Talentech

NIS2 Directive

Compliance strategy

Last updated: 28 October 2024

Talentech

TALENTECH – THE FUTURE OF HR

Talentech provides a scalable SaaS platform for every step of the talent journey: Attracting candidates, recruitment, onboarding of employees, talent management, employee engagement and eventually off boarding. Our platform supports every stage of the talent pipeline, designed with personalization and flexibility in mind, with the aim of facilitating a seamless talent journey, from start to finish, in one central platform.

Talentech is committed to provide industry leading solutions with information security as our main priority. Talentech considers information and personal data as key assets, which we safeguard for ourselves and on our customers' behalf.

THE NIS2 DIRECTIVE

The NIS2 Directive (Network and Information Security Directive 2) is an updated European Union directive aimed at improving cybersecurity resilience across the EU. It builds on the original NIS Directive from 2016, but introduces stricter cybersecurity requirements and extends the scope to include more sectors and types of companies. NIS2 is intended to strengthen the cybersecurity practices of "essential" and "important" entities, including sectors like energy, healthcare, digital infrastructure, and transport, as well as public administration.

The goal of NIS2 is to address increasing cyber threats by setting minimum standards for risk management, incident response, supply chain security, and overall resilience.

Compliance timeline

Companies affected by NIS2 must comply with national regulations derived from NIS2 by October 2024. However, some specific measures may have extended deadlines, depending on national guidelines.

Since Talentech operates in all of Europe, we will adhere to the specific national legislations as well as EU guidelines and recommendations.

Talentech

COMPLIANCE STRATEGY

To ensure compliance with NIS2, we have implemented an Information Security Management System that covers the key areas of the directive:

Risk Management

We have implemented a comprehensive risk management framework that aligns with NIS2 requirements, focusing on identifying, assessing, and mitigating risks.

Cybersecurity policies

We have implemented cybersecurity policies addressing risk assessment, network security, data integrity, and incident detection and response. These policies are part of our information security framework, which is currently (October 2024) being ISO27001 certified.

Incident response

We have established an Incident Response Policy to quickly address cybersecurity incidents, including clear procedures for detection, management, and mitigation. According to the policy, we have a reporting mechanism to notify authorities within 24 hours of significant incidents, as required by NIS2.

Supply chain security

We have implemented a framework for assessing and monitoring the cybersecurity practices of our main third-party vendors (our hosting suppliers) and partners to ensure compliance throughout our supply chain. We conduct annual security audits on our hosting suppliers, focusing on critical supply chain risks and dependency management.

Continuous monitoring

We have implemented continuous monitoring of network and information systems to detect, analyze, and respond to threats in real time. We also use threat intelligence tools to stay updated on emerging risks and adjust our security posture as necessary.

Employee training

We have a comprehensive cybersecurity awareness program for employees, including regular training on risk management and incident reporting, through a cyber security partner. The training is mandatory for all employees. We also ensure that all team members understand NIS2 obligations, the importance of security practices, and the reporting process for potential incidents.

Talentech

CONCLUSION

Talentech is well-positioned to meet the requirements of the NIS2 Directive, ensuring enhanced cybersecurity resilience and compliance across our operations.

POLICY IMPLEMENTATION

This strategy has been approved by the management team and implemented in the Talentech organisation.