

## CLIENT ALERT

### EU Legislators Agree on First EU-Wide Legislation on Cybersecurity

Dec.09.2015

On December 7, the European Parliament and the European Council reached a political agreement paving the way for the first European Union-wide legislation on cybersecurity. The new legislation, the *Directive on Network and Information Security* (known as the "NIS-Directive") was originally proposed by the European Commission in 2013 and aims at ensuring common standards of network and information security in the European Union.

A final text of the political agreement has not yet been released. Statements from the relevant authorities, however, confirm that, under the new rules, businesses operating "essential services" will have to take appropriate security measures and will also be obliged to report data incidents to the applicable national authorities. The European Union Member States will be responsible for identifying the businesses concerned in the following "essential services" sectors:

- Energy: electricity, oil, gas;
- Transport: air, rail, water, road;
- Banking and financial market infrastructures: credit institutions, trading venues, central counterparties;
- Health and living: health care providers, drinking water supply and distribution; and
- Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registries.

Notwithstanding serious lobbying from major internet companies, the Directive will also impose security measures and notification requirements on important digital businesses, referred to as "digital service providers" (DSPs), which include online marketplaces, cloud computing services, and search engines. Their obligations are said to be less stringent than those imposed on the essential services operators.

The relevant authorities will be empowered to impose fines if companies fail to comply.

The political agreement must still be formally approved by the European Parliament and the European Council. After publication in the European Official Journal, European Union Member States will have 21 months to implement and transpose the Directive into national law and an additional six months to identify the "operators of essential services" in accordance with the criteria set forth in the Directive.

In addition, European Union Member States will be required to adopt a national NIS strategy defining objectives and appropriate measures in relation to cybersecurity. They will also be required to designate a competent authority for the implementation and enforcement of the new rules, as well as Computer Security Incident Response Teams (CSIRTs) that will be responsible for investigating data-related incidents.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

**Jeffrey L. Poston**

Partner – Washington, D.C.  
Phone: +1 202.624.2775  
Email: [jposton@crowell.com](mailto:jposton@crowell.com)

**Jeane A. Thomas, CIPP/E**

Partner – Washington, D.C., Brussels  
Phone: +1 202.624.2877, +32.2.282.4082  
Email: [jthomas@crowell.com](mailto:jthomas@crowell.com)

**Emmanuel Plasschaert**

Partner – Brussels  
Phone: +32.2.282.4084  
Email: [eplasschaert@crowell.com](mailto:eplasschaert@crowell.com)

**Frederik Van Remoortel**

Partner – Brussels  
Phone: +32.2.282.1844  
Email: [fvanremoortel@crowell.com](mailto:fvanremoortel@crowell.com)