Cooley

EU Privacy Q&A – Network and Information Security Directive

January 11, 2017

The UK Government has published its report entitled "Cyber Security Regulation and Incentives Review", which sets out its intentions following Brexit on the implementation of the Network and Information Security Directive ("NISD"); this affects organisations in sectors such as energy, transport, water, banking, healthcare and digital infrastructure.

Q1. What is the NISD?

A1. The NISD entered into force in August 2016 as part of the European Commission's Digital Single Market Strategy and Member States will have 21 months to transpose it into national law. It provides legal measures to boost the level of cybersecurity across the EU, with measures such as: ensuring Member States have a Computer Security Incident Response Team (CSIRT); a cooperation group to support and facilitate strategic cooperation among Member States; and encouraging a culture of security across critical sectors such as energy, transport, water, banking, healthcare and digital infrastructure.

Q2. Why should you care?

A2. Although Brexit means that the UK will not be obliged to implement the NISD, there is a strong argument to at least consider it. Both the global political and digital landscapes have seen huge exposure to cyber-attacks over the past year, with the threat only increasing. Organisations must consider their own cyber security. According to a 2016 HM Government survey, the average direct costs for a breach are £36,000 for large businesses and £3,100 for small businesses, with potential losses for large firms capable of reaching millions.

Q3. What will the Government do?

A3. It intends to apply the General Data Protection Regulation aka the "GDPR" (which will be enforceable from May 2018 and significantly raises the bar on how organisations treat personal data). In addition, it will employ "non-regulatory interventions to incentivise better cyber risk management", including: maximising awareness on cyber security via GDPR implementation; using breach report data to increase regulator understanding of threats; and establishing a regulators' forum. The report also indicates that the UK regulator (the ICO) will take an increased role on cyber security in partnership with the new National Cyber Security Centre (NCSC).

Q4. What *won't* the Government do?

A4. It will *not* mandate: cyber insurance, cyber health checks, statements on cyber risk management in annual reports, or breach reporting beyond the GDPR requirements. For now, the Government will not pursue regulation beyond the GDPR; it sees further regulation as unjustified and unlikely to outweigh the burden further implementation measures would place on business. That said, it will keep this area under review as the evidence bases on threats grows and it is separately considering whether additional regulation may be required for critical sectors.

Q5. What should you do?

A5(a). *For organisations in the US*: Don't confuse NISD (the European legislation) with NIST (the US voluntary cybersecurity framework); you will *not* be subject to the NISD and instead you should comply with US cybersecurity regulation. That said, you will likely be subject to the GDPR if you sell to the EU or monitor data in the EU; a way of improving chances of compliance with the GDPR may be to consider adopting the voluntary US NIST framework.

A5(b). *For organisations in the UK*: one has to ask – if the GDPR really is enough, why would the EU bother with

the NISD at all? Take matters into your own hands. The report is clear on one thing; "*it should ultimately be for organisations to manage their own risk in respect of sensitive data*". Only 10% of businesses in the UK have a formal incident management plan. Get advice. Analyse the risks. Take control.

Key Contacts

Ann Bevitt London	abevitt@cooley.com +44 (0) 20 7556 4264