NSI2 FINES: GET AN OVERVIEW OF THE POTENTIAL PENALTIES FOR NSI2 NON-COMPLIANCE

What is NIS2?

NIS2 builds on the requirements of the original directive; it still aims to protect critical infrastructure and organizations within the EU from cyber threats and achieve a high level of common security across the EU.

To achieve this goal, NIS2 requires member states to take a number of additional measures, including:

- Establishing an incident response plan that coordinates with other member state plans.
- Establishing a national Computer Emergency Response Team.
- Strengthening cooperation between public and private sector entities.
- Improving information sharing between member states.

By working with member states to help them improve their defenses against cyberattacks, and by providing support and guidance to businesses and individuals, the EU is making sure that its citizens are protected from the growing risk of online threats.

Consequences of NIS2 Non-Adherence

The NIS2 Directive outlines clear consequences for breaches, encompassing:

- Remedies that don't involve money
- Financial penalties
- Legal repercussions

Both essential and important entities may face these consequences for lapses such as not adhering to security protocols or neglecting to report certain incidents.

Non-Financial Consequences

NIS2 empowers national oversight bodies with the ability to levy non-financial penalties, which include:

- Orders to comply
- Direct mandatory instructions
- Mandates for security audits
- Alerts to an entity's clientele about potential risks.

Financial Penalties Overview

The NIS2 directive clearly differentiates the financial penalties for essential versus important entities:

- Essential Entities: Member States are directed to levy fines up to the greater of €10,000,000 or 2% of the global yearly revenue.
- Important Entities: Under NIS2, the fines can reach up to either €7,000,000 or 1.4% of the annual global revenue, with the higher amount being applicable.

NSI2 FINES: GET AN OVERVIEW OF THE POTENTIAL PENALTIES FOR NSI2 NON-COMPLIANCE

CORE ENTITIES (EE)

- This category encompasses both public and private sector organizations operating in fields like transportation, finance, energy, water, aerospace, healthcare, public governance, and digital infrastructure.
- Potential Fine: The higher of €10 million or 2% of their yearly global turnover.

SIGNIFICANT ENTITIES (IE)

- This group covers both public and private enterprises in industries including food production, digital services, chemicals, postal operations, waste management, research, and manufacturing sectors.
- Penalty Threshold: Either €7 million or 1.4% of the total annual global revenue, whichever is greater.

Managerial Liability for Cyber Incidents

To reduce the overwhelming responsibility traditionally placed on IT departments for organizational security and shift the perception of accountability in cybersecurity, NIS2 introduces regulations to hold senior management directly accountable for significant negligence during security breaches.

Under NIS2, if gross negligence is established following a cyber-related incident, Member State authorities can:

- Mandate organizations to publicly disclose compliance breaches.
- Issue public announcements highlighting both the individual(s) and the corporate entity accountable for the breach and outlining its specifics.
- For organizations categorized as essential entities, impose a temporary prohibition on specific individuals from assuming managerial roles if violations recur.

These provisions aim to ensure top-tier management's commitment and accountability in addressing cybersecurity risks.

LOGPOINT

www.logpoint.com