EU NIS II Proposed Rules Agreed By EU Countries & EU Parliament

Date : May 23, 2022

What's this about?

In 2016 the EU introduced the so-called NIS Directive (NIS I) which EU countries had to implement in 2018 (just before EU GDPR fully came into force!). Broadly-speaking, NIS I aimed at ensuring cybersecurity regulatory harmonization across the EU. Under the NIS I regime, entities that fall in scope have to report cybersecurity incidents to regulators and can face fines for compliance failures.

However, the NIS I regime didn't seem to go entirely to plan, especially as regards a major lack of enforcement, and so in 2020 the EU proposed to completely overhaul it and replace it with new legislation, i.e. NIS II. The EU Member States (the Council of the EU) and the European Parliament have now reached political agreement on NIS II, which this article takes a brief look at.

What did NIS I achieve?

In sum, NIS I:

- Contributed to improving cybersecurity capabilities at national level by requiring EU countries to adopt national cybersecurity strategies and to appoint cybersecurity regulators;
- Increased cooperation between EU countries at the EU level by setting up various ways to facilitate the exchange of strategic and operational information; and,
- Improved the cyber resilience of public and private entities in seven specific sectors (energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution, and digital infrastructures) and across three digital services (online marketplaces, online search engines and cloud computing services) by requiring EU countries to ensure that operators of so-called essential services and digital service providers put in place cybersecurity requirements and report incidents.

What went wrong?

In its review of NIS I the European Commission conclusions included the following:

- The scope of NIS I is too limited in terms of the sectors covered, mainly due to: (i) increased digitisation in recent years and a higher degree of interconnectedness; and, (ii) the scope of NIS I no longer reflects all digitised sectors providing key services to the economy and society as a whole;
- NIS I is not sufficiently clear when it comes to the scope for operators of essential services ("OESs") and its provisions do not provide sufficient clarity regarding national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in all EU countries and are therefore not required to put in place security measures and report incidents;
- NIS I allows wide discretion to EU countries when laying down security and incident reporting requirements for "OESs". In some instances EU countries have implemented these requirements in significantly different ways, creating additional burden for companies operating in more than one EU country;
- The supervision and enforcement regime of NIS I has been ineffective – EU countries have been very reluctant to apply penalties to entities who failed to put in place security requirements or report incidents;
- The financial and human resources set aside by EU countries for fulfilling their tasks and consequently the different levels of maturity in dealing with cybersecurity risks vary greatly; and,
- EU countries do not share information systematically with one another, with negative consequences in particular for the effectiveness of cybersecurity measures and for the level of joint situational awareness at EU level.

What's in the politically agreed NIS II?

In broad terms, NIS II includes the following:

- It covers medium and large entities from more sectors that are critical for the economy and society, including: (a) public electronic communications service providers; (b) digital service providers; (c) waste water and waste management service providers; (d) critical products manufacturers; and, (d) postal and courier service providers. It also covers more broadly the healthcare sector, for example by including medical device manufacturers, given the increasing security threats that arose during the Covid-19 pandemic. NIS II in effect introduces a size-cap meaning that all medium-sized and large entities operating within the applicable sectors or providing services covered by NIS II will fall within its scope;
- It strengthens cybersecurity requirements imposed on companies (use of cryptography and encryption etc.);
- It addresses security of supply chains and supplier relationships;
- It introduces accountability of top management for non-compliance with cybersecurity obligations;
- It streamlines reporting obligations: (a) any significant incidents will have to be reported, namely when an incident potentially causes severe operational disruption or financial losses for the entities concerned, or affects other natural or legal persons by causing considerable material or non-material losses; (b) incidents must be reported to individuals and, to the general public in some cases; (c) entities in scope must notify the relevant regulator within 24 hours of becoming aware of an incident and provide a more detailed report within 72 hours – a report containing minimal requirements must also be submitted; and, (d) failure to implement security measures or report incidents can result in fines of up to 2% of the preceding year's annual global turnover;
- It introduces more stringent supervisory measures for national regulators, as well as stricter enforcement requirements;
- It aims at harmonising sanctions regimes across EU countries; and,
- It will increase information-sharing and cooperation on cyber crisis management at both the national and EU levels.

What's next?

NIS II is now coming to the end of its passage through the EU legislative pipeline. The political agreement reached by the European Parliament and the EU Council on NIS II is now subject to formal approval by them, as co-legislators. Once NIS II is published in the EU Official Journal, as an EU directive it will enter into force 20 days after its and EU countries will then have 21 months to implement it into their respective national laws.

What are the takeaways?

The expansion in scope under NIS II means that more entities and sectors will have to undertake cybersecurity risk management measures.

Post-Brexit the UK will of course not apply NIS II – as to whether the UK chooses to introduce any of NIS II in its own expected reforms of the NIS I regime in the UK remains to be seen. Organizations operating in the UK and the EU will however have to ensure compliance between what may be two diverging regimes.

Organizations who are likely to fall under NIS II should:

- Alert the Board about NIS II and plan resources to address it;
- Review procedures to address risk assessment, response management, internal investigation, and, incident reporting;
- Update and/or revise policy documentation;
- Review contracts with vendors and adapt/introduce supply-chain NIS reporting obligations;
- Undertake training and develop internal cyber-security advocacy and awareness;
- Re-evaluate and/or prepare a press strategy in the event of an IT security breach; and,
- Consider reassessing existing cyber-insurance or taking out a new policy.

Resources

We have written about the NIS regime here https://www.corderycompliance.com/client-alert-nis-2-directive/, here https://www.corderycompliance.com/eu-network-information-security-directive-faqs/, here

https://www.corderycompliance.com/uk-to-implement-eu-cybersecurity-directive/, and here https://www.corderycompliance.com/uk-government-response-to-cybersecurity-nis-digital-service-providers-consultation/.

We report about cyber security issues here: https://www.corderycompliance.com/category/cyber-security/.

We report about data protection and privacy issues here https://www.corderycompliance.com/category/data-protection-privacy/.

The EU's press release about political agreement on NIS II can be found here https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

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