GOWLING WLG

AN UPDATE ON THE IMPLEMENTATION OF THE CYBER SECURITY DIRECTIVE

12 March 2018

Articles

In August 2017, the Department for Digital, Cultural, Media and Sport issued a public consultation on its plans to implement the Network and Information Systems Directive (the Directive) - also known as the Cyber Security Directive - into UK legislation by 9 May 2018. We highlighted some of the key proposals in Consultation on the Implementation of the Cyber Security Directive. The Government's response has now been published.

Over 350 responses were received to the consultation showing broad support for the Government's approach but also highlighting concerns which the Government has tried to address as set out in its response to public consultation: Security of network and Information Systems, January 2018 (the Response). Some areas in which there have been key changes to the original proposals are highlighted below.

OPERATORS OF ESSENTIAL SERVICES (OES) AND DIGITAL SERVICE PROVIDERS (DSP)

The thresholds for identifying OES have been refined so that it is clearer for companies whether they are in scope of the Directive. Revised thresholds are set out at Annex 1 to the Response. The Government has refrained from 'gold-plating' or widening the scope of the Directive to include additional sectors such as government, chemicals and food and agriculture. It will however revisit this when it undertakes a post-implementation review three years after the legislation comes into effect.

The definition of DSP has also been refined although the Government recognises that the definition continues to be a challenge.

COMPETENT AUTHORITY APPROACH

The Government has decided to maintain its approach for sector/subsector based competent authorities which will monitor and oversee the implementation of the Directive in their respective sectors. An updated list is provided at Annex 2 of the Response. The distinction between their role and that of the National Cyber Security Centre (NCSC) has been clarified. The NCSC will provide expert advice, guidance, assessment tools and incident response capability to cyber-attacks but will not act as the regulator.

Extra clarification and guidance will be published on the role of competent authorities and how they will interact with each other and across other regimes such as the General Data Protection Regulations (GDPR) before May 2018. However, the Response sets out an indicative list of what a competent authority's powers will include and the factors to be taken into account in deciding what action to take. The Government is live to the possibility of divergence of approaches using this multi competent authority approach but it intends that common guidance will be produced by the NCSC and competent authorities will be encouraged to cooperate with each other.

Where an OES falls under the jurisdiction of more than one competent authority, the intention is that the competent authorities will cooperate with each other and not make conflicting demands. However, each will be responsible for their respective jurisdiction and the OES will have to engage with both. The Government also acknowledges the unavoidable risk of OES infringing more than one piece of legislation at a time. If this occurs, competent authorities should discuss the best approach with other regulators but will be free to undertake their own response to any infringement so long as it is appropriate and proportionate.

SECURITY REQUIREMENTS AND HIGH LEVEL PRINCIPLES

Updated high level security principles appear in Appendix 3 to the Response. These are 14 high level, overarching principles to assist OES determine the most appropriate security measures within their organisational context in discussion with the relevant competent authority. The updated principles place a greater emphasis on ensuring all levels of an organisation understand the risk of cyber security and the measures the OES has put in place.

The Government has also confirmed OES and DSPs are responsible for ensuring their suppliers have appropriate measures in place to ensure they are compliant. The Directive will not apply directly to suppliers and competent authorities will not enforce its requirements on such suppliers.

The NCSC has published new supplementary guidance (including on ensuring the security of the supply chain) and will also publish a NIS Cyber Assessment Framework (CAF) in Spring 2018 to provide further clarity. It is expected that determinations on acceptable levels of cyber security will be made by competent authorities through use of the CAF.

INCIDENT REPORTING

The Government has accepted that clearer guidance on the threshold for reportable incidents is required. It will be the responsibility of the designated competent authority in each sector or sub-sector to calculate and publish - before May 2018 - the incident reporting thresholds that will apply as they are best placed to consider the different cyber security challenges and what is a 'significant impact' in the particular sector, sub-sector or even micro-sector. The Government has set out minimum parameters to be used being:

- the number of users affected by the disruption of the essential service;
- the likely or actual duration of the incident; and
- the geographical area affected by the incident.

All breaches or incidents meeting the parameters set by the competent authority should be reported to and logged by the competent authority which will then decide if any follow up investigation is required.

The timescale previously proposed of no later than 72 hours to report an incident is retained to align with the GDPR. Voluntary reporting can be made to either a competent authority or the NCSC.

PENALTY REGIME

The Government's originally proposed penalty regime will be amended. The four percent of global turnover element will be removed and the two penalty bands initially proposed will be merged into a single band. This single band will cover all contraventions such as failure to cooperate with the competent authority, failure to report a reportable incident, failure to implement appropriate and proportionate security measures. The maximum financial penalty will be £17 million which figure should only be reserved for the most severe cases.

Fines should be appropriate and will vary across the sectors with the relevant competent authority deciding the level of fine which must be reasonable, appropriate and proportionate to the particular contravention. Mitigating factors, including steps taken to comply with the legislation and actions taken to remedy any consequences must be considered when determining the level of penalty. Fines should be considered only as a last resort.

The Government understands that potential 'doubly jeopardy', through the doubling up of fines, remains a possibility where an incident contravenes the Directive and the GDPR or other sectoral or national legislation such as safety legislation. Although OES and DSPs should not be tried for the same offence twice, there may be reasons for them to be penalised under different regimes for the same event because the penalties might relate to different aspects of the wrongdoing and different impacts. However, as mentioned above, competent authorities should work with other relevant regulators in the event of different regimes applying to determine the appropriate approach to take.

COMMENT

The Government recognises that the process of improving network security will take a number of years and it anticipates a collaborative approach by stakeholders. It is intended that competent authorities will take a reasonable and proportionate approach to enforcement and that OES will be given time to implement the required security measures. The main priority for the competent authorities in the first year will be information gathering within their sectors. OES will be expected to have begun analysing their systems and existing security measures in order to understand where further work is required and to develop plans in order to reach the appropriate levels of security requirements.

Related Energy, Aviation, Aerospace & Defence, Health & Care, Infrastructure, Natural Resources, Tech, Digital Risk, General Data Protection Regulation, ThinkHouse

AUTHOR(S)

Helen Davenport

Director

Birmingham
T: +44 (0)121 393 0174
helen.davenport@gowlingwlg.com

View profile

Jane Bates

PSL Principal Associate

Birmingham
T: +44 (0)121 393 0039
jane.bates@gowlingwlg.com

View profile

RELATED INSIGHTS & RESOURCES

Ethiopia introduces a Public Private Partnership Law

Jonathan Brufal

Brand owners beware: how GDPR will make online enforcement a lot tougher

George Sevier

UK ratifies Hague Agreement on industrial designs

John Coldham

Articles 27 Mar 2018

Articles 21 Mar 2018

Articles 14 Mar 2018

View all