	DIGITAL MANUFACTURING IRELAND	
Document Title:	Personal Data Breach Management Process Digital Manufacturing Ireland	
Document Approvers:	**Signature**	**Department**
	Tracey Mannion	Privacy Officer
	Martina Ryan	Director of Corporate Services
Version Number:	V1.0	
Effective Date:	18Sep2023	

Contents

1 Introduction

Digital Manufacturing Ireland (Referred to as “DMI”, “The Company”, “we”, “us, “our” in this document) acknowledges its responsibility to comply with personal data protection practices which includes and is not limited to the requirements of the GDPR Regulation (EU) 2016/679 and the Data Protection Acts 1988-2018.

2 Purpose

The purpose of this Data Breach Management Process is to provide a baseline procedure for the planning, detection, remediation, and post-incident review activities in the event of a personal data breach. In addition, it is also used to provide guidance on the roles and responsibilities to the relevant affected stakeholders that may be involved during a data breach incident.

3 Scope

This procedure applies to all types of personal data, and to employees, contractors, and third-party service providers that process personal data on behalf of DMI.

4 Roles and Responsibilities

The Personal Data Breach Team will consist of both Standing and Non-Standing members and will be convened by the Privacy Officer.

The Standing members will consist of:

- The Privacy Officer
- Representative from the Cyber-security / IT team.
- Legal Representative

The Non-Standing members can include the below and other stakeholders that may be required to be involved in managing the data breach incident, depending on what expertise is required for a particular incident. It will consist of:

- Public Relations or Corporate Communications representative.
- Application or Business Owner.
- Any other stakeholders that will be required to support the process.

The Privacy Officer will be responsible for coordinating the response and recording all actions taken in response to the breach.

The table below outlines the key roles and responsibilities that would be carried out:

Role	Responsibilities
Privacy Officer	• Manage the overall Data Breach Management process when dealing with potential or actual incidents. • Identifying which non-Standing members must be part of managing the data breach incident. • Ensure an ongoing communication and reporting to the relevant stakeholders. • Manage and coordinate the overall response effort and the team, including establishing clear ownership of priority tasks when dealing with an actual or suspected data breach incident. • Ensure the documentation of the incident response process and procedures. • Ensure employees are trained in overall data breach incident response. • Together with legal liaises with the Data Protection Commissioner (DPC) and Data Subjects (when required).
Legal and Corporate Communication	• Provide legal input to data breach incidents and the overall management of such incidents i.e., if there are contractual breaches by or with third parties as a result of the incident and other legal matters. • Provide input and review on all written material related to the data breach from a legal point of view. For example, communications to Data Subjects or the DPC. • Corporate communication together with legal will develop content to be released to the media, with input from the Privacy Officer.
IT Team	• Provide consultation during a confirmed data breach, as required based on the nature of the incident. • Ensure that any cyber security incident reporting feeds into the Data Breach Management Procedure. • If the IT Team has identified a personal data breach that is not system related, notify the Privacy Officer.
Business Representatives	• Depending on the data breach various business representatives may be involved. For example, if HR data was involved in the data breach, HR will be involved as a non-Standing member.

5 Planning for Data Breach Incident Management

5.1 Channels for Reporting a Potential or Actual Data Breach

DMI is required to ensure that it has the relevant procedures in place to effectively receive notification of a suspected or actual data breach. Employees must be trained on identifying suspected data breach incidents and reporting it to the correct channels. Reporting of the suspected or actual data breach incidents will be received through and is not limited to the following channels:

Channel	To be Noted
• **Employees** Email to: incidentresponse@dmireland.org Contact: 061975220 • **Customers** Email to: incidentresponse@dmireland.org Contact: 061975220 • **Third Parties** Email to: incidentresponse@dmireland.org Contact: 061975220 • **Regulatory Bodies** Email to: incidentresponse@dmireland.org Contact: 061975220 • **Public** Email to: incidentresponse@dmireland.org Contact: 061975220	It is critical to ensure that all the stakeholders mentioned are aware of the channels to report a suspected or actual data breach incident. Personal data breaches that have been detected through the Cyber Security Incident Management Process will be managed by that process with touch points into this process. (i.e., IT will manage Cybersecurity incidents, with support from the Privacy Officer as required).

5.2 Develop a Communication Plan

A stakeholder notification and communication plan must be put in place to ensure adequate communication and notification to the relevant stakeholders. The formal communication plan must be defined and documented to include at a minimum:

- Communication mechanism from the Privacy Officer to the relevant internal / external stakeholders, frequency, communication roles, action status reporting, escalation processes where required etc.
- Communication to the affected Data Subject (internal and external).
- Communication to external stakeholders such as the Data Protection Commissioner and law enforcement as applicable.

Note: These plans will be tailored to each data breach incident.

5.3 Timing of Notifications and Communications

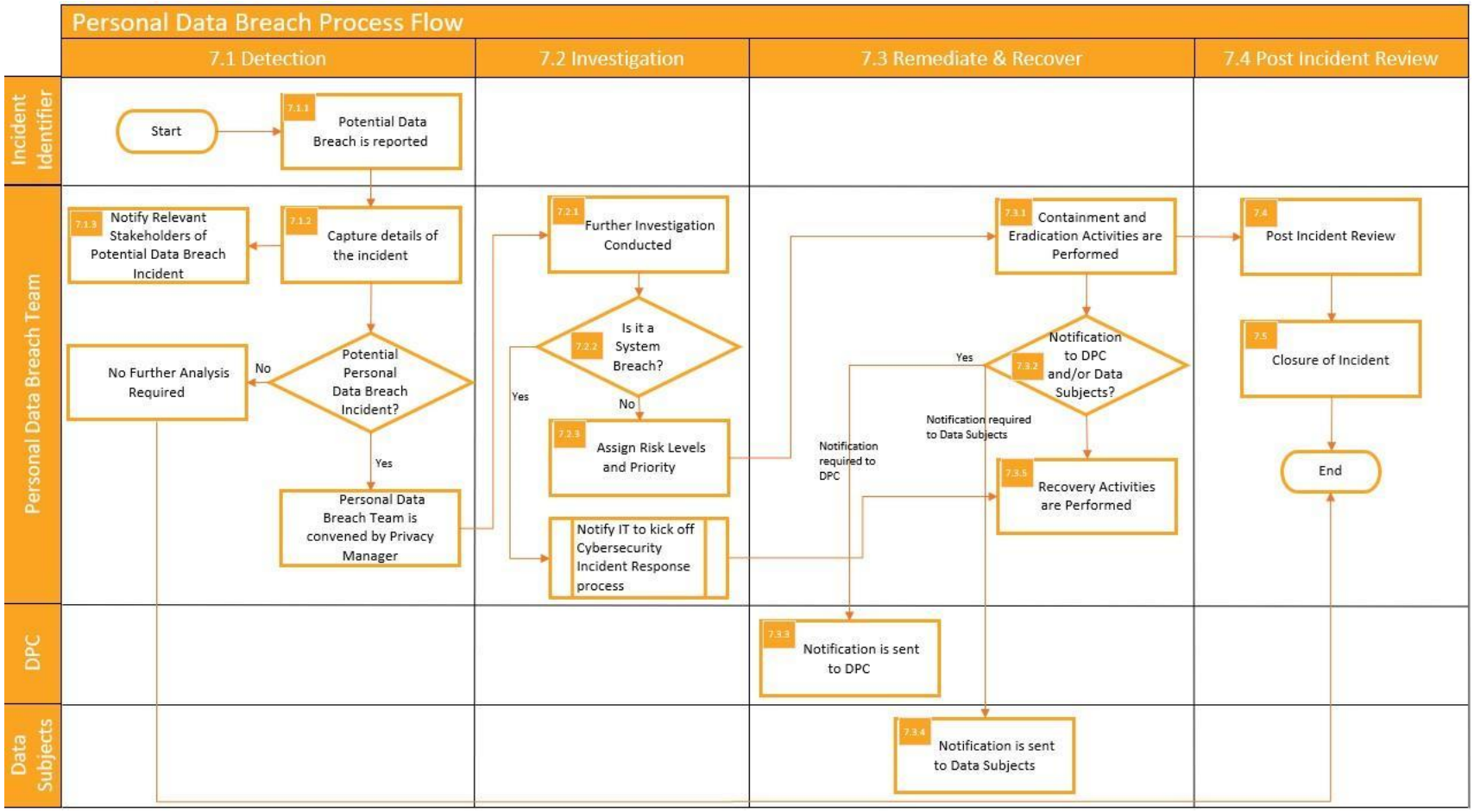
The timing of notification and communication must be based on the communication's objective, for example:

- Internal stakeholders - may need to be informed immediately as the objective for communication is to help resolve and manage the incident.
- External stakeholders - such as the Data Protection Commission (DPC) and / or affected Data Subjects, need to be informed according to the following timelines:
    - The DPC must be informed within 72 hours of DMI becoming aware of the data breach.
    - The affected Data Subjects must be informed without undue delay.

  An external party to whom DMI provides a service to, may have a service level requirement to be notified of suspected or confirmed data breaches within a certain period.
- Other stakeholders - such as the media or members of the public that may have been impacted, may contact DMI for responses. DMI must ensure that responses are ready and have been internally vetted from a legal perspective, prior to being released.
- An Garda Síochána - must also be notified in consultation with the legal team if a criminal act is suspected in relation to the incident.

6 Personal Data Breach Management Process Diagram

The below process flow diagram describes the flow of responsibilities and actions of various teams in DMI across the different phases of the personal data breach process.



7 Personal Data Breach Management Process

7.1 Detection Phase

○ Potential Data Breach Is Reported

DMI must ensure that the relevant stakeholders are aware of what channels are in place to communicate a suspected or actual personal data breach. A personal data breach will be reported by any of the below means:

- DMI Employees: Employees will report a suspected or actual personal data breach incident to the Privacy Officer through the available channels as outlined above in Section 5.1.
- DMI IT Team: IT Team will directly notify the Privacy Officer of a suspected or actual personal data breach incident.
- Third Parties: Third Parties will notify DMI of suspected or actual personal data breach. The notification will be received directly from the Third Party or IT Team.
- The Data Protection Commission (DPC): The DPC will notify the Privacy Officer of a suspected or actual personal data breach incident in the event that the DPC receives a complaint from a Data Subject.

○ Capture Details of the Incident

The Privacy Officer must capture the relevant details related to the suspected or potential data breach incident. This will include the following:

- Complete the Data Breach Incident Management Template- All information related to the incident must be captured during the initial reporting of the potential or actual data breach incident. It is important to log incidents correctly so that appropriate steps can be taken. The Data Breach Incident Management template must be fully completed by the Privacy Officer.
- Notify the relevant stakeholders of the potential data breach incident (initial notification before all members are convened).
- At this point if it is determined that there is no personal data involved, no further analysis will be required, and the process will end.

Note:

- The incident must be treated as a priority unless determined to be false positive or has a low impact (i.e., the incident does not involve a personal data breach or a very low volume of personal data).
- Communication about the potential / actual data breach incident must be treated and marked as highly confidential and sent only to the relevant stakeholders.

○ Notify the Relevant Standing and Non-Standing Members

The Privacy Officer will determine who needs to be included to manage the incident and will notify the relevant stakeholders. Refer to Section 4.

7.2 Investigation Phase

○ Further Investigation Conducted

- Investigate the nature and extent of the incident as well as the sensitivity of the personal data involved in the incident.

- Assess legal as well as regulatory implications.
- Determine who (if anyone) needs to be notified in accordance with applicable laws and contractual undertakings. Refer to Section 5.3 for details on Notification.
  - **Determine if a System Breach is involved.**
- If a system breach is involved- The Privacy Officer must immediately contact the IT Team. The IT Team will then follow the Cyber Security Incident Response Process.
- Non-System breaches – The Privacy Officer will continue to manage the incident as per the guidance below.

7.3 Priority and Risk Levels

The Privacy Officer will assign the incident a priority level and risk level, with input from the teams identified in Section 4.

Priority	Risk Level	Description
Priority 1	Severe	If the data breach incident includes: • Exposure of personal data and / or sensitive personal data. • The personal data breach may have a critical, extensive, or dangerous impact on affected individuals. • High likelihood that the breach will result in identity fraud, financial loss, or physical & material damage to individuals.
	High	If the data breach incident includes: • Exposure of personal data and / or sensitive personal data. • The personal data breach may have a considerable impact on affected individuals. • Incidents have the potential to damage corporate reputation and expose the company to penalties. Material risk of regulatory scrutiny, reputational / revenue loss.
Priority 2	Medium	If the Privacy incident includes: • Exposure of personal data. • The personal data breach may have an impact on individuals, but the impact is unlikely to be substantial. • Incidents have the potential to affect operational systems and disrupt normal business. • Incident is noticeable to external customers and may attract regulatory attention. Risk of revenue loss.

Priority	Risk Level	Description
Priority 3	Low	• The personal data breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
Priority 4	No Risk	• The personal data breach has no direct or indirect impact on individuals.

The following factors (including but not limited to) can also be considered for the above (Applicable to Severe, High, and Medium risk levels):

- The likelihood of identity fraud, financial loss, or other forms of misuse of the personal data.
- Whether the personal data could be, or is likely to be, used maliciously.
- The likelihood that the personal data breach could result in, and the severity of, physical, material, or non-material damage to Data Subjects.
- Whether the personal data breach could result in discrimination, damage to reputation or harm to Data Subjects' other fundamental rights.

7.4 Remediate and Recover Phase

Remediation and recovery actions for all confirmed data breaches to take place as per the below.

○ Containment and Eradication Activities are Performed.

The Privacy Officer must take every practical measure to contain and eradicate data breach incidents. As part of this step DMI must assess and investigate the extent to which the data breach incident has impacted the organisation and ensure that measures are put in place to limit further spread of the data breach.

For example, when the Personal Data Breach Team is dealing with a physical data breach (where hardcopy documents have been stolen), they promptly identify the source of the breach. All storage areas housing hard copies of the documents are secured to prevent further unauthorised access. Access to the compromised storage areas may be limited or temporarily suspended to mitigate the risk of additional breaches and ensure the integrity of the stored data. Efforts are made to determine the exact location of the breached information. The objective is to evaluate if the compromised data can be retrieved or if it has been permanently lost or destroyed. Based on the finding of the retrieval assessment, the next steps and notification requirements are determined. This evaluation considers the nature and extent of the breach, potential risks to individuals, and legal requirements for reporting and notifying affected parties.

DMI has a legal and ethical responsibility to implement practical steps to mitigate any effects from a data breach incident. The Privacy Officer and respective stakeholders within the organisation will be responsible for implementing the identified organisational or technical measures to ensure that such data breach does not occur again.

Is Notification to Data Subjects and the DPC Required

The Privacy Officer will determine whether a notification must be made to the below stakeholders based on its investigation of the personal data breach, including but not limited to:

- The Data Protection Commission (DPC) (Within 72 hours of the identification of the incident).
- Data Subjects.
- An Garda Síochána
- The press / media.
- DMI's insurers.
- External legal advisers.

Notification to The Data Protection Commission (DPC)

The notification to the DPC must be made without 'undue delay' and within 72 hours of DMI becoming aware of the personal data breach. The notification can be recorded on the DPC website.

- In case of a delay in the 72-hour reporting timeline, the notification to the DPC must be accompanied by a justification of the delay.
- The notification must include the following details:
    - The nature of the personal data breach.
    - Categories of Data Subjects and personal data concerned.
    - Approximate number of Data Subjects and personal data records concerned.
    - Name and contact details of the Privacy Officer.
    - Description of the likely consequences of the personal data breach.
    - Description of the measures taken or proposed to be taken by DMI to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Notification to the DPC is not required if the personal data breach is categorised as 'No Risk' according to the risk levels specified in Section 7.2.3.

Notification to The Data Subjects

A communication to Data Subjects is required where the personal data breach is categorised as 'High Risk' and 'Severe Risk' according to the risk levels specified in Section 7.2.3.

- The communication must be made without 'undue delay'.
- The communication must include the following details:
    - Nature of personal data breach.
    - Name and contact details of the Privacy Officer.
    - Description of the likely consequences of the personal data breach.
    - Description of the measures taken or proposed to be taken by DMI to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.5 Recover Phase

The Privacy Officer will conduct a root cause analysis and ensure actions are taken to recover from the incident and also determine if a prevention plan needs to be developed.

Post Incident Review

After successfully containing and resolving the personal data breach, the Privacy Officer will initiate a comprehensive review process. This review aims to examine the causes of the breach, assess the effectiveness of the response, and pinpoint areas that require additional improvement. The Privacy Officer will undertake the following actions:

- Document root-cause analysis: A thorough investigation will be conducted to identify the underlying causes of the personal data breach. This analysis aims to uncover any vulnerabilities or weaknesses in the systems, processes, or security measures that contributed to the breach.
- Evaluate and review the personal data breach log: The team will carefully assess the personal data breach log, which documents the details and timeline of the breach. This evaluation helps in gaining insights into the sequence of events, identifying any missed opportunities for detection or prevention, and enhancing future incident response strategies.
- Report findings to business unit leaders and affected parties: The team will communicate their findings to the leaders of the respective business units. Additionally, individuals impacted by the personal data breach will be informed about the outcomes of the review process. Transparent and timely communication is crucial in building trust and keeping stakeholders informed.
- Request appropriate enhancements for further securing the environment: This may involve implementing additional safeguards, upgrading systems or processes, or enhancing employee training and awareness programs.

Refer to the Appendix 2 for a personal data breach review meeting agenda template.

Closure of Incident

Before closure of the personal data breach, the Privacy Officer must ensure the completion of the following actions:

- Determine stakeholders and reporting requirements: Identify the relevant stakeholders, forums, or committees that need to receive the final report. Determine the specific information that needs to be reported and the level of detail required for each group.
- Post mitigation activities must be determined.
- Document lessons learned: As part of the incident report, document the lessons learned from the incident.
- Whether policies, procedures or reporting lines need to be improved to increase the effectiveness of the response to the personal data breach.

8 Annual Review

This procedure will be reviewed on an annual basis for effectiveness by the Privacy Officer and revised to address any improvements required. The Privacy Officer will document any improvements to the process by updating this procedure as needed.

9 Appendix

9.3 Appendix 1 - Data Breach Incident Management Template

The template below will be completed by the Privacy Officer for suspected and actual data breach incidents.

Data Breach Incident Management Template	
Details of the Individual Who Has Identified the Actual or Suspected Data Breach Incident	
Name & Surname:	Division / Department:
Role / Position:	Contact Number: Email Address:
Date of Capture:	Time of Capture:
Details Related to the Suspected or Actual Data Breach Incident:	
Date of Incident:	
Time of Incident:	
Location of Incident:	
Categorisation: This can include: ● Loss, theft, compromise of personal data. ● Unauthorised access to personal data. ● Unauthorised disclosure of personal data.	
Does the Potential Data Breach Incident Include Electronic Data or Hard Copies?	
Provide the Types of and Number of Data Fields That Are Involved.	
Description of Incident and How It Was Discovered.	
Business Unit That Has Been Impacted.	
Data Subject(s) Involved and Type of Personal Data Involved.	
Description of What Happened (Record in Detail):	

9.4 Appendix 2 - Personal Data Breach Review Meeting Agenda

The personal data breach team meets after the incident recovery actions are completed to analyse the root cause of the breach, assess the effectiveness and timeliness of the response, and identify areas of improvement. The following meeting agenda template must be followed during the discussion.

This activity is part of the Post Incident Review phase.

Area of Concern	Relevant Questions
Introduction	Introduction to the personal data breach (what happened, root cause, and impact?)
Why did the personal data breach occur?	10 Did we have sufficient controls? 11 Did a control fail? 12 Did a process failure contribute to the likelihood of the personal data breach occurring? 13 Are additional controls required? 14 What action steps are needed to be completed on controls, if any? 15 Was this due to a failure in an existing work-around?
How did we respond?	• How effective was the diagnosis and response? • Did we engage the resources and people at the right time? • Did communication, third party coordination and escalation work as planned? • How could the recovery process be shortened once the fix was identified? • What must we do differently?
How can we prevent similar unexpected issues from occurring?	• Are there gaps in the current process flow? • Was an issue identified during the review of the roles and responsibilities? • Do policies and procedures exist? Are they current? • If no policies and procedures exist, how do we get them created?
Mitigation steps.	• What are the agreed upon mitigation steps and timeline? • Have we elected to implement a manual work-around to address the same?

9.5 Appendix 3 - Definitions

Some of the Privacy and Data Protection terms used in the document are defined here.

No.	Term	Definition

1	GDPR	The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy that sets guidelines for the collection and processing of personal data from individuals who live in the European Union (EU).
2	DPA 2018	The Data Protection Act (DPA) 2018 is designed to protect the privacy of individuals. Depending on the nature and circumstances of the personal data processing, the type of personal data being processed, or when the data protection issue occurred, this legislation may be applicable instead of GDPR.
3	Personal data breach	Personal data breach is 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.
4	DPC	The Data Protection Commission (DPC) is the national supervisory authority in Ireland responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected. It is responsible for monitoring the application of the GDPR and other data protection laws.
5	Data Subjects	An individual about whom personal data is collected and processed.
6	Personal data	Personal data is any information relating to an identified or identifiable natural person. E.g., Name, Contact Details, Postal Address, Gender, Date of Birth.
7	Sensitive personal data / Special categories of personal data	A subset of personal data which could cause harm to the individual if leaked or misused. This category of personal data requires additional safeguards to be in place. E.g., Racial or Ethnic Origin, Political Opinions, Genetic or Biometric Data.

No #	**Revision Description**	**Date Approved**
1.0	New Document	18Sep2023