Client Alert | Intellectual Property / Technology

EU-wide cybersecurity rules nearing final agreement

December 2015

Authors: Philip Trillmich, Tim Hickman, Matthias Goetz

The EU is close to finalising the Cybersecurity Directive, which will place significant security and incident reporting obligations on operators of essential services and digital service providers.

On 7 December 2015, the EU's legislative institutions agreed a compromise on the text of a new EU Directive designed to create common standards on network and information security across the EU (the "NIS Directive", also known as the "Cybersecurity Directive"). This development follows a prolonged period of negotiations, and marks a significant step towards the completion of the Directive.

The Directive requires EU Member States to implement a common set of cybersecurity standards. Businesses that are subject to these standards will have to implement certain minimum security measures and to report major security breaches. If they fail to do so, they may face enforcement action.

The final text of the Directive is not yet available. However, official press releases issued by the European Commission, the Council of the EU, and the European Parliament provide a number of important clarifications on the requirements that the Directive will impose. A compromise text is expected before the end of 2015, and we will circulate a further Client Alert, with more in-depth analysis, once that text is available.

Which businesses are affected?

The three official press releases indicate that the scope of the Directive is very broad, and will apply to two categories of businesses:

"Operators of Essential Services"

This category includes businesses in the following sectors:

- Energy: electricity, oil and gas;
- Transport: air, rail, water and road;
- Banking: credit institutions;
- Financial market infrastructures: trading venues, central counterparties;
- Health: healthcare providers;
- Water: drinking water supply and distribution; and
- Digital infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers and top level domain name registries.

Importantly, each EU Member State will be responsible for identifying businesses that are "*Operators of Essential Services*", based on criteria set out in the Directive. The criteria include: (i) whether the relevant service is critical for society and the economy of that Member State; (ii) whether the service depends on network and information systems; and (iii) whether a cybersecurity incident could have significant disruptive effects on the provision of the relevant service, or on public safety.

This appears to leave open the possibility that services provided by a business may be more critical in one Member State than in another, and therefore that a business may find that its services are subject to the requirements of the Directive in some Member States but not others. As a result, such a business may face inconsistent compliance obligations across the EU.

"Digital Service Providers"

This category includes businesses in the following sectors:

- Online marketplaces (including those that allow other businesses to set up 'shops' within the marketplace in order to make their products and services available online);
- Cloud computing services; and
- Search engines.

It appears that other categories of online service providers that had been included in earlier drafts of the Directive (e.g., social network providers) will be removed from the scope of the Directive. The Council and Parliament press releases also indicate that small digital businesses will benefit from an exemption, although no detail is provided on the relevant thresholds.

Unlike Operators of Essential Services, Member States will not designate particular businesses as Digital Service Providers. Instead, the same rules will apply to all entities falling within the definition of 'Digital Service Providers' set out in the Directive, throughout the EU.

What does the Cybersecurity Directive require from affected businesses?

It appears that the Directive will place more onerous obligations on Operators of Essential Services than on Digital Service Providers:

- Operators of Essential Services will be required to ensure that the structures and systems that they use to provide critical services are sufficiently robust to resist cyber-attacks. According to the Council's press release, this "reflects the degree of risk that any disruption to their services may pose to society and the economy."
- Digital Service Providers, on the other hand, will only be required to ensure the safety of their own infrastructure. It is inferred from the press releases that Digital Service Providers will be held to lower technical standards than Operators of Essential Services, although it is not clear how this will be applied in practice.
- Both Operators of Essential Services and Digital Service Providers will be required to report major security breaches to the relevant national regulators. There is, as yet, no guidance on the definition of a 'major' breach.

When will the Cybersecurity Directive come into force?

The next step in the EU legislative process is for the Parliament and the Council to formally approve and adopt the Directive, after which it will be published in the EU Official Journal and will officially enter into force. The Directive will then need to be implemented into the national laws of each of the 28 EU Member States within a maximum of 21 months before its provisions become binding law. Members States will have a further 6 months to identify the relevant Operators of Essential Services.

What will the impact of the Cybersecurity Directive on affected businesses be?

The impact of the Directive on affected businesses will largely depend on the enforcement powers granted to national authorities, and the approach taken by those authorities in exercising those powers. The relevant national authorities and the European Commission are expected to issue further guidance, once the Directive is finalised. Affected Businesses should also bear in mind that certain requirements under the Directive overlap with the existing requirements under EU data protection law, which already imposes information security requirements and data breach reporting obligations, in relation to systems that are used to process personal data. At this stage, affected businesses should keep their cybersecurity systems and controls under review, and undertake a more detailed consideration of their obligations once the Directive is finalised.

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

T +44 20 7532 1000