European Parliament approves NIS Directive

A common EU approach on cyber security

On 6 July, the European Parliament voted to adopt a new Directive laying down measures aimed at achieving a high common level of security of networks and information systems within the EU (the NIS Directive). The NIS Directive sets out, for the first time, a common EU approach on cyber security and imposes enhanced security requirements and incident notification obligations on banks and other ‘operators of essential services’, together with certain digital service providers.

The NIS Directive was originally proposed as part of the EU’s Cyber Security Strategy, published in February 2013. However, despite numerous high profile cyber breaches across Europe and heightened media attention on the cyber terror threat, political agreement was only reached on the substance of the Directive in December 2015. The European Parliament’s vote represents the final hurdle in the European legislative process and the culmination of years of negotiations.

Some of the key aspects of the agreed Directive include:

- security and notification requirements for businesses in certain ‘critical’ sectors - it adopts two regimes, one for operators of essential services in sectors such as energy, transport, banking and health, and another for certain digital service providers (which is intended to be less stringent);

- obligations on EU Member States to adopt an NIS strategy and designate national competent authorities, a single point of contact and a Computer Security Incident Response Team (CSIRT) with tasks related to the security of networks and information systems; and

- establishing a European framework, with a cooperation group and CSIRTs network, to support and facilitate strategic cooperation on network and information security across Europe.

Whilst the Directive will have its greatest impact on those organisations directly covered by the regime (i.e. certain digital service providers and those identified by Member States as being operators of essential services within their territories), we anticipate that the security requirements contained in the NIS Directive may begin to set the bar for all large organisations operating within Europe. Also, similar security provisions (around having appropriate technical and organisational measures in place) already apply where personal data is involved under the EU’s Data Protection regime.

For more detail on the contents of the NIS Directive and information on what the Directive will mean for your business (including some suggested ‘next steps’ to enable you to best prepare), please see our briefing “New cyber security law: what does the NIS Directive mean for your business?” published on 10 February 2016.

Next steps

The approved draft of the NIS Directive will soon be published in the EU’s Official Journal, and will enter into force on the twentieth day after its publication. EU Member States will then have 21 months to transpose the Directive into their national laws, and six additional months to identify the operators of essential services within their territories. It is only then that the obligations contained in the NIS Directive will apply to such organisations established in those EU Member States.

Of course, whether or not such obligations will bind organisations established in the UK going forwards is uncertain. It will depend on many factors, including:
• the outcome of any EU exit negotiations and the model of engagement with the remainder of the EU that the UK adopts (as to whether or not European laws will continue to bind the UK);

• whether the UK decides to transpose the NIS Directive (or something very similar) into national law in any event (especially as the UK is still likely to be a Member State of the EU when the 21 month transposition period expires); and

• whether the extra-territorial reach of the NIS Directive will extend to many UK organisations: the Directive will continue to apply to (i) any UK operators of essential services which are also considered to be essential in any other Member States, as long as those organisations provide services into those Member States through non-prescriptive ‘stable arrangements’, and (ii) digital service providers that are established in the UK but continue to offer their services into the remainder of the EU; these organisations shall have to designate a representative to be established in a Member State where those services are offered.

In any event, our advice to clients at this stage is to prepare as though the Directive (or something similar) will still apply. This mitigates uncertainty around the future implementation of the Directive (and the risk of being unprepared) and also reflects the fact that having sufficient cyber security provisions in place (as required by the Directive) is a business necessity in today’s environment. We also expect that future UK Governments will still want to be seen to be cooperating on matters such as information security with their European counterparts; a message reinforced by Baroness Neville-Rolfe, Minister for Data Protection, at her speech on 4 July 2016 at the Privacy Laws & Business conference on data protection.

As the importance of effective cyber security continues to increase, it is encouraging to see that governments across Europe are working together to put measures in place to ensure that businesses operating in critical sectors, and the Member States in which they are established, are well protected and prepared for future cyber threats.

Natalie Donovan, Professional Support Lawyer
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com

Rob Sumroy, Partner
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Nikhil Shah, Associate
T +44 (0)20 7090 3631
E nikhil.shah@slaughterandmay.com

© Slaughter and May 2016
This material is for general information only and is not intended to provide legal advice. For further information, please speak to your usual Slaughter and May contact.

July 2016