Are you a DSP? Uncertainty over scope of NIS Directive

September 2018

New security and breach notification laws for online market places, online search engines and certain cloud computing service providers ('Digital Service Providers' or 'DSPs') have applied in the UK since May this year, but there is still some uncertainty as to who exactly is in scope.

Last month the Government published the response to its targeted consultation on how the Security of Network and Information Systems (or 'NIS') Directive will apply to DSPs in the UK. It looked at:

- the identification of DSPs;
- security measures; and
- further guidance.

In this briefing, we look at how the Government has tried to clarify which DSPs are in scope through its consultation response and what being an in-scope DSP (or an organisation that obtains services from an in-scope DSP) means in practice.

Targeted consultation on DSPs

The Government carried out its main consultation on the UK's implementation of the NIS Directive in 2017, publishing its response in January 2018. However, it committed to carrying out a smaller, targeted, consultation on DSPs when the European Commission's Implementing Regulation (a piece of secondary legislation setting out security measures and incident reporting thresholds for DSPs) had been agreed. The response to this second, targeted, consultation was published after the Network and Information Systems Regulations 2018 ('NIS Regulations'), which implemented the NIS Directive into UK law, came into force. The Government therefore plans to use the response to help the regulator for DSPs (the Information Commissioner's Office, or 'ICO') to clarify its NIS guidance. The key areas the Government wants to clarify are: how DSPs can more easily identify whether they are within scope of the NIS Regulations; how cloud services in particular are defined; and how the ICO's cost recovery process will operate.

Background: aim of the NIS Regime and Brexit impact

The NIS Directive aims to improve the overall level of network and information system security in the EU by (amongst other things) ensuring Member States have a national framework in place to support and promote the security of network and information systems (for example having a National Cyber Security Strategy) and ensuring that framework is applied effectively across critical sectors which rely heavily on information networks. This includes imposing security and breach notification obligations on DSPs and on operators of essential services (or OES) in the energy, transport, water, healthcare and digital infrastructure sectors – see our briefing New cyber rules: what should you do to comply for more information on how the NIS Directive applies to OES.

The Government has already confirmed that, post Brexit, it intends for these policy provisions to continue to apply in the UK.

The Identification of DSPs: who is in scope?

The UK's NIS Regulations impose obligations on Relevant DSPs ('RDSPs'). To be a RDSP you must:

- provide a 'digital service' – a digital service is an Information Society Service which is an online market place, online search engine or cloud computing service provided to an external customer (see box: "What is a digital service?");

- have your head office in the UK, or have appointed a representative established in the UK; and

- not be a small or micro enterprise (i.e. an individual firm with fewer than 50 staff and a turnover of less than Euro 10 million – the rules are more complicated where you are part of a group).

However, there has always been some confusion as to who exactly this definition covers. Just under half (45%) of the respondents to the Government's DSP consultation said they were not 'readily able' to identify themselves as DSPs. The main area of difficulty related to the definition of cloud service providers.

The current ICO guidance for RDSPs regarding cloud computing services confirms that cloud computing services are digital services that enable access to a scalable and elastic pool of computing resources. This covers Platform, Infrastructure and Software as a service ('PaaS, IaaS and SaaS'), although SaaS services are only covered if they are business-to-business and meet the scalable and elastic requirements.

Respondents to the consultation questioned the UK's proposal to limit cloud services to public cloud services and asked how elastic and scalable were defined. In its response to the consultation, the Government confirmed that its intention has always been to 'limit the scope of those who have to comply with the Directive to those companies whose loss of service could have the greatest impact on the UK economy either directly or through impact on other companies.' This does not include all online activity, or activity that could be classified as 'software as a service'. Cloud services are limited to those which are scalable and elastic, which the Government considers to 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)."

Some respondents to the consultation also raised questions over the definition for online marketplaces. The Government confirmed in its response that the service has to be "a genuine marketplace for goods or services and not an online retailer" to be within the online marketplace definition. Payment for the goods or services sold must also take place through that online marketplace (whether their payment service are operated by a third party or not) and not be transferred back to the original sellers' website.

Security measures

The Government response confirmed the importance of ensuring that any security and incident reporting measures put in place in the UK are consistent with the Commission's Implementing Regulation and compatible with those across Europe (given the fact that many RDSPs also operate across Europe). They have recommended that the ICO, who is responsible for publishing further guidance on how RDSPs can meet the security requirements set out in the NIS Regulations, advise RDSPs to follow the technical guidance published by the European Network and Information Systems Agency ('ENISA'). The National Cyber Security Centre and ICO GDPR Security Outcome guidance is also compatible with the ENISA requirements.

What does this mean in practice?

The ICO has already published its initial advice for DSPs on compliance with the NIS Regulations which address many of the points raised in the Government's consultation, and the consultation response states that the ICO will issue updated guidance "as soon as is feasible". In the meantime, those providing cloud services should check they understand:

- whether they are RDSPs before 1st November – the deadline by which RDSPs must register with the ICO;

- which services they offer are in-scope - if only part of the RDSPs services are in scope, the Government advises contacting the ICO for clarification on how the NIS Regulations will apply;

- their security and breach notification obligations under the NIS and how these will work in practice with similar obligations (for example, under the GDPR).

Organisations buying cloud and other digital services from providers who may be RDSPs may also like to know whether those providers are within scope of the NIS or not. This is particularly important for OES engaging RDSPs, as an OES must notify its regulator about any significant impact on the continuity of the service it

provides caused by an incident affecting the RDSP. When engaging RDSPs, a customer may therefore want to:

- build NIS compliance into their supplier due diligence and selection processes and contractual warranty-style protections; and
- consider whether to extend contractual protections relating to security compliance and breach notification which apply to the GDPR so that they also cover the NIS regime.

What is a digital service?

A digital service is an Information Society Service (as defined in Article 1(1) of Directive 2015/1535) which is an online market place, online search engine or cloud computing service.

- online marketplace means a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;
- online search engine means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found; and
- cloud computing service means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

This article was written by Rob Sumroy and Natalie Donovan of Slaughter and May's Cyber Advisory team.

Our Cyber Advisory team can help your business plan for and manage your cyber risk, working closely with you to develop tailored cyber risk management frameworks and training and response plans, providing hands-on support to your internal stakeholders in the event of a cyber attack, and helping you to mitigate cyber risk generally in your business. For more information, please contact Rob, Natalie or your usual Slaughter and May contact.

Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com