NIS2指令

**1. NIS2 指令的目标**

**Objective of NIS2 Directive**

**中**：  
NIS2 指令旨在建立统一的网络安全标准，加强成员国在网络安全事件防护、风险管理和应急响应方面的能力。

**英**：  
The NIS2 Directive aims to establish a unified cybersecurity framework, enhancing the capabilities of member states in preventing, managing, and responding to cybersecurity incidents.

**2. 主要法律义务**

**Main Legal Obligations**

**(1) 主动义务 – Proactive Obligations**

**中**：

* 实施适当的风险管理和安全控制措施。
* 建立定期的网络安全审计和监控机制。
* 提供网络安全培训和教育。

**英**：

* Implement appropriate risk management and security control measures.
* Establish regular cybersecurity audits and monitoring mechanisms.
* Provide cybersecurity training and education.

**(2) 被动义务 – Reactive Obligations**

**中**：

* 事件发生后及时报告。
* 采取补救措施，减少事件影响。
* 向国家主管部门提交事件调查报告。

**英**：

* Report incidents promptly after detection.
* Take remedial actions to mitigate the impact of incidents.
* Submit incident investigation reports to national authorities.

**3. 扩展范围（Expanding the Scope）**

**中**：

* 新指令扩大了适用的行业范围，包括公共管理、医疗、能源和运输等关键领域。
* 覆盖更多中小企业，确保它们符合最低网络安全标准。

**英**：

* The new directive broadens the scope to include sectors such as public administration, healthcare, energy, and transportation.
* Covers more SMEs to ensure they meet minimum cybersecurity standards.

**4. 高层管理的责任**

**Responsibility of Senior Management**

**中**：

* 高层管理者需要承担网络安全的最终责任。
* 他们需确保组织内网络安全政策的落实，并提供必要的资源。

**英**：

* Senior management must take ultimate responsibility for cybersecurity.
* They should ensure the implementation of cybersecurity policies within the organization and allocate necessary resources.

**5. 重大影响事件的定义**

**Definition of Significant Impact Incidents**

**中**：

* 对关键服务的中断超过一定时间。
* 导致经济损失或社会影响。
* 对国家安全或公共安全造成威胁。

**英**：

* Disruption of critical services for a specified period.
* Resulting in economic loss or societal impact.
* Threatening national security or public safety.

**6. 违规后果（Consequences of Infringements）**

**中**：

* 对违规企业或个人实施经济处罚。
* 严重违规可能导致运营许可证的吊销或其他行政处罚。

**英**：

* Imposing financial penalties on non-compliant entities or individuals.
* Severe infringements may lead to revocation of operational licenses or other administrative penalties.

**7. 合规性实践指南**

**Practical Guidance for Compliance**

**中**：

* 组织需要制定内部合规政策和程序。
* 建立网络安全应急响应团队（CSIRT）。
* 定期进行风险评估，确保技术和管理控制的有效性。

**英**：

* Organizations must establish internal compliance policies and procedures.
* Set up a Cybersecurity Incident Response Team (CSIRT).
* Conduct regular risk assessments to ensure the effectiveness of technical and managerial controls.

**总结**

NIS2 指令为欧盟成员国和相关行业设定了明确的网络安全要求，包括风险管理、事件报告和高层管理的责任。这一框架旨在提高整个欧盟的网络安全水平，保护关键基础设施和公共服务的正常运行。

如果您需要深入解释某个具体条款或进一步分析，请告诉我！

《NIS2指令》的主要条款和变化可以总结为以下几点，中英对照：

**1. 目标与背景 (Objective and Background)**

* **中**：NIS2旨在提高欧盟范围内网络安全的共同水平，覆盖关键行业和服务，解决现有法规实施中的碎片化问题。
* **英**：The NIS2 Directive aims to enhance the common level of cybersecurity across the EU, covering critical sectors and addressing fragmentation in the implementation of existing regulations.

**2. 扩大适用范围 (Expanded Scope)**

* **中**：新指令涵盖能源、交通、公共行政、医疗、金融等关键部门，以及电信和数字基础设施。
* **英**：The new directive covers critical sectors such as energy, transport, public administration, healthcare, finance, as well as telecommunications and digital infrastructure.

**3. 报告义务 (Incident Reporting Obligations)**

* **中**：关键实体必须在24小时内提交初步报告，并在一个月内提交完整报告。
* **英**：Essential entities must submit an initial report within 24 hours and a full report within one month.

**4. 管理责任 (Management Responsibility)**

* **中**：高级管理层需对网络安全承担最终责任，并确保实施适当的风险管理措施。
* **英**：Senior management must take ultimate responsibility for cybersecurity and ensure the implementation of appropriate risk management measures.

**5. 处罚与执行 (Penalties and Enforcement)**

* **中**：违规可能面临高达1000万欧元或全球营业额2%的罚款。
* **英**：Non-compliance may result in fines of up to €10 million or 2% of global turnover.