Browne Jacobson

Government publishes its proposals for expanding the Scope of the Network and Information Systems Regulations 2018

27 January 2023

The Network and Information Systems Regulations 2018 (NIS Regulations) are the main legislative vehicle for promoting the security of networks underpinning the UK's essential and digital services.

In the last quarter of 2022 the European Council formally adopted legislation for a high common level of cybersecurity across the Union, to further improve the incident and response capabilities of both the public and private sector and the EU as a whole. The new directive will be called NIS2 (EU NIS2) and will replace the current NIS directive. Although the EU NIS2 Directive is now in effect, member states have 21 months to incorporate its provisions into their national law.

In the same week of the adoption of EU NIS2 the UK Government confirmed that it will move forward with plans to update the NIS Regulations based on the responses to its consultation launched in January 2022 on the proposals for legislation to improve the UK's cyber resilience. These are currently expected to be implemented and brought into force some time in 2024.

This article provides a summary of the proposed amendments to the NIS Regulations in respect of its extended application to digital service providers and the establishment of a risk-based supervisory regime.

Scope of consultation

The aforementioned proposals were split across two pillars namely:

- Pillar 1 – proposals to amend provisions relating to digital service providers. This pillar included the proposals for expanding the regulation of digital service providers and the supervisory regime.
- Pillar II – proposals to future proof the UK NIS regulations. This pillar included proposals for delegated powers to update and amend the scope of the NIS Regulations and proposals for additional incident reporting duties beyond continuity of service.

Expansion of the scope of regulation to providers of digital managed services

Currently the NIS Regulations apply to operators of essential services and relevant digital service providers.

Generally speaking, operators of essential services are those operating in the electricity, oil, gas, air transport, water transport, rail transport, road transport, healthcare, drinking water supply and distribution and digital infrastructure subsectors.

Relevant digital service providers are anyone who provides an online marketplace, online search engines or a cloud computing service.

The NIS Regulations are to be expanded to apply to the providers of digital managed services and accordingly, the provision of such managed services will be subject to such regulations.

It is currently proposed that the characteristics of digital managed services that will be included are:

- The managed service is provided by one business to another business

- The service is related to the provision of IT services, such as systems, infrastructure, networks and/or security
- The service relies on the use of network and information systems, whether this is the network and information systems of the provider, their customers or third parties
- The service provides regular and ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, IT network and/or the security thereof

The published list of example services which would fall within the scope of a managed service includes:

- IT outsourcing services
- Private WAN managed services
- Private LAN managed services
- Service integration and management (SIAM)
- Application modernisation
- Application management
- Managed security operations centre (SOC)
- Security monitoring (SIEM)
- Incident response
- Threat and vulnerability management

At present the UK Government is not proposing to bring data centres within the remit of the NIS Regulation but this is being kept under review. It does however, point out that some data centres may be captured within the scope of NIS through the use by cloud service providers and similarly through forming part of the network and information systems that support the provision of a managed service or managed security service.

The current intention is that there will be an exemption for small or micro businesses from the NIS Regulations but the Information Commissioner will have the power to designate them as being in scope if the business in question is deemed systematically critical to the UK's critical services or national security.

Proposed supervisory regime of digital service providers

The Government had consulted on proposals to establish a two-tier supervisory regime for those digital services providers falling within the expanded scope of the NIS Regulations. This would be the establishment of a proactive supervisory regime for the most critical digital services and a reactive supervisory regime for the remaining digital services. However, based on consultation feedback it has decided that this could be problematic and that it would therefore consider a more flexible, risk-based approach.

The current thinking is that the supervisory approach will be implemented through non-legislative means with the Information Commissioner being given responsibility for how it will regulate digital services and how it will identify and assess those digital service providers which play the most critical role in supporting the resilience of the UK's essential services.

Implications

Under the amended NIS regulations, a wider range of organisations will be caught by them. Organisations will also need to ascertain to what extent they fall under the UK NIS Regulations, the EU NIS2 regime or both and then determine the measures they need to take to ensure compliance. Measures may include investing in new technologies and security systems or updating processes and procedures for reporting incidents to relevant authorities such as Ofcom, Ofgem, and the Information Commissioner's Office.

The consequences for non-compliance of the UK NIS Regulations includes regulatory sanctions such as fines of up to £17m. However, the ramifications of non-compliance could also result in claims for contractual breach and associated reputational damage.

The future

It is inevitable that as the UK economy becomes increasingly reliant on digital infrastructure and security that it will be subject to more regulation. Accordingly the expansion of the NIS regulations is expected to increase the focus on the importance of protecting network and information systems, encouraging organisations to take a more proactive approach to cybersecurity and prioritise the protection of their systems. This will improve the overall cyber security of critical infrastructure in the UK, helping to protect against potential disruptions to essential services and ensuring that organisations are better equipped to respond to and recover from cyber-attacks.

Contact

Kay Chand

Partner

Kay.Chand@brownejacobson.com

+44 (0)330 045 2498

Related expertise

CleanTech and renewables

Energy and infrastructure

FinTech

HealthTech

InsurTech

Logistics

Technology