Group Briefing
March 2016

Agreed Text of the Directive on Network and Information Security

KEY CONTACT

For further information please speak to your usual Arthur Cox contact or:

PEARSE RYAN
PARTNER
+353 1 618 0518
pearse.ryan@arthurcox.com

SARAH MCDERMOTT
TRAINEE
+353 1 618 0000
sarah.k.mcdermott@arthurcox.com

The Network and Information Security Directive was agreed by the European Council and the Parliament on 7 December 2015, and the agreed final compromise text was approved by the Member States on 18 December 2015.

This update on the Directive follows on from an earlier article, which identified the Directive as the European Union's first comprehensive attempt to establish a set of minimum cybersecurity standards that would apply across the Union.[1]

Speaking after the agreement on 7 December 2015, the European Commission's Vice President Andrus Ansip remarked "*The Internet knows no border - a problem in one country can have a knock-on effect in the rest of Europe. This is why we need EU-wide cybersecurity solutions. This agreement is an important step in this direction.*"

MOVING THE DIRECTIVE TOWARDS AN AGREED TEXT

The progress of the Directive has been addressed at several meetings of the Transport Telecommunications and Energy Council configuration ("TTE Council") over the last number of years, and has also been the subject of a number of progress reports submitted to the TTE Council.

Once the Parliament approved the Directive in March 2014, as discussed in greater detail in the article mentioned above, informal trilogues were utilised to allow the Council and the Parliament work through the main differences between their positions, which facilitated agreement in principle for much of the text of the Directive.

The most significant change which has been adopted since we last reviewed the Directive is the extension of the entities to which the Directive applies. The draft Directive adopted by the Parliament had excluded "*key internet enablers*" such as e-commerce platforms, internet payment gateways and social networks from the remit of the Directive. However, certain "*digital service providers*" ("DSPs") have been reinstated to the agreed text of the Directive, with the effect that online marketplaces, online search engines and cloud computing services will now be subject to similar requirements as "*operators of essential services*" ("OESs").

The co-legislators agreed to provide for uniform rules on certain aspects

1. See Society for Computers & Law website - http://www.scl.org/site.aspx?i=ed39127

in relation to the DSPs. In particular, it was agreed Member States should not impose stricter security and notification requirements on those providers and the European Commission will have the power to further specify certain elements in implementing acts.

SECURITY OF NETWORK AND INFORMATION SYSTEMS

Chapter IV of the Directive provides for mandatory security breach and incident notification requirements. While the requirements for DSPs and OESs under Chapter IV are similar, they are not identical. OEPs will be required to provide evidence of the effective implementation of security policies, such as the results of a security audit, while DSPs will not have to comply with this requirement. DSPs must designate a representative in the European Union where the DSP is not established in the Union, but offers relevant services within the Union. OEPs are not subject to this requirement.

The Directive also provides that certain requirements in respect of DSPs do not apply to enterprises with less than 50 employees and whose annual turnover and/or annual balance sheet does not exceed EUR10 million. There is no equivalent de minimus threshold in respect of OESs.

The national competent authority ("NCA") will have the power to require both OESs and DSPs to provide the information needed to assess the security of their networks and information systems, including documented security policies.

NOTIFICATION OF A SECURITY INCIDENT

OESs are required to notify the NCA of incidents which have a '*significant impact*' on the continuity of the essential services they provide. In order to determine the significance of the impact of an incident, consideration will be given to the number of users affected by the disruption of the essential service, the duration of the incident, and the geographical spread with regard to the area affected by the incident.

DPSs must notify the NCA of any incident having a '*substantial impact*' on the provision of an online marketplace, online search engine or cloud computing services. In determining the impact of an incident, the same factors will be considered, and additionally the extent of the disruption of the functioning of the service, and the extent of the impact on economic and societal activities will also be considered.[2]

Our previous article discussed the key area of potential penalties levied by the NCAs. This sharp point of the Directive stick is of concern to OESs and DSPs. The Directive sets out that each Member State shall lay down rules on penalties applicable to infringements of the provisions of the Directive, and such penalties shall be '*effective, proportionate, and dissuasive*'. The potential levying of penalties is arguably the most important risk management provision of the Directive, for its OES and DSP audience.

VOLUNTARY NOTIFICATIONS

The Directive retains the option for voluntary notification, which provides for entities which have not been identified as OESs or DSPs to notify incidents having significant impact on the continuity of the services they provide on a voluntary basis. Such a voluntary notification will not have the effect of imposing on the notifying entity the obligations under the Directive.

Member States will process the mandatory notifications in priority to such voluntary notifications, and shall only process the voluntary notifications where such processing does not constitute a disproportionate or undue burden on the Member State concerned.

CO-OPERATION BETWEEN COMPETENT AUTHORITIES

It is notable that a number of the provisions relating to co-operation between the Member State NCAs have been diluted in, and in some cases excluded from, the agreed text of the Directive.

The draft of the Directive approved by the Parliament mandated '*early warnings*' on risks which, or which may, grow rapidly in scale, exceed national response capacity, or affect more than one Member state, and required a coordinated response from the competent authorities. This requirement has been replaced with tasking the Computer Security Incident Response Teams with discussing, exploring and identifying further forms of operational cooperation, including in relation to early warnings and principles and modalities for coordination.

It also appears the provisions relating to the exchange of sensitive and confidential information within the cooperation network to take place through a secure infrastructure have been removed.

WHAT'S NEXT?

The text of the Directive must now be formally approved by the Council and the Parliament. It is anticipated this will take place in the coming months. The text of the Directive will then be published in the Official Journal of the European Union, and shall enter into force 20 days from the date of its publication. The deadline for transposition in the Member States will be 21 months from the coming into force of the Directive. Member States will then have a further 6 months to identify OESs with an establishment in their territory.

2. There is an interesting argument to be made, for example, whether copying without deleting data has a substantively negative impact.

arthurcox.com

Dublin
+353 1 618 0000
dublin@arthurcox.com

Belfast
+44 28 9023 0007
belfast@arthurcox.com

London
+44 207 832 0200
london@arthurcox.com

New York
+1 212 782 3294
newyork@arthurcox.com

Silicon Valley
+1 650 943 2330
siliconvalley@arthurcox.com