UPKEEPER
Work less. Manage more.

How to prepare your organization for the NIS Directive

A 3 MIN CRASH COURSE IN **NIS** FROM UPKEEPER.
DOWNLOAD, SAVE AND SHARE WITH YOUR PEERS.

1. What is NIS?

NIS stands for “Network and Information Security”, and is an EU directive coming to effect in 2018 .

In brief, NIS aims to increase the network and information security for crucial societal and digital services within the EU. Since NIS is a directive (unlike GDPR which is a regulation), it needs to be translated into law in each EU member country before it takes effect. Therefore, the exact date for when NIS will be implemented in the different member countries varies.

2. What are the basic principles of NIS?

Suppliers of crucial societal and digital services shall take measures to increase the reliability and security of networks and information systems.

Cybersecurity incidents shall be reported to respective country's NCAs (National Competent Authorities) and CSIRTs (Computer Security Incident Response Teams), and knowledge and experience shared between EU member states in order to increase cooperation around IT security within the EU.

Those who do not comply with the NIS directive will risk steep fines.

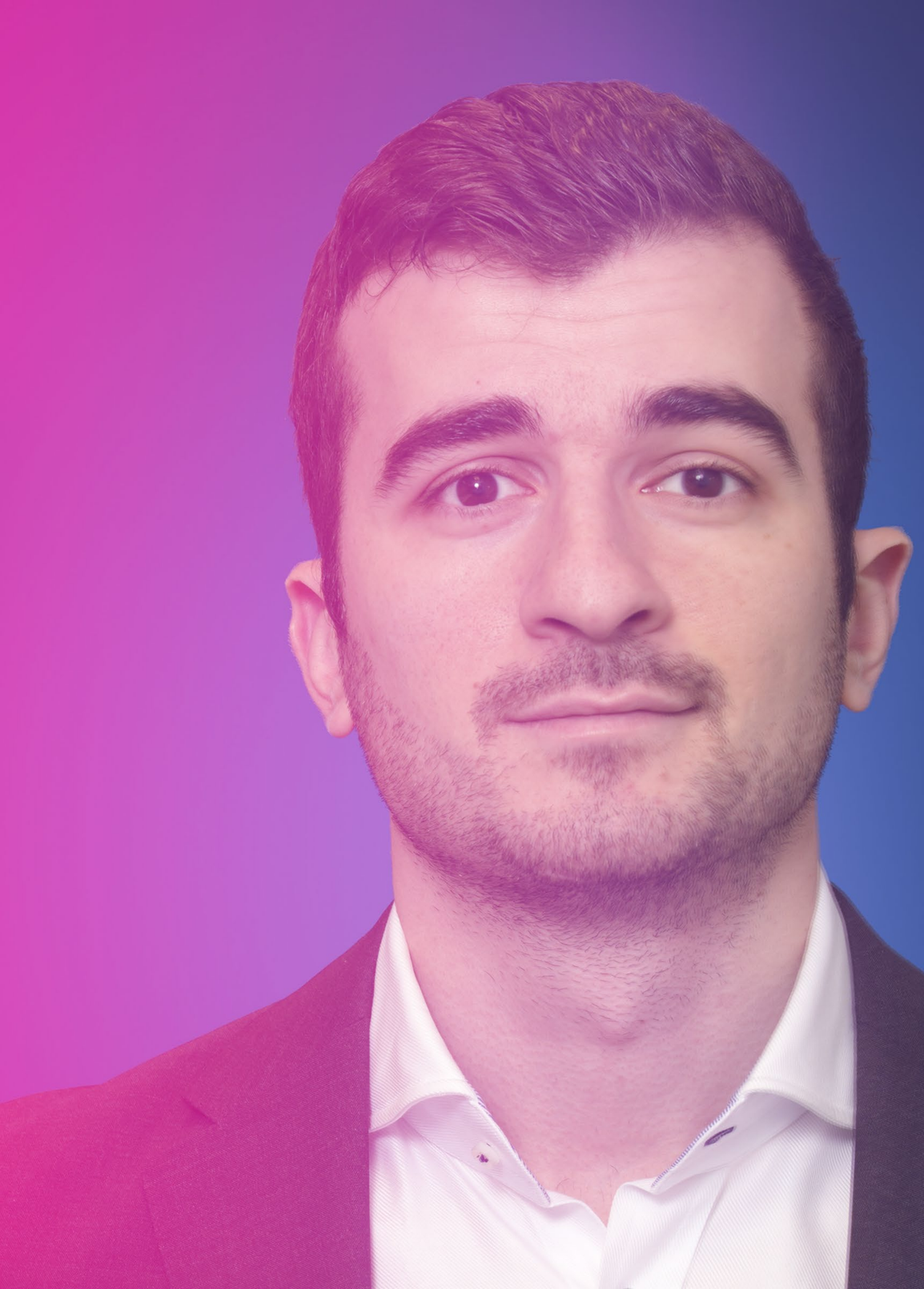
3. Who are affected by NIS?

NIS concerns public and private functions in seven sectors:

- Energy
- Transportation
- Banking
- The infrastructure of the financial market
- Healthcare
- Drinking water supply and distribution
- Digital infrastructure

PLEASE NOTE! Subcontractors and/or associated activities are also affected.

UPKEEPER
Work less. Manage more.



The availability and security of network and information systems are fundamental to economic and social activities today.

Visar Lapashtica, Information Security Specialist at KPMG.

UPKEEPER
Work less. Manage more.

4. What does NIS entail for companies and authorities?

Everybody who operates within one of the seven affected sectors must:

- report all IT-related incidents to respective country's NCAs (National Competent Authorities) and CSIRTs (Computer Security Incident Response Teams)
- work methodically in a structured way with IT security in order to maintain a high level of security in both IT systems and in physical facilities

As a guideline for how IT security work should be conducted, the internationally accepted ISO27000 standard can be used.

5. What can you and your organization do to prepare yourselves?

In order to report IT incidents, the first step is to be able to discover them. Therefore, continuous monitoring of mission-critical networks and their traffic is required.

Structured IT security work means, among other things:

- routines are in place for backup, disaster recovery, and incident management
- the digital assets in the network are regularly inventoried and classified according to security and threat level
- you have a systematic and automated approach to managing your company's computers, phones, and other devices.

UPKEEPER
Work less. Manage more.

To be able to quickly block and wipe lost or stolen devices in order to prevent critical data falling into the wrong hands is crucial to structured information security work.

Visar Lapashtica, Information Security Specialist at KPMG.

UPKEEPER

Work less. Manage more.

Learn more about how you can deploy and maintain all ofyour devices, keeping them secure and updated in a blink of an eye? Head on to our website www.upkeeper.se