**Information Security and Compliance Automation**

**信息安全定义（Definition of Information Security）**

**中文：**  
根据《网络与信息系统安全指令》（NIS指令）以及更新后的NIS 2指令，信息安全的核心是保护网络和信息系统的**可用性**、**真实性**、**完整性**和**机密性**，以确保数据和服务不受以下事件的影响：

* 未经授权的访问
* 数据篡改或破坏
* 系统中断或停机

此外，法规如《网络安全法》（Cybersecurity Act）明确了信息安全的标准，要求成员国和企业采取措施保护网络和数据系统的运行安全。

**英文：**  
According to the Network and Information Systems Security Directive (NIS Directive) and the updated NIS 2 Directive, information security focuses on protecting the **availability**, **authenticity**, **integrity**, and **confidentiality** of network and information systems. This ensures that data and services are safeguarded from:

* Unauthorized access
* Data alteration or destruction
* System interruptions or downtime

Furthermore, regulations like the Cybersecurity Act specify security standards, requiring member states and enterprises to implement measures to ensure the operational security of networks and data systems.

**法律角色（Role of the Law）**

**中文：**  
法律在信息安全和合规中发挥着以下重要作用：

1. **预防性措施（Preventive Measures）**
   * **设立保护级别的规则**：定义数据和系统的安全标准，如加密和访问控制。
   * **管理和治理规则**：要求企业和组织设立信息安全管理体系，确保合规性。
   * **强制性报告和合作要求**：规定在发生安全事件时需向监管机构报告，并与其他相关实体合作。
2. **补救性措施（Reparative Measures）**
   * **违规处罚机制**：针对未遵守安全标准的实体，法律设有严格的行政罚款和其他责任追究方式（例如GDPR中的罚款最高可达年营业额的2%）。
   * **经济赔偿与保险**：如网络犯罪和责任保险、身份盗窃保险，用以覆盖潜在损失。
   * **司法取证（Forensic IT）**：通过技术手段调查安全事件，为法律追责提供证据。

**英文：**  
The law plays a critical role in information security and compliance by establishing both preventive and reparative measures:

1. **Preventive Measures**
   * **Rules for protection levels**: Define security standards for data and systems, such as encryption and access controls.
   * **Rules for management and governance**: Require enterprises and organizations to establish information security management systems to ensure compliance.
   * **Mandatory reporting and cooperation requirements**: Specify that security incidents must be reported to regulatory authorities and mandate cooperation with other relevant entities.
2. **Reparative Measures**
   * **Sanction mechanisms for violations**: Laws impose strict administrative fines and other liabilities for non-compliance (e.g., GDPR fines can reach up to 2% of annual turnover).
   * **Economic compensation and insurance**: Includes cybercrime and liability insurance, as well as identity theft insurance to cover potential losses.
   * **Forensic IT**: Employ technical methods to investigate security incidents and provide evidence for legal accountability.

**1. GDPR 相关条款**

**Article 5 – Principles relating to processing of personal data**

**第5条 – 个人数据处理原则**

1. Personal data shall be:  
   **个人数据应：**  
   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');  
   **(a)** 合法、公平并以透明方式处理（“合法性、公平性和透明性”）；  
   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');  
   **(b)** 为特定、明确和合法的目的收集，不得以与这些目的不符的方式进一步处理（“目的限制”）；  
   (c) adequate, relevant and limited to what is necessary in relation to the purposes ('data minimisation');  
   **(c)** 数据应适当、相关并限于必要范围（“数据最小化”）；  
   (d) accurate and, where necessary, kept up to date ('accuracy');  
   **(d)** 数据应准确并在必要时及时更新（“准确性”）；  
   (e) kept in a form permitting identification of data subjects for no longer than necessary ('storage limitation');  
   **(e)** 数据应以允许识别数据主体的形式保存，保存时间不得超过必要时长（“存储限制”）；  
   (f) processed in a manner ensuring appropriate security ('integrity and confidentiality').  
   **(f)** 以确保适当安全的方式处理，包括防止未经授权的处理（“完整性和机密性”）。

**Article 25 – Data protection by design and by default**

**第25条 – 通过设计和默认实现数据保护**

* Implement appropriate technical and organisational measures, such as pseudonymisation, to integrate data-protection principles effectively.  
  **采取适当的技术和组织措施（如伪匿名化），以有效实施数据保护原则。**

**Article 30 – Records of processing activities**

**第30条 – 处理活动记录**

* Controllers must maintain records of processing activities, including the purposes, categories of data, and security measures.  
  **控制者必须记录处理活动，包括目的、数据类别和安全措施。**

**Article 32 – Security of processing**

**第32条 – 处理的安全性**

* Implement appropriate measures such as encryption and the ability to ensure system resilience.  
  **实施适当措施（如加密），确保系统的持续可用性和恢复能力。**

**Article 33 – Notification of a personal data breach**

**第33条 – 个人数据泄露的通知**

* Notify the supervisory authority of a data breach within 72 hours of becoming aware of it.  
  **在发现数据泄露后72小时内通知监督机构。**

**Article 34 – Communication of a data breach to the data subject**

**第34条 – 向数据主体通报数据泄露**

* If the breach poses a high risk to data subjects' rights, they must be informed without undue delay.  
  **如果泄露可能对数据主体的权利构成高风险，应毫不延迟地通知相关个人。**

**Article 35 – Data protection impact assessment**

**第35条 – 数据保护影响评估**

* Conduct an impact assessment before processing high-risk data activities.  
  **在进行高风险数据活动之前进行影响评估。**

**Article 39 – Tasks of the data protection officer (DPO)**

**第39条 – 数据保护官的任务**

* Ensure compliance with GDPR, monitor activities, and provide advice on data protection.  
  **确保符合GDPR，监控活动，并就数据保护提供建议。**

**2. NIS 2 指令相关条款**

**Article 2 – Scope and exclusions**

**第2条 – 范围和排除范围**

* Applies to entities listed in Annex I and II, such as energy, finance, and healthcare sectors.  
  **适用于附件I和II中列出的实体，例如能源、金融和医疗行业。**

**Article 21 – Cybersecurity risk management measures**

**第21条 – 网络安全风险管理措施**

* Entities must implement technical, operational, and organisational measures such as risk analysis, incident handling, and supply chain security.  
  **实体需实施技术、操作和组织措施，包括风险分析、事件处理和供应链安全。**

**Article 23 – Reporting requirements**

**第23条 – 报告要求**

* Significant incidents must be reported within specific timeframes:
  + 24 hours: early warning
  + 72 hours: formal notification
  + One month: final report  
    **重大事件需在以下时间内报告：24小时内初步警告；72小时内正式通知；1个月内提交最终报告。**

**Article 30 – Records of processing activities**

**第30条 – 处理活动记录**

* Entities must document cybersecurity measures and their implementation.  
  **实体需记录网络安全措施及其实施情况。**

**Article 33 – Supervision and enforcement**

**第33条 – 监督与执行**

* Authorities may conduct inspections, audits, and security scans to ensure compliance.  
  **主管机构可进行检查、审计和安全扫描，以确保合规。**

**Article 34 – Penalties**

**第34条 – 处罚**

* Administrative fines can reach up to €10 million or 2% of annual turnover for essential entities.  
  **对关键实体的行政罚款最高可达1000万欧元或年营业额的2%。**