July 2018

The Network and Information Systems Regulations: will your business have to comply?

The Network and Information Systems Regulations came into effect with little fanfare on 10 May 2018, when most businesses were in the throes of grappling with GDPR compliance. For this reason they seem to have passed largely under the radar. Here we assess whether you might be caught by the new Regulations, and if so, what you have to do to comply.

The Regulations implement the EU's Network and Information Security Directive. They set up a national framework for regulating cyber security, and require businesses which fall within their scope to:

1. maintain measures to ensure that their critical network and information systems remain secure from cyber attacks and vulnerabilities

2. observe reporting obligations – in the event of certain security incidents.

The penalty for non-compliance is potentially severe –up to £17 million for the most serious breaches – which are defined as those which have caused or could cause an immediate threat to life or a significant adverse impact on the UK economy. This is in addition to any fine issued by the ICO for breach of GDPR, to the extent that the same incident also causes a loss of personal data.

Enforcement of the Regulations will be overseen by competent authorities – a number of government departments and regulators, the identity of which differs depending on the sector that your business is in, and in the case of relevant digital service providers (see below), the Information Commissioner's Office (ICO).

Who do the Regulations apply to?

The Regulations apply to two types of business: relevant digital service providers (RDSPs) and operators of essential services (OES').

RELEVANT DIGITAL SERVICE PROVIDERS

RDSPs are defined as any business which operates an online market place, an online search engine or provides cloud computing services and which has its head office in the UK. At face value, this might include online retailers as well as any business which supplies software as a service, and the question of exactly which tech businesses are

caught by the Regulations has been the source of more than a little confusion.

If you are hoping to avoid the additional regulation, the good news is that the net is not as wide as it would first seem.

Essentially the Regulations are intended to catch those RDSPs which other businesses or people rely on to provide a service which is in some way critical to the way they continue to operate. The Department of Culture, Media and Sport (DCMS) has indicated that in the case of online market places, it is those businesses which provide the infrastructure to enable people to trade with others online who will be caught, rather than price comparison websites or online retailers. In the case of cloud computing service providers, the DCMS has said that the Regulations will focus primarily (though not exclusively) on public cloud providers – that is, providers of digital services which enable access to "a scalable and elastic pool of shareable resources", as opposed to those which provide services using private IT infrastructure to a single organisation or customer. So for example, if you provide a cloud storage facility to customers, then you need to make sure that that facility is secure, to the standards set out in the Regulations.

This approach makes more sense when considered in the context of the other group which the Regulations apply to – which is those businesses that supply an 'essential service' (see below). However, if you are in doubt as to whether your business is covered, then the best course of action is to contact the ICO for further guidance.

OPERATORS OF ESSENTIAL SERVICES

The other group of businesses which the Regulations apply to, are OES'. These are set out in the Regulations as those businesses which supply electricity, provide oil and gas, transportation, healthcare, water supply or digital infrastructure, and meet certain detailed thresholds in terms of size (for example, electricity suppliers which supply more than 250,000 customers, and oil suppliers which produce a minimum tonnage of oil per year). Whilst many would regard finance and banking as a sector in which essential services are provided, the banking industry falls outside the Regulations, on the basis that there are already industry specific rules in place which address similar risks.

The Regulations go into considerable detail in terms of thresholds and if your business falls within a sector which is caught by the Regulations, and you suspect that you supply a service which would be caught, then the best starting point is to work through the thresholds to ascertain whether they apply. If in doubt, then as with RDSPs, the best course of action is to consult further with your competent authority – again, its identity is set out in the Regulations.

Note that the Regulations leave open the possibility for competent authorities to pronounce other businesses as subject to the Regulations where they think that an incident affecting the provision of an essential service is likely to have a significant disruptive effect on the continuity of that service. So it is not wise to disengage completely if you are border line and not currently within scope.

What must you do to comply?

If you are caught by the Regulations, what must you do to comply? Fortunately the standards which a business is required to meet are not dissimilar to those which are set under GDPR, albeit that they apply to any aspect of a network and information system on which an essential or digital service relies, not just systems on which personal data is processed. The requirements (below) are supported with an audit right which the Regulations provide for competent authorities and the ICO (as applicable).

SECURITY OF SYSTEMS

The requirement is to "take appropriate and proportionate technical and organisational measures to manage the risks posed" to such systems, and to "prevent and minimise the impact of incidents".

The sources of guidance as to what this means in practice, and as referred to by the Government in various communications, is again a potential source of confusion and at times overwhelming. For example, for RDSPs the ICO has said that the guidance it produces will be based on technical guidance published by the European Network and Information Systems Agency in 2017 (ENISA), whilst DCMS has recommended that the National Cyber Security Centre Cyber Assessment Framework should be used to make

determinations on acceptable levels of cyber security for OES'.

However the following steps are all sensible precautions for businesses to take when putting together a compliant cyber strategy:

- Do your due diligence, both internally and on others in your supply chain to identify what cyber risks you face.
- Maintain a framework, both technical and organisational, to manage these risks, regularly test for weaknesses, and respond effectively to the results.
- Make sure that your supply chain is covered as necessary by your framework, to the extent that a supplier is responsible for any part of the systems on which you rely to provide your service.
- Have a documented, tested plan with clear lines of communication and action, for responding to cyber (and other) incidents and ensuring business continuity, which incorporates a process for reporting incidents to a 'competent authority'.
- Support all of the above steps with a clear and well documented audit trail.

The key thing for any business which is caught by the Regulations to bear in mind is that it is not necessarily the fact that it has suffered an incident which will attract the fine, but what it did or did not do to try and prevent the incident. This is supported by DCMS' commentary which urges competent authorities to take a cautious approach to enforcement, at least for the first year, and to give businesses time to reach the appropriate levels of security, working in consultation with the relevant authority.

REGISTRATION

The final requirement for businesses which are in scope, and again something which businesses which are familiar with data protection law will know well, is to register with their competent authority. For RDSPs, the deadline is 1 November 2018 (new RDSPs will have three months from the date they fall within scope to register). There are further details about how you can register on the ICO's website.

For OES' who are caught by the Regulations, the deadline for notification to their competent authority is **10 August 2018**. If your business is such that you are both an OES and an RDSP (as some digital infrastructure businesses might well be), then you will need to register as both and be mindful of both regimes, albeit that DCMS has said that the ICO and the relevant competent authority (Ofcom for digital infrastructure) should work together in relation to such businesses.

WHAT ABOUT OTHER BUSINESSES?

If you are a business positioned in the supply chain to an OES or RDSP – for example, a provider of outsourced IT services or infrastructure – you may well see some of the requirements under the Regulations passed back to you by way of additional contractual obligations, audit rights and due diligence.

The Regulations are otherwise unlikely to have much of a direct impact on other businesses outside their scope. That said, in an age where cyber incidents are on the increase, and where the cost to businesses in terms of rectification and reputational loss can be far reaching, it is worth keeping an eye on what happens under the Regulations, as they may lead to good practice of general application.

POST SCRIPT: THE BREXIT EFFECT

For those hoping that Brexit will take the pressure off complying, think again; as Regulations implementing an EU directive, the new laws will continue to apply after 31 March 2019, and the Government has made clear that it intends to maintain the Regulations post EU exit.

IF YOU WOULD LIKE TO DISCUSS ANY OF THE ISSUES RAISED IN THIS BRIEFING, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Richard Brown
Partner, Commercial, IP & Technology

E: richard.brown@traverssmith.com
T: +44 (0)20 7295 3254

James Longster
Partner, Commercial, IP & Technology

E: james.longster@traverssmith.com
T: +44 (0)20 7295 3496