UK Government Response to Cybersecurity/NIS Digital Service Providers Consultation

Date : September 26, 2018

Introduction & Background

The UK government recently published its response to digital service providers in the context of its cybersecurity consultation, which this brief article is about.

This May 2018 the UK adopted the EU Cybersecurity Directive into UK law, called the Network and Information Systems Regulations 2018 (the NIS regime), which we wrote about here http://www.corderycompliance.com/uk-implements-eu-cybersecurity-rules-2/ (the rules can be found here https://www.legislation.gov.uk/uksi/2018/506/made).

Amongst other things these rules aim to ensure that "Operators of essential services" (OESs) and "relevant digital services providers" (RDSPs) in the EU have appropriate and proportionate cyber security measures in place and report cyber security incidents to a regulator.

An organization will be considered to be an RDSP if it has its head office or "nominated representative" in the UK (and is not a micro or small enterprise). An RDSP must notify itself to and register with its regulator, which in the UK is the UK data protection regulator, the Information Commissioner's Office ("the ICO"), by 1 November 2018; for further information about OES regulatory registration requirements please see the article referred to above.

In April 2018 the UK government opened a targeted consultation (consisting of five questions) on how this new cybersecurity regime would apply to RDSPs (called DSPs in the consultation context) – the government's response to this consultation was recently published and is summarized below (the response can be found here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737327/NIS_DSP_Consultation_Response__Final___1_.pdf).

Consultation Response

In sum, the consultation looked at how the NIS regime will apply to DSPs, focusing in particular on: the identification of DSPs; security measures; and, further guidance.

The responses (of which there were twelve in total) expressed uncertainty about who exactly is in scope, particularly as regards cloud service providers, and that greater clarification is needed concerning cost recovery by the ICO. Therefore the UK government proposes using the outcome of the consultation to assist the ICO in clarifying:

- how DSPs can more easily identify if they fall within the scope of the NIS regime;
- how cloud services can be defined;
- and, how the ICO's cost recovery process will work.

The scope issue is a key concern for many organizations and the UK Government's response on this is worth referring to in detail as follows:

"The Government continues to believe that interpreting the definition of DSPs to include all online activity, or all activity that could potentially be classed as 'software as a service' is not consistent with the NIS Directive. Cloud services are limited to those that are scalable and elastic – by which we mean computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand (scaleable) and computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload (elastic).

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

For online marketplaces, the Government is clear that the service has to be a genuine marketplace for goods or services and not an online retailer. Where a provider offers both retail services and online marketplace services, the online marketplaces services are covered by the NIS Directive. In relation to payment for those services, if a purchaser purchases a product from an online marketplace, and payment for that product takes places through services provided by that online marketplace (whether third party or not) then they are within scope of the NIS Regulations. If the online marketplace transfers the purchases to the original product seller's website, and the purchase and transaction take place there, then they are not within scope of the NIS Regulations. In relation to size, the primary requirement is that the DSP must be larger than a small or micro-sized business (i.e. have 50 or more staff and an annual turnover of €10m a year). The size of its marketplace, or number of customers is not considered in any assessment of a DSP. If only part of a DSP's services are potentially within scope of the NIS Regulations, then the Government advises that the DSP contact the ICO (nis@ico.org.uk) to seek clarification on how the Regulations will apply.

Where a prospective DSP is unclear about whether or not they are in scope of the NIS Regulations, they are strongly advised to contact the ICO (nis@ico.org.uk) for clarification."

Next steps and key takeaway

If organizations wish, they can submit comments on the Government's response. The ICO currently has some guidance about NIS (which can be found here: https://ico.org.uk/for-organisations/the-guide-to-nis/) and it is anticipated that the ICO will update this in light of the Government's consultation exercise. The Government's response can be seen as an indication of how the ICO might approach the NIS regime as regards DSPs.

For other articles that we have written about cybersecurity please see here: http://www.corderycompliance.com/category/cyber-security/

We also report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.