NORMA DATATRUST - NOBLESSE			
	Last Review Date: 12/10/2025	**Reviewed:** CTO Noblesse	**Code:** DTN-ICS-001

Certification Standard in Cybersecurity, Privacy and Digital Trust

1. Introduction

In the context of a global and interconnected digital economy, the secure and ethical management of information has emerged as a strategic imperative for organizations. The DataTrust Noblesse Standard (DTN), developed by Noblesse SpA, establishes a comprehensive, verifiable, and high-level framework for assessing and certifying cybersecurity, privacy, and digital trust management systems.

The fundamental purpose of this standard is to provide a robust framework that allows organizations to objectively and auditably demonstrate their adherence to the principles of confidentiality, integrity, availability, transparency, and resilience in the processing of personal data and critical information assets. The DataTrust Noblesse Seal constitutes the tangible seal that certifies compliance with these rigorous requirements, functioning as a seal of guarantee that strengthens reputation and fosters sustainable relationships of trust with customers, partners, regulators, and society at large.

2. Scope and Applicability

The DataTrust Noblesse Standard is generically applicable and is designed to be implemented by any organization, regardless of its size, sector of activity, legal nature, or technological complexity. Its scope includes, but is not limited to:

- Private sector companies (SMEs and large corporations).
- Public sector institutions and government agencies.
- Non-profit organizations (NGOs).
- Technology, financial, and healthcare service providers.
- E-commerce and digital economy platforms.
- Educational and research entities.

The scope of the certification may be defined as Organizational (Global), covering the entire entity, or Specific (Partial), limited to clearly defined processes, services, information systems, or business units. This flexibility allows for progressive adoption proportional to the risk profile and structure of each organization.

3. Objectives of the DataTrust Seal

The mission of the DataTrust Noblesse Seal is to serve as a catalyst for improving the security and privacy posture in the digital ecosystem. Its strategic objectives are articulated in the following points:

Ensure Information Protection: Ensure that information assets are protected against unauthorized access, alteration, destruction, or disclosure by implementing technical and administrative controls aligned with the principles of the CID triad (Confidentiality, Integrity, Availability).

Ensure Regulatory Compliance: Establish a framework that facilitates compliance with a complex regulatory ecosystem, including, but not limited to, the GDPR, LGPD, CCPA, as well as international standards such as ISO/IEC 27001, ISO/IEC 27701, and the NIST Cybersecurity Framework.

Promote Transparency and Ethics: Promote transparent practices in the management of personal data, ensuring that data subjects can effectively exercise their rights (ARCO/PARC and other similar rights) and that data processing is carried out under the principles of legality, loyalty, and minimization.

Mitigate Operational and Reputational Risks: Reduce the likelihood and impact of security incidents that may result in legal sanctions, financial losses, or damage to corporate reputation.

Establish a Culture of Continuous Improvement: Promote a perpetual cycle of evaluation, implementation, review, and improvement of security and privacy controls, proactively adapting to the evolving threat landscape.

4. Guiding Principles

The certification is based on the following guiding principles, which constitute the philosophical basis of all its requirements:

Transparency: Organizations must maintain clear, accessible, and truthful communication about their policies, practices, and controls related to data security and privacy to all stakeholders.

Responsibility: A clear governance structure must be established and documented that assigns specific roles, responsibilities, and accountabilities for cybersecurity and privacy at all levels of the organization.

Objective Evidence: All claims of compliance must be supported by objective, verifiable, and reproducible evidence obtained through records, logs, audit reports, and other documentary artifacts.

Risk-Based Approach: The control measures implemented must be proportional to the identified risks, considering the nature, scope, context, and resources of the organization, avoiding unnecessary burdens without compromising effectiveness.

Continuous Improvement: Certification is not a static state, but a dynamic process that requires periodic review and optimization of management systems to respond to changes in the internal and external environment.

5. Certification Requirements

Compliance

The DataTrust Noblesse Standard requires the implementation and effective operation of controls in the following five critical areas:

5.1. Security Governance and Management

The organization must establish a formal governance framework that includes an information security policy, a Security Committee, the designation of a Chief Information Security Officer (CISO) and/or a Data Protection Officer (DPO), and the clear assignment of responsibilities.

5.2. Data Protection and Privacy by Design and by Default

The implementation of technical and organizational measures is required to ensure compliance with privacy principles from the design phase of any product or process. This includes conducting Data Protection Impact Assessments (DPIAs), managing consent, and enabling effective channels for data subjects to exercise their rights.

5.3. Risk Management and Technical Controls

The organization must maintain a systematic process for identifying, analyzing, evaluating, and addressing information security risks. Robust controls must be implemented, including, but not limited to: access and identity management, data encryption, perimeter and endpoint security, backups, and recovery plans.

5.4. Security Incident and Data Breach Management

It is mandatory to have a formalized procedure for the detection, reporting, analysis, response, and communication of security incidents and personal data breaches. Detailed records of each incident must be kept, and the response plan must be periodically tested.

5.5. Internal Audit and Documentary Evidence

The organization must conduct planned and periodic internal audits to verify compliance with the standard. An up-to-date and accessible body of documentation must be maintained, including policies, procedures, activity logs, audit reports, and evidence of the operation of controls.

6. Certification Process

The process for obtaining the Noblesse DataTrust Seal is structured in the following phases:

Application and Contract: Formal submission of the application and signing of the contract with Noblesse SpA, defining the scope of the certification.

Gap Analysis: Voluntary preliminary audit to identify deviations between the organization's current status and the standard's requirements.

Implementation and Preparation: The organization addresses the identified nonconformities and prepares the required body of documentary evidence.

Certification Audit: A team of independent and qualified auditors, appointed by Noblesse, conducts an on-site and/or remote assessment to verify the implementation and effectiveness of all requirements.

Decision and Issuance of the Seal: After analyzing the findings and resolving all major nonconformities, Noblesse issues the certificate and grants the right to use the DataTrust Seal.

Surveillance Audits: Annual surveillance audits are conducted to confirm continued compliance.

Renewal: At the end of the certificate's validity period (3 years), a new complete certification audit cycle begins.

7. Use of the Seal and Trademarks

The DataTrust Noblesse Seal is a registered trademark owned by Noblesse SpA. Its use is strictly regulated and limited to organizations that maintain a current certification. It must be displayed along with the license number and validity dates. Any unauthorized use, falsification, or misleading use of the Seal will result in immediate revocation of the certification and may lead to legal action.

8. Contractual Commitments and Revocation

The relationship between Noblesse SpA and the certified organization is governed by a service agreement. This document establishes the rights and obligations of both parties, the conditions of the audits, the fees, and the specific grounds for suspension or revocation of the certification. The certified organization agrees to notify the organization of any significant changes that may affect its compliance.

9. Regulatory Annexes

This standard is complemented by a series of informative and regulatory annexes (these can be requested via email info@noblessepartners.com), which provide detailed guidance and include:

- Annex A: Policy and Procedure Templates (Security, Privacy, Incident Management).
- Annex B: Guide for the Implementation of a Risk Management System.
- Annex C: Standard Contractual Clauses and Confidentiality Agreements.
- Annex D: Record Templates (Risk Matrix, Incident Logs, Audit Minutes).
- Annex E: Metrics and Key Performance Indicators (KPIs) for Maturity Measurement.

10. Conclusion

The Noblesse DataTrust Standard represents a benchmark of excellence in the field of cybersecurity and privacy. Its ad

This option transcends mere regulatory compliance, positioning itself as a strategic statement of commitment to digital trust. Obtaining the DataTrust Seal is not an end, but rather the beginning of a path of continuous improvement, providing a sustainable competitive advantage and demonstrating responsible, ethical, and resilient information management to the market.