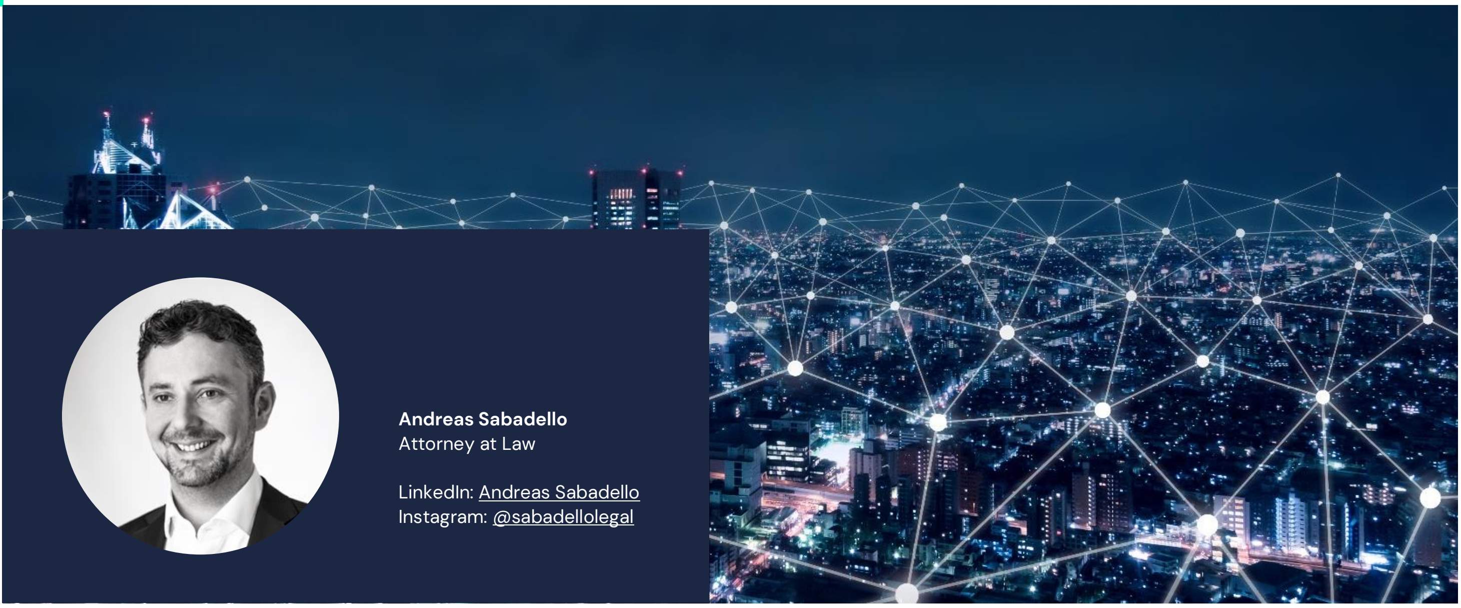

Andreas Sabadello
Attorney at Law

LinkedIn: Andreas Sabadello
Instagram: @sabadellolegal

Draft transposition of the NIS 2 Directive into Austrian law

On July 3rd, 2024, the Austrian National Council (*Nationalrat*) declined to pass a federal act to transpose Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (**NIS 2 Directive**). The "Federal Act to Ensure a High Level of Cybersecurity of Network and Information Systems (Network and Information System Security Act 2024) "[i] foresaw that the Act should have come into **effect on June 1, 2025**. The draft legislation was set to be passed in the National Council on relatively short notice after a nearly identical draft from spring 2024 had failed to receive positive feedback from stakeholders.

The only slightly revised draft still contained several provisions that were unclear and contrary to principles of the allocation of competences between federal and state bodies. Due to the latter the government would have needed a qualified majority vote to pass the draft legislation. All opposition parties withheld their approval.

However, it can be expected that several key substantive regulations will be found in the eventual national act that are already included in the current draft(s). The summary below can therefore serve as a guideline for the obligations to come. The time still available for preparation should be utilized in view of the threat of draconian penalties (cf. Violations and fines below).

Key obligations

According to the last available draft, [ii] entities who are subject to the NIS2 Act have to comply with the following key obligations:

1) Registration with the Cybersecurity Authority

Under **section 29** of the draft the Cybersecurity Authority[iii] shall maintain a register of essential and important entities, including entities providing domain name registration services. All essential and important entities are **obliged to register with the cybersecurity authority** within **three months of the entry into force of the NIS2 Act**. The entities must transmit the following information to the Cybersecurity Authority electronically in a structured manner via a secure communication channel:

1. the name of the entity;
2. the address and current contact details and, if applicable, the representative appointed in accordance with section 28 para 4 of the Draft; these contact details must include at least a telephone number and an e-mail address for the receipt and exchange of cybersecurity information with the Cybersecurity Authority;[iv]

3. the sector or sectors, the subsector or subsectors and the type or types of entity referred to in Appendix 1 or 2 of the draft;
4. the Member States of the European Union in which it provides services;
5. where applicable the entity's IP ranges;
6. the address of the main establishment of the entity and its other branches in the European Union or, if it is not established in the European Union, the address of its representative appointed in accordance with section 28 para 4 of the Draft;
7. information on the thresholds set out in section 25 of the NIS2 and whether it is a significant or important entity.

Note, that at the time of this publication no concrete details on the electronic submission via a secure communication channel are available. The explanatory notes to the draft legislation state that the communication channel to be used (e.g. an online form provided) should be brought to the attention of essential and important entities in good time, for example by publication on a publicly accessible website. It could also be considered to provide for electronic transmission via the already existing "Business Service Portal" (*Unternehmensserviceportal*).[v]

Changes of the data regarding items 1, 2 and 3 must be notified to the Cybersecurity Authority as soon as possible but in any case, **no later than two weeks** from the date of the change. Changes regarding items 4, 5, 6 and 7 above must be notified as soon as possible but in any case, no later than **three months** from the date of the chage.

2) Governance[vi]

The act clearly underlines the importance of cybersecurity as a management task and **section 31 para 1** of the Draft stipulates, that the **management bodies** of essential and important entities **must ensure and supervise compliance** with the risk management measures in accordance with section 32 of the Draft. This obligation is further reinforced by section 31 **para 2** which obliges **management bodies** of essential and important entities to **participate in cyber security training** specifically designed for them. Furthermore, entities shall regularly **provide appropriate training to employees** to enable them to acquire sufficient knowledge and skills to recognise and assess risks and management practices in the area of cybersecurity and its impact on the services provided by the entity.

3) Cybersecurity risk-management measures

Section 32 para 1 of the Draft stipulates that **essential and important entities** must implement **appropriate and proportionate** technical, operational and organisational **risk management measures** in several areas. These subject areas are laid out in Appendix 3 of the Draft, which you will find below with a translation to English.

Such risk management measures must aim at

* managing the risks to the security of the network and information systems these entities use to operate or provide their services and
* to prevent or minimise the impact of cyber security incidents on the recipients of their services and on other services.

Section 32 **para 2** of the Draft lays out the following criteria for risk management measures, which shall duly take into account:

1. ensure a level of cybersecurity appropriate to the existing risk, taking into account
   a) the state of the art and, where appropriate, the relevant national, European and international standards and best practices; and
   b) the costs of implementation;
2. be based on a multi-hazard approach aimed at protecting network and information systems and their physical environment from cybersecurity incidents; and
3. for the security of supply chains

a) the specific vulnerabilities of each direct supplier and service provider, the overall quality of the products and cybersecurity practices of their suppliers and service providers, including the security of their development processes; and

b) the results of the coordinated risk assessments carried out in accordance with Article 22 no 1 of the NIS 2 Directive in relation to the security of critical supply chains,

Section 32 **para 3** of the NIS 2 Act provides the following parameters for assessing the proportionality of risk management measures: due consideration shall be given

* to the extent of the risk exposure of the entity and its services,

* the size of the entity and

* the likelihood of cybersecurity incidents occurring and their severity, including their social and economic impact.

As these criteria and parameters are still rather broad, section 32 **para 4** of the Draft stipulates that the **Federal Minister** of the Interior **shall specify the risk management measures** in these subject areas with regard to technical, operational and organisational requirements **by** a **(future) ordinance**. In addition, the Federal Minister of the Interior may also specify sector-specific requirements for these risk management measures by ordinance. These future specifications are intended to provide the parties subject to these obligations with a clear framework within which risk management measures can be implemented in a proportionate, suitable and risk-appropriate manner. In addition, the state of the art, relevant standards and best practices and the costs of implementation must be taken into account. The supplements to the draft legislation also mention that (co-determination) rights to which the works councils and other affected parties are entitled, in particular those under the Labour Constitution Act (*Arbeitsverfassungsgesetz*) and the GDPR, remain unaffected.

4) Demonstration of the effectiveness of risk management measures

Section 33 para 1 of the Draft stipulates that **essential and important entities** must submit a list of implemented risk management measures pursuant to section 32 in a structured form in accordance with the Cybersecurity Authority's specifications (self-declaration) **within six months of being requested** to do so by the Cybersecurity Authority. (Sub)sectoral risk analyses by the Cybersecurity Authority can, for example, be the basis for requesting the submission of such self-declaration(s).

Section 33 **para 2** of the Draft stipulates that **essential entities** shall **within three years of being requested** to do so by the Cybersecurity Authority, provide the Cybersecurity Authority with evidence of the current implementation of risk management measures pursuant to section 32 by means of an **audit by an independent body**. For this purpose, the respective essential entity shall submit to the Cybersecurity Authority an audit report on the effectiveness of the current implementation of risk management measures pursuant to section 32, including any deficiencies identified, and an action plan addressing these deficiencies in a structured form in accordance with the specifications of the Cybersecurity Authority, signed by the authorised management bodies of the essential entity and by the independent body as well as by the concrete independent auditors appointed.

With regard to **important entities** however, section 33 **para 3** Draft stipulates that the Cybersecurity Authority can (only) **request** such entities to provide evidence of the implementation of the risk management measures pursuant to section 32 by means of an audit by an independent body **if** there is supporting evidence, in particular a self-declaration, or other well-founded indications and information that suggest that an important organisation is not fulfilling its obligations under the Draft (particularly under sections 32 and 34). The same criteria apply to the audit as for essential entities. The difference between the obligations for essential entities and for important entities is therefore, that essential entities have to submit the audit report within three years of the request to submit the self-declaration (para 1), whereas important entities only have to submit such report within three years of a separate, specific request to do so.

The **costs of audits** by independent bodies pursuant to the respective paragraphs shall be borne by the audited entity, unless the Cybersecurity Authority decides otherwise in duly justified cases (section 33 para 4). Oddly the draft does not clarify what such "duly justified cases" could be.

Furthermore, **essential and important** entities shall notify the Cybersecurity Authority of planned audits pursuant to paras. 2 and 3 at least one month in advance in accordance with the Cybersecurity Authority's specifications by submitting an audit plan (section 33 para 5).

5) Reporting obligations

Section 34 of the Draft stipulates that essential and important entities shall immediately **report** any **significant cybersecurity incident** (section 35) to the sectoral CSIRT or sectoral CSIRTs responsible for them or, in the absence thereof, to the national CSIRT. Under the definition of section 35 of the Draft a **cybersecurity incident is considered significant if** it

1. has caused or may cause serious operational disruption to the services provided by the entity or serious financial loss to the entity concerned
2. it has caused or may cause significant material or immaterial damage to other natural or legal persons.

The report to the CSIRT has to include the following:

1. without undue delay, but in any case within 24 hours after becoming aware of the significant cybersecurity incident, an early warning indicating, if applicable, whether the significant cybersecurity incident is suspected to be due to unlawful and culpable acts or could have cross-border effects;
2. without undue delay and in any event within 72 hours of becoming aware of the significant cybersecurity incident, a notification of the cybersecurity incident updating, where applicable, the information referred to in point 1 and providing an initial assessment of the significant cybersecurity incident, including its severity and impact and, where applicable, the indicators of compromise;
3. at the request of a CSIRT or, where applicable, the cybersecurity authority, an interim report on relevant status updates;
4. no later than one month after the submission of the cybersecurity incident notification pursuant to No. 2, a final report containing the following:
    a. a detailed description of the cybersecurity incident, including its severity and impact;
    b. information on the nature of the threat and underlying causes that likely triggered the cybersecurity incident
    c. information on the remedial actions taken and ongoing;
    d. where applicable, the cross-border impact of the cybersecurity incident;
5. to the extent that the cybersecurity incident is still ongoing at the time the final report pursuant to No. 4 is due, the entities concerned shall submit a progress report by that time, whereby the final report must be submitted no later than one month after the end of the incident handling.

Violations and fines

The current draft legislation foresees (section 44) that the local district administrative authorities are competent to decide on fines in first instance. Several commentators have raised concerns that these rather small units with a wide variety of competences may not have the expertise to decide on matters relating to cyber security.

In section 45 the draft foresees that **essential entities** are punishable by a fine of up to EUR 10 million or up to 2 % of the total worldwide turnover in the previous financial year of the undertaking to which the essential entity belongs, whichever is higher, for violations of the act. For **important entities** the fines can go up to EUR 7 Million or up to 1.4 % of the total worldwide turnover. These fines are equally applicable to the following violations:

1. failure to fulfil the obligation to provide cybersecurity training for management bodies
2. failure to fulfil the obligation to provide cybersecurity training for employees pursuant

3. failure to implement risk management measures (unless this circumstance has become known to the cyber security authority only on the basis of a self-declaration pursuant);
4. failure to fulfil the obligation to report a significant cybersecurity incident and the associated reporting obligations,
5. failure to comply with the obligation to immediately inform the recipients of the services of an essential and important entity
6. failure to comply with the enforcement measures ordered under the act in a timely manner.

Appendix 3 to the NIS2-Act

Note: German original on the left, (unofficial) translation on the right.

Themengebiete der Risikomanagementmaßnahmen	Subject areas of risk management measures
1. Leitungsorgane	**1. Management Bodies**
a. Rollen und Verantwortlichkeiten der Leitungsorgane	a. Roles and Responsibilities of Management Bodies
2. Sicherheitsrichtlinien	**2. Security Policies**
a. Sicherheitsrichtlinien	a. Security Policies
b. Funktionen, Aufgaben und Verantwortlichkeiten	b. Functions, Tasks, and Responsibilities
3. Risikomanagement	**3. Risk Management**
a. Risikomanagementrichtlinie und Risikomanagementprozess	a. Risk Management Policy and Risk Management Process
b. Beurteilung der Effektivität von Risikomanagementmaßnahmen	b. Assessment of the Effectiveness of Risk Management Measures
c. Überwachung der Einhaltung von Vorgaben	c. Monitoring Compliance with Requirements
d. Unabhängige Überprüfungen	d. Independent Reviews
4. Verwaltung von Vermögenswerten	**4. Asset Management**
a. Inventarisierung von Vermögenswerten	a. Asset Inventory
b. Klassifikation von Vermögenswerten	b. Asset Classification
c. Handhabung von Vermögenswerten	c. Asset Handling
d. Umgang mit Wechseldatenträgern	d. Handling of Removable Media
e. Rücknahme oder Löschung von Vermögenswerten	e. Asset Disposal or Deletion
5. Personalwesen	**5. Human Resources**
a. Sicherheit im Personalwesen	a. Personnel Security
b. Hintergrundüberprüfung	b. Background Check
c. Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses	c. Procedures for Termination or Change of Employment
d. Umgang mit Verstößen gegen die Sicherheitsrichtlinie	d. Handling Violations of Security Policy
6. Cybersicherheitskompetenzen und Cybersicherheitsschulungen	**6. Cybersecurity Competencies and Cybersecurity Training**
a. Vermittlung von Cybersicherheitskompetenzen	a. Imparting Cybersecurity Competencies
b. Cybersicherheitsschulungen	b. Cybersecurity Training
7. Sicherheit von Lieferketten	**7. Supply Chain Security**
a. Richtlinie zur Sicherheit von Lieferketten	a. Supply Chain Security Policy
b. Lieferantenverzeichnis	b. Supplier Directory
8. Zugangssteuerung	**8. Access Control**
a. Zugangssteuerungsrichtlinie	a. Access Control Policy
b. Verwaltung von Zugriffsberechtigungen	b. Management of Access Rights
c. Privilegierte und administrative Zugänge	c. Privileged and Administrative Access
d. Systeme und Anwendungen zur Systemadministration	d. Systems and Applications for System Administration

Themengebiete der Risikomanagementmaßnahmen	**Subject areas of risk management measures**
e. Identifikation	e. Identification
f. Authentifikation	f. Authentication
g. Multi-Faktor-Authentifikation	g. Multi-Factor Authentication
9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung	**9. Security in Procurement, Development, Operations, and Maintenance**
a. Konfigurationsmanagement	a. Configuration Management
b. Änderungsmanagement	b. Change Management
c. Umgang mit Schwachstellen und deren Offenlegung	c. Vulnerability Handling and Disclosure
d. Sicherheitstests	d. Security Testing
e. Patchmanagement	e. Patch Management
f. Sicherheit bei der Beschaffung von IKT-Diensten und IKT-Produkten	f. Security in Procurement of ICT Services and ICT Products
g. Sichere Softwareentwicklung	g. Secure Software Development
h. Netzwerksegmentierung	h. Network Segmentation
i. Netzwerksicherheit	i. Network Security
j. Schutz vor bösartiger und unautorisierter Software	j. Protection Against Malicious and Unauthorized Software
10. Kryptographie	**10. Cryptography**
a. Kryptographierichtlinie	a. Cryptography Policy
11. Umgang mit Cybersicherheitsvorfällen	**11. Handling Cybersecurity Incidents**
a. Richtlinie zum Umgang mit Cybersicherheitsvorfällen	a. Policy for Handling Cybersecurity Incidents
b. Überwachung und Protokollierung	b. Monitoring and Logging
c. Meldung von Ereignissen	c. Event Reporting
d. Korrelation und Analyse von Ereignissen	d. Event Correlation and Analysis
e. Reaktion auf Cybersicherheitsvorfälle	e. Response to Cybersecurity Incidents
f. Erkenntnisse nach Cybersicherheitsvorfällen	f. Lessons Learned from Cybersecurity Incidents
12. Betriebskontinuitäts- und Krisenmanagement	**12. Business Continuity and Crisis Management**
a. Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne	a. Business Continuity Management and Disaster Recovery Plans
b. Backup-, Redundanz- und Wiederherstellungsmanagement	b. Backup, Redundancy, and Recovery Management
c. Krisenmanagement	c. Crisis Management
13. Umgebungsbezogene und physische Sicherheit	**13. Environmental and Physical Security**
a. Sicherheitsperimeter und physische Zutrittskontrollen	a. Security Perimeter and Physical Access Controls
b. Schutz vor umgebungsbezogenen Gefährdungen	b. Protection Against Environmental Hazards
c. Versorgungseinrichtungen	c. Utility Services

[i] 4129/A XXVII. GP - *Initiativantrag*: Motion concerning a federal law enacting a Network and Information System Security Act 2024 and amending the Telecommunications Act 2021 and the Health Telematics Act 2012.

[ii] Cf. above.

[iii] The "Cybersecurity Authority" (*Cybersicherheitsbehörde*) is established with the Federal Minister for the Interior and is the competent authority under Article 8 of the NIS 2 Directive.

[iv] Cf. section 29 para 6 Draft.

[v] 2638 of the Supplements to the Stenographic Protocols of the National Council XXVII. GP.

[vi] Transposition of Article 20 of the NIS2 Directive.