Client Alert | Intellectual Property/Data Privacy

Network and Information Systems Regulations introduce significant new penalties from 10 August

06 August 2018

Author: **Tim Hickman, John Timmons**

The Network and Information Systems Regulations 2018 ("**NIS Regulations**") came into force in the UK on 10 May 2018. For much of the year, attention has been focused on implementation of the General Data Protection Regulation ("**GDPR**"). As a result, the implementation of the NIS Regulations has largely gone unnoticed. However, organisations caught by the NIS Regulations should be familiar with their requirements, as failure to comply can result in significant financial penalties.

What are the NIS Regulations?

The NIS Regulations implement an EU directive, the Network and Information Systems Directive (EU) 2016/148 (**NIS Directive**). The aim of the NIS Directive is to create common standards on network and information security across the EU. The NIS Directive and the UK's NIS Regulations are an attempt by lawmakers to address some of the risks posed to individuals and the wider economy that can arise from security incidents affecting key networks and information systems. The NIS Regulations therefore impose obligations on in-scope organisations to implement certain levels of security and to make notifications in the event of security incidents.

Who is in scope?

The NIS Regulations apply to "operators of essential services" ("**OES**") and "digital service providers" ("**DSP**").

The OES category includes organisations in the following sectors:

- **Energy:** electricity, oil and gas;
- **Transport:** air, water, rail, road;
- **Health:** healthcare providers;
- **Water:** drinking-water supply and distribution; and
- **Digital infrastructure:** domain name system service providers, top level domain name registries and internet exchange point operators.

The NIS Regulations set out minimum threshold criteria for organisations in these sectors to assess whether they are in-scope. The criteria include factors such as: (i) the number of customers being provided with services and (ii) the output of the service provider.

If an organisation within one of the sectors does not meet the threshold criteria, it may still be in-scope if the relevant regulator determines that it should be in-scope. The relevant regulator can make such a determination by considering factors such as: (i) the number of users of the service; (ii) the impact on the economy resulting from a failure of the services; and (iii) the likely consequences for national security if an incident affects the services.

The DSP category includes organisations providing one of the following digital services:

- **Online marketplace;**
- **Online search engine;** and
- **Cloud computing service.**

An organisation providing one or more of these services will be in-scope provided it satisfies the following criteria: (i) it is headquartered in the UK or has nominated a representative established in the UK; and (ii) it is not a "micro" or "small enterprise" (i.e. it has fewer than 50 staff and a turnover of less than €10 million per year).

What are the main obligations imposed by the NIS Regulations?

Some of the key obligations imposed by the NIS Regulations on in-scope organisations include:

- The requirement for an organisation to notify the fact that it is in-scope for the NIS Regulations to the relevant regulator.
- The requirement to implement appropriate and proportionate measures to manage risks posed to network and information systems and to prevent, and minimise the impact of, incidents affecting the security of the network and information systems.
- The requirement to notify the relevant regulator of the occurrence of incidents (including security breaches) which have an impact on the delivery of its services.

Consequences of non-compliance

The NIS Regulations allow for the imposition of significant fines on organisations for failure to comply.

The level of the applicable fine will be determined with reference to the nature of the non-compliance. Fines can reach a maximum of £17 million.

In addition to the power to impose fines, the relevant regulators also have the power to:

- **Conduct inspections:** to assess if the organisation has met its obligations under the NIS Regulations;
- **Serve information notices:** to require an organisation to provide information to enable the regulator to assess the organisation's compliance with the NIS Regulations; and
- **Serve enforcement notices:** which shall set out the steps that the organisation must take to rectify identified failures by the organisation.

Why is this relevant now?

The NIS Regulations are now in force. Organisations subject to the NIS Regulations should be taking steps to comply with their obligations.

The notification deadline for organisations falling within the OES category is **10 August 2018**. This means that all organisations which satisfy the OES criteria, and which are therefore in-scope for the NIS Regulations must notify the relevant regulator of their in-scope, status by this deadline. Organisations falling within the DSP category have until **1 November 2018** to notify the Information Commissioner of their in-scope status. Organizations active in essential services and digital services spaces therefore need to ensure that they have considered whether the NIS Regulations apply to them and, if so, taken steps to implement appropriate compliance measures.

White & Case LLP
5 Old Broad Street
London
EC2N 1DW

T +44 20 7531 1000