to Rectification:** Data Subjects can request to change or correct any inaccurate data belonging to them. ● **Right to Restriction of Processing:** Data Subjects have the right to object to having their data processed within lawful means. ● **Right to Erasure and to be Forgotten:** Data Subjects may request to delete data that DMI holds. ● **Right to Data Portability:** Data Subjects can request to have their data transferred outside of DMI if it is in an electronic format. ● **Right to Object to Automated Decision Making, including Profiling:** Data Subjects can object to a decision made by automated processing, with certain limited exceptions (such as legitimate grounds for the processing or the defence of legal claims) and request that any decision made by automated processes, have some human element.
Third Party	Under GDPR a 'Third Party' means a natural or legal person, public authority, agency, or body, other than the data subject, controller, processor, and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to process Personal Data.

Revision History

No #	Revision Description	Date Approved
1.0	New Document	06Sep2023