

## 1 Introduction

---

### 1.1 Purpose

The Privacy by Design (PbD) principle means that privacy and data protection are embedded throughout the life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. This in particular means that the protection of data must be at the heart of a company's internal processes.

Users of this document are all specialists of LLC MOI Tech, LLC MOVI TECH(hereinafter referred to as the Company).

## 2 GDPR Requirements

---

### 2.1 Data Protection by Design

Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start. It means building privacy into the design, operation and management of IT systems, networks and business processes.

As per GDPR: **"the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner."**

Examples of how to achieve Privacy by Design requirements:

- Minimising the processing of personal data;
- Pseudonymising personal data as soon as possible;
- Transparency with regard to the functions and processing of personal data;
- Enabling the data subject to monitor the data processing;
- Enabling the controller to create and improve security features;
- Staff training.

In particular, Article 25 specifically focuses on data minimisation. It says that for data protection, organisations should implement and practise methods of data minimisation by default.

As per GDPR: **"the controller shall implement technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."**

This obligation applies to:

- The amount of personal data collected;
- The extent of their processing;
- The period of their storage;
- Their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Data protection by default encourages organisations to apply the strictest privacy settings to a particular product or service at the outset of when that product or service is made available.

## 3 Privacy by Design and Default Principles

---

### 3.1 Proactive not Reactive; Preventative not Remedial

- Privacy should be part of the complete lifecycle of the project / software development and start early to prevent data breach.

### 3.2 Privacy as the Default

- Most data protection-friendly pre-settings.
- Personal data must be protected without action from the individual. GDPR has specific requirements to ensure the data subject does not have to take action in order to protect their data.

### 3.3 Privacy Embedded into the Design

- Privacy controls should be embedded in the architecture of IT systems, operations, and business processes without lessening functionality for the User.

### 3.4 Full Functionality

- Ensure that full functionality is available to users without affecting their privacy and data security.

### 3.5 End-to-End Security: Lifecycle Protection

- Early pseudonymisation.
- Embed privacy and data protection into systems throughout the data lifecycle — from Collection to Destruction.

### 3.6 Visibility and Transparency

- Transparency of privacy and data protection policies to the data subjects.
- Respect for User Privacy.

## 4 Privacy by Design and Default Checklist

---

- Before any new application or process is implemented, a DPIA shall be carried out.
- In addition to a DPIA, the Privacy Team shall also ensure compliance with Privacy by Design / Default guidelines detailed in Annexure A – PbD Guidelines.
- PbD Checklist (attached separately) shall be completed for each assessment of Privacy by Design and Default.

### Annexure A – PbD Guidelines

| PbD Principle / Area    | Requirement                                                                                                                                                                                   |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proactive, Not Reactive | <ul style="list-style-type: none"><li>– Project should identify assignment of responsibility and accountability for privacy in the organisation, and privacy training programme(s).</li></ul> |

|                                     |                                                                                                                                                                                                                                                            |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                     | – Reference all external sources of privacy requirements, including policies, principles, and regulations.                                                                                                                                                 |
|                                     | – Identify and include privacy requirements specific to the service / product being engineered, and anticipated deployment environments.                                                                                                                   |
|                                     | – As part of DPIA, include privacy risk / threat model(s) including analysis and risk identification, risk prioritisation, and controls clearly mapped to risks.                                                                                           |
| <b>Privacy as Default</b>           | – List all [categories of] data subjects as a stakeholder.                                                                                                                                                                                                 |
|                                     | – Clearly document the purposes for collection and processing, including retention of personal data.                                                                                                                                                       |
|                                     | – Document expressive models of detailed data flows, processes, and behaviours for use cases or user stories associated with internal software projects and all data / process interaction with external platforms, systems, APIs, and / or imported code. |
|                                     | – Describe selection of privacy controls and privacy services / APIs and where they apply to privacy functional requirements and risks.                                                                                                                    |
| <b>Privacy Embedded into Design</b> | – Have Privacy sections in BRD / FSD / SSD.                                                                                                                                                                                                                |
|                                     | – Contain description of business model showing traceability of personal data flows for any data collected through new software services under development.                                                                                                |
|                                     | – Describe privacy UI / UX design.                                                                                                                                                                                                                         |
|                                     | – Show tests for meeting privacy objectives, in terms of the operation and effectiveness of implemented privacy controls or services.                                                                                                                      |
| <b>Other Aspects</b>                | – Ensure data minimisation as part of software development.                                                                                                                                                                                                |
|                                     | – Minimise replication of personal data in log tables, user tables and other database tables / archives.                                                                                                                                                   |
|                                     | – Avoid archives that retain personal data for extended periods of time.                                                                                                                                                                                   |
|                                     | – Backups are retained for a limited period necessary for system recovery, in accordance with the Data Retention Policy.                                                                                                                                   |

## 5 Validity and Document Management

---

This document is valid from the date of approval until superseded by a new version. The document owner is responsible for keeping this policy current and aligned with applicable data protection legislation and organisational requirements.