European cyber security laws - a step closer

On 7th December the European Parliament and the Luxembourg Presidency of the EU Council of Ministers reached informal agreement on the much awaited Network and Information Security (NIS) Directive. Amongst other things, the Directive will set out cyber security obligations for operators of essential services (including banks, energy and water companies and transport operators) and some digital service providers.

Recent high profile cyber breaches like TalkTalk, and media attention on the terror cyber threat in the wake of the Paris attacks have highlighted the need for Europe to implement adequate cyber protections. However, negotiations on the NIS Directive, proposed under the 2013 EU Cyber Strategy, were taking longer than expected. A number of sticking points had emerged, including which organisations should be covered by the regime. The treatment of digital service providers in particular proved a contentious issue in discussions (our previous article The NIS Directive: Genesis, Status and Key Aspects provides more detail on the background of these discussions).

It was hoped that trilogue negotiations on 17th November would resolve the outstanding points. However, informal agreement was only reached this week, following which the EU Council, Parliament and Commission all swiftly published press releases acknowledging and welcoming the deal. While an agreed text is not yet available, these press reports do provide some insight:

1. Security measures and mandatory breach notification

- Operators of essential services will be required to take appropriate security measures and to notify breaches (serious incidents) to the relevant national authority. The Directive lists a number of critical sectors including: energy; transport; banking; financial market infrastructures; health; and water. Member states will identify the operators providing essential services within these sectors based on clear criteria laid down in the Directive. For example, is the service critical for society and the economy and does it depend on network and information systems?

- Some digital services (such as e-commerce platforms, search engines and cloud services) will also be covered. These providers will have to ensure the safety of their infrastructure and report on major incidents, although the requirements and supervision will not be as stringent for digital service providers as those in the critical sectors listed above. There will also be exemptions for small digital companies.

2. Increased cooperation on cyber issues

- National and EU level frameworks will encourage cooperation between member states on cyber issues. Member states must designate a national competent authority to implement and enforce the Directive, and Computer Security Incident Response Teams (CSIRTs) to deal with incidents and risks. They must also adopt a strategy to deal with cyber issues.

- The Directive will create a strategic cooperation group between member states to facilitate co-operation and exchange information and best practice. It will also create a CSIRTs Network to aid effective cooperation on specific incidents and share information about risks.

3. Formal approval is still needed

- This political agreement must be followed by formal approval. The Council has already stated that the deal needs to confirmed by member states, and it will 'present the agreed text for approval by member states' ambassadors at the Permanent Representatives Committee (Coreper) on 18 December'.[1] Formal adoption by both the Council and Parliament is required to conclude the procedure, and BBC reports suggest that the European Parliament vote is expected to take place in Spring 2016.

- Once it has been formally agreed, and officially enters into force, member states will have 21 months to implement it into national law and a further 6 months to identify operators of essential services.

Comment

The deal has been heralded by the European institutions as "a milestone"[2] and "a major step in improving the resilience of our network and information systems in Europe"[3]. Given the growing cyber threat, it is exciting that political (although not formal) agreement has been reached at last. That said, we await the 'agreed' text to see exactly how the regime will work, and it will still be some time yet before legal obligations will bite on organisations that fall within that regime. However, and perhaps unsurprisingly, we are advising organisations to put their cyber house in order now, rather than wait for the NIS Directive to become law.

This article was written by Rob Sumroy (Partner) and Natalie Donovan (PSL) from Slaughter and May's Technology team. Please contact Rob, Natalie or your usual Slaughter and May contact if you would like more information on cyber security issues.

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

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

[1] Council's press release

[2] Andreas Schwab (Parliament's Rapporteur) – quoted in the European Parliament's press release

[3] Günther H. Oettinger (Commissioner for the Digital Economy and Society in the European Commission's press release

December 2015