BRJ Logo

Government to expand network and information systems regulations

18 April 2023 Selina Hinchliffe

The government has published proposals to expand the scope of the Network and Information Systems Regulations 2018 (NIS Regulations).

The NIS Regulations are the main legislative vehicle for promoting the security of networks underpinning the UK's essential and digital services.

The government has 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:

1. its extended application to digital service providers;
2. the establishment of a risk-based supervisory regime; and
3. the potential implications of these proposals for higher education (HE) and further education (FE) institutions.

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 2 — 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 scope to include service providers

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 digital 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 government is not proposing to bring data centres within the remit of the NIS Regulations, 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.

Proposed supervisory regime of service providers

The government 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 was 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 of the NIS Regulations for HE and FE Institutions

The past few years has seen a rapid move towards digitisation, due in part to the impact of COVID-19. As a result, providers of digital managed services have become an attractive option for HE and FE institutions where there has been an increased reliance upon technology and digital resources.

Through the procurement of digital solutions, HE and FE institutions can continue to support their students and learning providers in a more agile and modern way and in a way that enables continuity of learning through disruption (as we saw in during the pandemic).

This is ever more so the case in a world where the HE/FE sector has seen a phenomenal growth in its international reach as regards student mobility, joint partnership arrangements with overseas institutions and cross-border research and development programmes. Therefore, resilience in the sector’s digital infrastructure and digital solutions is becoming increasingly paramount.

Managing risk in the face of increased cyber security attacks

In this regard, many HE and FE institutions are beginning to rely heavily on digital managed services whilst at the same time we are seeing an increase in cyber security attacks. Whilst outsourcing the provision of digital managed services is seen as a way to better manage this risk due to the perceived expertise and capabilities of the service providers, the risk nevertheless remains.

According to the Cyber Security Breaches Survey which took place in 2022, 62% of HE institutions reported experiencing breaches or attacks at least weekly in the 12 months preceding the survey, with 71% experiencing a negative outcome, such as loss of money or data from a breach.

Consequently, the inclusion of digital managed services within the scope of the NIS Regulations will at least go some way to ensuring that appropriate and proportionate security measures are in put in place by digital managed service providers.

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

Key contacts

Kay Chand

Partner

Kay.Chand@brownejacobson.com

+44 (0)330 045 2498

Related expertise

Criminal compliance and regulatory

Digital and sourcing

Information law