TITLE: Information Security and Data Protection Policy

CONTENTS

1. INTRODUCTION 2

2. FUNDAMENTAL PRINCIPLES OF INFORMATION SECURITY 2

3. DATA SUBJECT RIGHTS 4

4. INFORMATION MANAGEMENT AND ORGANIZATIONAL PROCESSES 4

5. INFORMATION SECURITY 4

1. INTRODUCTION

Purpose

This Policy has been drafted to demonstrate the Organization's commitment to ensuring the security of valuable information and protecting personal data.
Its objective is to guarantee transparent, secure, and compliant information processing, in accordance with applicable mandatory requirements, including ISO/IEC 27001, the VDA ISA 6.0.3 "Information Security Assessment Questionnaire" standard, the European Union General Data Protection Regulation (GDPR), and relevant Italian legislation.
This Policy adopts an approach designed to foster stakeholders' trust and safeguard the Organization's reputation, while ensuring effective and efficient operations.

Scope of Application

This Policy applies to all information that holds value for TMB S.p.A, including all personal data collected, processed, stored, or transferred by the Organization, regardless of format. This includes, but is not necessarily limited to, information relating to customers, employees, suppliers, and other stakeholders, as well as information concerning products manufactured by or on behalf of such Parties.
The Policy applies to all organizational units, the personnel operating within them, and third parties processing valuable information, including personal data, on behalf of the Organization.
In the following paragraphs, the term "information" refers to one or more pieces of information, of any nature, that hold value for TMB S.p.A, including personal data. Similarly, the term "information security" refers collectively to the framework adopted by TMB S.p.A. to protect valuable information, including personal data. Any principles and provisions specifically applicable to personal data will be appropriately highlighted throughout the text.

Responsibilities and Governance

Responsibility for managing and ensuring compliance with this Policy is assigned to the Information Security Committee, which includes representation from senior management and the Privacy Officer, supported by external consultants.
However, information security is a shared responsibility. All personnel handling information of value to TMB S.p.A. are required to understand and comply with this Policy and all related implementing documentation.

2. FUNDAMENTAL PRINCIPLES OF INFORMATION SECURITY

Security Aspects

The Organization recognizes that an information security approach entails a commitment to preserving over time:

- **Confidentiality**: ensuring that information is accessible only to authorized entities.
- **Integrity**: ensuring that information retains its accuracy and completeness over time with respect to the fact, act, or entity it represents.
- **Availability**: ensuring that information is accessible to an authorized entity upon request.

Legal and Regulatory Foundations

The Organization is committed to identifying and complying with all mandatory requirements (laws, regulations, and standards) applicable to information security.
In particular, this Policy is aligned with the following fundamental principles:

1. **Need-to-know principle**: access rights to and processing of valuable information are granted strictly on a necessity basis, with all rights and privileges denied by default unless strictly required for the proper execution of authorized processing activities.

2. **Zero Trust model**: any processing activity involving valuable information is, by default, considered potentially harmful and is therefore governed accordingly, regardless of whether it is initiated by an individual, IT system, or infrastructure component operating under the Organization's control.

With regard to personal data processing, in compliance with the GDPR, the following additional principles apply:

1. **Lawfulness, fairness, and transparency**: data are processed lawfully, fairly, and transparently toward the data subject.
2. **Purpose limitation**: data are collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data minimization**: data collected are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: data are accurate and, where necessary, kept up to date; all reasonable measures are taken to promptly erase or rectify inaccurate data.
5. **Storage limitation**: data are retained in a form that permits identification of data subjects for no longer than necessary for the purposes for which they are processed.
6. **Integrity and confidentiality**: data are processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, through appropriate technical and organizational measures.

Pragmatic Compliance

The Organization adopts a pragmatic approach to compliance, aiming to integrate regulatory requirements in a manner that supports business objectives. This entails:

1. **Continuous assessment**: ongoing monitoring of the relevant regulatory framework to ensure procedures and practices remain current and compliant.
2. **Technological integration**: use of advanced tools and technologies to facilitate compliance, such as automated systems for managing access rights and privileges, obtaining processing consent, tracking and managing data subject requests, and maintaining records and documentation.

To this end, the Organization has adopted an Information Security Organizational Model designed to govern information security in compliance with applicable mandatory and voluntary requirements, including the GDPR, VDA ISA 6.0.3 "Information Security Assessment Questionnaire," and ISO/IEC 27001.

Data Minimization and Efficiency

The collection and retention of information must be limited to what is strictly necessary for legitimate purposes. This includes:

1. Assessment of necessity: prior analysis to determine the necessity and relevance of information before collection.
2. Data deletion: periodic deletion or anonymization of information no longer required for legitimate purposes.

Transparency and Clear Communication

The Organization is committed to clearly and transparently communicating its information processing practices and the technical and organizational measures implemented to safeguard information security. This includes:

1. **Documented policies and procedures**: technical and organizational measures must, where necessary, be accompanied by documented implementation procedures.
2. **Privacy notices**: easily accessible and understandable privacy notices, including schematic formats where appropriate, explaining how and why personal data are collected and used.

3. **Proactive communication**: notification to data subjects of significant changes in data processing practices or privacy policies.

3. DATA SUBJECT RIGHTS

The Organization recognizes and respects all data subject rights in accordance with the GDPR and Italian law. Simplified procedures are adopted to ensure:

1. Access to data: enabling data subjects to easily access their personal data.
2. Rectification and erasure: providing straightforward mechanisms for correcting or deleting personal data.
3. Objection to processing: enabling data subjects to object to processing under applicable circumstances.

4. INFORMATION MANAGEMENT AND ORGANIZATIONAL PROCESSES

The effective integration of information security into organizational processes is essential. This includes:

1. Risk assessment: conducting regular risk assessments to identify and mitigate potential risks associated with processing valuable information.
2. Flexible procedures: developing policies adaptable to evolving business and regulatory requirements.
3. Continuous improvement: deriving lessons from both routine operations and abnormal or critical situations (such as security incidents) to continuously enhance the Information Security and Privacy Organizational Model.

5. INFORMATION SECURITY

Security Measures

To protect information against breaches of confidentiality (unauthorized access or disclosure), integrity (unauthorized alteration), and availability (accidental or deliberate events resulting in loss of access), the Organization implements appropriate security measures, including:

1. Technical safeguards: adoption of physical and technological solutions such as locked cabinets, encryption, access control mechanisms, and network security measures that are effective while remaining operationally sustainable.
2. Organizational procedures: establishment of clear data management procedures, including protocols for internal information sharing and secure transfers to and from external Parties.

Proactive Security Incident Management

In the event of security incidents, including personal data breaches, the Organization follows a defined procedure:

1. Detection and rapid response: prompt identification and response to minimize impact.
2. Breach notification: communication of breaches to supervisory authorities and affected data subjects as required by law.
3. Review and prevention: root cause analysis and implementation of corrective measures to prevent recurrence.

International Transfers of Personal Data

International transfers of personal data are carefully managed to ensure compliance with the GDPR and other applicable laws, balancing the preference for EU-based suppliers and technologies with the potential use of extra-EU solutions. Preference is given to:

1. Contractual safeguards: use of standard contractual clauses and other legal mechanisms to ensure adequate protection when transferring data outside the European Union.
2. Adequacy assessments: evaluation of data protection laws in recipient countries to ensure an adequate level of protection.

Training and Awareness

To ensure all personnel understand their role in information security and how to handle information securely, the Organization provides:

1. Regular training programs: ongoing training on information security, cybersecurity, GDPR compliance, and security best practices.
2. Training materials: accessible resources such as manuals and online guides to support understanding and implementation of information security policies.

Monitoring, Evaluation, and Updating

To ensure policies and practices remain effective and relevant, the Organization undertakes:

1. Audits and assessments: internal audits and risk assessments to monitor compliance and the effectiveness of technical and organizational measures.
2. Continuous updates: revision of policies and procedures in response to regulatory, technological, or business changes to maintain effective information security.

Disciplinary Aspects

The Organization's commitment to information security and personal data protection is not solely the result of legal and contractual obligations but also a deliberate choice aimed at fostering and maintaining the trust of all stakeholders (Customers, Institutions, Authorities).

Active cooperation from all parties, whether internal or external to TMB S.p.A., in understanding and complying with policies, procedures, and internal regulations issued by TMB S.p.A. for information security and data protection is essential to ensure that the actual level of security achieved aligns with the Organization's commitments and objectives. All Company personnel are therefore required to understand and properly apply TMB S.p.A's information security and privacy provisions. Incidents involving valuable information or personal data that, following internal review, are attributable to inappropriate conduct (failure to comply with policies and procedures due to negligence, carelessness, or intentional misconduct) may result in disciplinary measures in accordance with applicable legislation.

Last Update: 2025/01/27