KINSTELLAR

NIS 2 Directive – What you need to know

January 2023

On 27 December 2022, the Directive on "measures for a high common level of cybersecurity across the Union", repealing Directive (EU) 2016/1148 (the "**NIS 2 Directive**"), was published in the Official Journal of the European Union. The NIS 2 Directive builds on a previous NIS Directive adopted in 2016 expanding its scope to other entities. Due to a rising number of cybersecurity incidents[1] as well as ongoing increased digitalization, the aim of the NIS 2 Directive is to cover more economic sectors and to introduce additional security and reporting requirements across all EU Member States. Member States will have until 17 October 2024 to transpose the NIS 2 Directive into their national laws.

1. Who will be impacted by the NIS 2 Directive?

To date, cybersecurity regulation has been targeted at a relatively narrow group, comprising just several hundred of the key organisations deemed to have the largest impact on society in this respect. However, the NIS 2 Directive will affect a far greater number of obliged entities.[2]

Any private or public entity that simultaneously meets the two following criteria will now be subject to regulation:

i. **It provides at least one service listed in the Annexes to the Directive; and**
ii. **It is a medium-sized or large enterprise** within the meaning of Commission Recommendation 2003/361/EC, i.e. it employs 50 or more employees, or has an annual turnover or balance sheet total of at least EUR 10 million (approximately CZK 250 million).

NIS 2 newly divides entities into:

i. **Essential entities: entities providing services in the sectors of**

- energy
- transport
- banking
- financial markets infrastructure
- health
- drinking water
- waste water
- digital infrastructure
- ICT service management (B2B)
- public administration and
- space.

1. Cybersecurity incidents have been on the rise worldwide, in many cases having cross-border elements or involving subjects such as hospitals or public transport providers – and their impact can be enormous. For instance, entities present in the Czech Republic registered a significant increase in cyberattacks in 2021, as documented in the latest Report on the Current Cybersecurity Situation in the Czech Republic issued by the National Cyber and Information Security Office ("**NCISO**"), available at https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf
2. For example, in the Czech Republic, at least 6,000 obliged entities will be so classified under the NIS 2 Directive compared to the current approximately 400 entities.

ii. Important entities: entities providing services in the sectors of

- postal and courier services
- waste management
- manufacture, production and distribution of chemicals
- production, processing and distribution of food
- the manufacture of:
  - medical devices and in vitro diagnostic medical devices
  - computer, electronic and optical products
  - electrical equipment
  - machinery and equipment n.e.c.
  - motor vehicles, trailers and semi-trailers
  - other transport equipment.

However, the size of the entity in conjunction with the particular service is not the only applicable criterion used to determine whether or not an entity is subject to regulation under the NIS 2 Directive.

For certain enumerated types of services, Article 2 of the NIS 2 Directive provides that **all entities, regardless of their size, will be subject to regulation**. This applies, **for example**, to entities providing **domain name registration services, providers of public electronic communications networks or publicly available electronic communications services, trust service providers, and entities deemed critical because of their specific importance at a national or regional level** for the particular sector or type of service, or for other interdependent sectors in the given EU Member State.

Regardless of the entities' size, the NIS 2 Directive will also apply to those **entities identified as being critical under the Directive (EU) 2022/2557 on the resilience of critical entities**.

From the above it is evident that a key aim of the NIS 2 Directive is to ensure the continuity of the above services in the face of potentially disruptive incidents – thus contributing to overall security and the effective functioning of the economy and society across all EU Member States.

The NIS 2 Directive also introduces two different regimes to essential and important entities. Although the fundamental obligations under the NIS 2 Directive, such as the implementation of security measures and the reporting of security incidents, will apply to both categories of obliged persons, the specific requirements, compliance monitoring, and the respective sanctions will be stricter concerning essential entities. Furthermore, both types of entities will also be required to register with the EU Agency for Cybersecurity (ENISA).

2. What measures will need to be implemented under the NIS 2 Directive?

Essential and important entities must **take appropriate and proportionate technical, operational, and organisational measures** to manage the risks posed to the security of their network and information systems used daily for operations or the provision of services. Both types of entities will also need to **prevent or minimise the impact of incidents** on users or service recipients and other services that rely on them.

Requirements include:

- implementing risk analysis and information system security policies;
- incident handling protocols;
- mandatory training for higher management;
- implementation of a disaster recovery plan;
- introducing supply chain and network security measures, cryptography, encryption; and
- ensuring basic computer hygiene (security) practices together with the strict use of multi-factor identity verification, and secure communications along with emergency communication tools.

3. What are the incident reporting requirements?

The NIS 2 Directive will also require both types of entities to **notify the competent supervisory authority without undue delay of any cybersecurity incident** (including personal data breaches) **that has had a "significant" impact on the provision of their services**. Notably, the focus here is primarily on service delivery.

Entities will also have to **notify** their **service recipients** without undue delay of any potential adverse effect on the provision of services, and will also need to communicate to service recipients any measures or remedies to take in response to significant cyber threats.

4. What are the consequences for non-compliance?

The NIS 2 Directive establishes **very strict sanctions** for breaches of its obligations. In contrast to the previous NIS Directive, which merely required Member States to set forth effective, proportionate and dissuasive penalties for non-compliance, the NIS 2 Directive introduces a much stricter regime.

The new duty to implement security measures or to report incidents will be punishable by a fine of **up to EUR 7 million or 1.4% of annual worldwide turnover for important entities and up to EUR 10 million or 2% of turnover for essential entities**.

The NIS 2 Directive also **allows EU Member States to introduce** in their national laws **the imposition of periodic penalty payments** to compel essential or important entities to cease infringement of NIS 2 Directive rules.

Furthermore, the NIS 2 Directive requires Member States to introduce rules allowing the competent regulatory authorities to impose **supervisory or enforcement measures**, such as, inter alia, **a temporary ban on the exercise of management functions or a temporary suspension of the certification or authorisation of services in case of essential entities**.

In many cases, cyber incidents involve personal data breaches. **Where non-compliance with the NIS 2 Directive may also involve a personal data breach, joint fines are not imposed under both the NIS 2 Directive and GDPR** if the breach arises from the same incident.

Key points

Entities are presently advised to do the following:

- ✓ Check whether they may fall under the expanded scope of the NIS 2 Directive
- ✓ Follow cybersecurity-related national legislative developments in their given EU Member State
- ✓ Carefully read any bulletins or notifications issued by local national cybersecurity authorities. [3]

The NIS 2 Directive arguably represents an excellent opportunity for businesses to assess their current processes and to implement policies, procedures, and training programmes to comply with all legal obligations as well as to bolster cybersecurity preparedness.

In case of any questions with respect to the above, our specialists are standing by to offer guidance and counsel.

Petr Bratský
Managing Associate

petr.bratsky@kinstellar.com

Vít Kopečný
Junior Associate

vit.kopecny@kinstellar.com

3. For example, in the Czech Republic, the NCISO has already implemented an NIS 2 Directive public awareness campaign, offering the opportunity to learn about the directive through a dedicated microsite available at nis2.nukib.cz.

Emerging Europe and Central Asia's Leading Independent Law Firm

With offices in 11 jurisdictions and over 350 local and international lawyers, we deliver consistent, joined-up legal advice and assistance across diverse regional markets – together with the know-how and experience to champion your interests while minimising exposure to risk.

ALMATY | KAZAKHSTAN
ASTANA | KAZAKHSTAN
BELGRADE | SERBIA
BRATISLAVA | SLOVAKIA
BUCHAREST | ROMANIA
BUDAPEST | HUNGARY
ISTANBUL | TURKEY
KYIV | UKRAINE
PRAGUE | CZECH REPUBLIC
SOFIA | BULGARIA
TASHKENT | UZBEKISTAN
ZAGREB | CROATIA

KINSTELLAR