<table>
<tr><td colspan="5"></td><td colspan="7">[Insert Registered Legal Entity Name Here]</td></tr>
<tr><td colspan="5">Document number:
P16</td><td colspan="7">Document Title:
<b>Data Masking and Pseudonymization Policy</b></td></tr>
<tr><td colspan="2">Version:
1.0</td><td colspan="3">Effective Date:
01.01.2025</td><td colspan="7">Document Owner:</td></tr>
<tr><td>X</td><td>Policy</td><td></td><td>Standard</td><td></td><td>Procedure</td><td></td><td>Form</td><td></td><td>Register</td><td></td><td>Other</td></tr>
</table>

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clauses 6.1.3	
ISO/IEC 27002:2022	Controls 8.11, 8.12	
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	
EU GDPR	Articles 4(5), 5(1)(c,f), 32	
EU NIS2	Article 21(2)(c)	
EU DORA	Articles 10(1), 10(2)(e)	
COBIT 2019	DSS05.01, DSS06.06, MEA03	

					[Insert Registered Legal Entity Name Here]						
Document number: P16					Document Title: **Data Masking and Pseudonymization Policy**						
Version: 1.0		Effective Date: 01.01.2025			Document Owner:						
X	Policy		Standard		Procedure		Form		Register		Other

1. **Purpose**
   1.1 This policy defines the organization's approach to implementing **data masking** and **pseudonymization** as privacy-enhancing technologies (PETs) to reduce identifiability and exposure of personal or sensitive data.
   1.2 It supports secure information use in testing, analytics, and operations while complying with legal and regulatory requirements, mitigating breach impact, and enforcing the principles of **data minimization** and **confidentiality**.
   1.3 The policy aligns with ISO/IEC 27001:2022, supports GDPR Article 4(5) on pseudonymization, and integrates risk-based implementation consistent with NIST, NIS2, DORA, and COBIT 2019 standards.
2. **Scope**
   2.1 This policy applies to:
      2.1.1 All employees, contractors, third parties, or vendors with access to systems that handle personal, confidential, or sensitive information.
      2.1.2 All data environments, including production, development, test, and staging.
      2.1.3 All forms of data masking (e.g., static, dynamic, deterministic, tokenization) and pseudonymization techniques used to reduce privacy risks.
      2.1.4 All data types (structured or unstructured), systems (on-premises or cloud-hosted), and applications involving personal or regulated data.
   2.2 The scope includes usage in:
      2.2.1 Application development and QA/testing environments
      2.2.2 Analytics or reporting platforms
      2.2.3 Data exchange with third parties or service providers
      2.2.4 Backup, archiving, or recovery systems
3. **Objectives**
   3.1 Ensure consistent and effective application of masking and pseudonymization to reduce risks of data exposure or misuse.
   3.2 Ensure that real data is never used in non-production environments unless it has been transformed via approved PET techniques.
   3.3 Maintain referential integrity, usability, and format-preserving transformations when required for operational consistency.
   3.4 Enforce strict access controls to original data, masked data, and re-identification keys.
   3.5 Treat masked or pseudonymized datasets as sensitive data, subject to access logging, retention controls, and incident response protocols.
   3.6 Validate the effectiveness of these controls through continuous testing, monitoring, and audit procedures.
4. **Roles and Responsibilities**
   4.1 Executive Management
      4.1.1 Approves this policy and ensures its enforcement as part of broader IT governance and data protection initiatives.

4.2 Chief Information Security Officer (CISO) / ISMS Manager

4.2.1 Oversees implementation and ongoing compliance.

[…….]

11. Reference Standards and Frameworks

This policy aligns with internationally recognized frameworks to ensure secure, compliant, and effective implementation of data masking and pseudonymization as privacy-enhancing technologies.

ISO/IEC 27001:2022

Clause 6.1.3 - Risk Treatment Plan: Establishes masking and pseudonymization as risk treatment mechanisms for reducing identifiability of sensitive data in non-essential processing environments.

Clause 8.1 - Operational Planning and Control: Mandates technical and procedural controls for secure data transformation during processing, storage, or transfer.

ISO/IEC 27002:2022 - Controls 8.11, 8.12

These controls provide detailed implementation guidance on selecting and applying data masking and pseudonymization techniques in operational and non-operational environments to reduce the risk of re-identification or data leakage.

NIST SP 800-53 Rev.5

PM-17 - Protection of PII: Requires implementation of privacy-enhancing technologies such as masking and pseudonymization to safeguard personal data.

PT-2, PT-3 - Minimization and Security of PII Processing: Supports transformation of data to reduce identifiability and enforce access control over re-identification processes.

SC-12, SC-28, SC-30 - Data Confidentiality and Integrity: Establish confidentiality and obfuscation controls for data in storage, transmission, and use, including tokenization and irreversible masking techniques.

EU GDPR (2016/679)

Article 4(5) - Definition of Pseudonymization: Formally defines pseudonymization as a processing activity that reduces identifiability while maintaining reversibility under strict controls.

Article 32 - Security of Processing: Recognizes pseudonymization as a technical and organizational measure to protect data subject rights and reduce breach impact.

Article 5(1)(c, f) - Data Minimization and Confidentiality: Mandates use of data masking and pseudonymization to reduce unnecessary exposure and ensure appropriate safeguards.

EU NIS2 Directive (2022/2555)

Article 21(2)(c): Requires proportionate technical and organizational measures, such as PETs, to reduce impact of data compromise through secure transformation and risk reduction techniques.

EU DORA (2022/2554)

Article 10(1) - ICT Risk Management Framework: Requires entities to integrate confidentiality and data protection controls, including masking and pseudonymization, into operational and testing environments.

Article 10(2)(e): Reinforces the need to protect personal and financial data across systems, including through use of transformation technologies to limit direct exposure.

COBIT 2019

DSS05.01 - Protect Information Assets: Requires data masking and pseudonymization to prevent unauthorized access and disclosure.

DSS06.06 - Secure Testing and Analytics: Directs organizations to apply masking in environments that are not subject to full production-level controls.

MEA03 - Monitor, Evaluate, and Assess Compliance: Calls for regular review of data protection controls, including validation of masking and pseudonymization efficacy.