CLIFFORD

CHANCE

NIS 2 DIRECTIVE: EUROPE REVAMPS ITS CYBERSECURITY FRAMEWORK

NIS 2 DIRECTIVE: EUROPE REVAMPS ITS CYBERSECURITY FRAMEWORK

On 28 November 2022, the Council of the European Union (**EU**) voted to adopt the Network and Information Systems Directive (EU) 2022/0383 (**NIS 2**). Seeking to expand, strengthen and harmonise implementation of the EU's existing cybersecurity framework, NIS 2 forms a key part of the EU's Cybersecurity Strategy and aligns with the European Commission's priority to make Europe fit for the digital age.

Approval by the European Parliament took place on 10 November 2022. Formal publication of NIS 2 is expected soon, with Member State implementations of NIS 2 to follow within 21 months. This briefing looks at key changes introduced by NIS 2 and what organisations should be doing now to prepare for them.

WHAT IS NIS 2?

NIS 2 repeals and replaces the Network and Information Systems Directive (EU) 2016/1148 (**NIS 1**), which sought to achieve a high common level of cybersecurity across the EU, with a focus on protecting critical infrastructure. NIS 2 builds on the NIS 1 framework to impose cyber risk management, incident reporting and information-sharing obligations on certain types of organisations in a range of sectors.

NIS 2 has been introduced because the implementation of NIS 1 was recognised to have limitations. In July 2020, the European Commission launched a consultation on potential reform, finding that updates to NIS 1 were required due to the rapid pace of digitalisation, the increasing interconnectedness of sectors and heightened cyber risks. The identified shortcomings of NIS 1 included a limited scope, lack of harmonisation across Member States, inconsistent levels of cyber resilience across Member States and business sectors, and a lack of joint crisis response mechanisms.

WHO IS IN SCOPE?

NIS 2 applies to all entities which: (i) provide their services or carry out their activities in the EU; and (ii) match the description of either an "essential" or an "important" entity in a defined list of sectors. Notable exceptions to this are: (i) a size-cap, which means small and micro businesses are excluded in many cases; and (ii) Member States can make exemptions for specific entities that carry out activities in the areas of national security, public security, defence or law enforcement.

The relevant sectors from which certain businesses may qualify as essential or important entities include banking, financial market infrastructures, digital providers (being online marketplaces, online search engines and social networking platforms), digital infrastructure (including providers of public electronic communications networks and services, cloud service providers and data centres), business-to-business ICT service management, energy, transport, health, space, certain types of manufacturing (including of machinery, computers and electronics, motor vehicles and other transport equipment), certain production and distribution (e.g. of food) and certain utilities.

SUMMARY OF KEY CHANGES

NIS 2 introduces significant changes, including:

- expanding the scope of NIS 1 and revising the way in which companies are classified;
- outlining 10 core cybersecurity measures that all in-scope organisations are required to put in place;
- addressing the security of ICT supply chains and supplier relationships;
- imposing direct obligations on "management bodies" in respect of an entity's' compliance with NIS 2;
- amending the incident reporting requirements;
- bolstering national authorities' ability to supervise companies, particularly those in critical sectors;
- strengthening sanctions for non-compliance; and
- enhancing co-operation and information sharing between Member States

Key differences compared with NIS 1

- Under NIS 1, entities were classified as either "operators of essential services" or "digital service providers" but this distinction did not reflect the importance of the entity to society and the economy. NIS 2 eliminates this classification, with the "essential" or "important" classification depending on sector or the type of service provided and, in most cases, an entity's size.

- Under NIS 1, Member States were responsible for the classification of "operators of essential services". NIS 2 applies in a more prescriptive manner, in order to ensure more consistent application across Member States.

- The scope of NIS 2 has been widened to capture entities in a number of additional sectors and subsectors compared with NIS 1, including, for example, social media platforms, public administration and certain manufacturing (e.g. of medical devices).

KEY NEW REQUIREMENTS AND RESPONSIBILITIES

All essential and important entities are subject to the same cybersecurity risk management requirements and incident reporting obligations under NIS 2 (with such obligations to be implemented into national law by Member States). However, appropriateness and proportionality requirements mean that the way in which these obligations are met will differ according to an entity's risk exposure, importance and size.

NIS 2 ensures a minimum level of harmonisation. Member States may adopt or maintain provisions that impose higher standards for cybersecurity, provided they are consistent with EU law

Cybersecurity risk management

NIS 1 included requirements for the adoption of appropriate and proportional technical and organisational measures to manage cybersecurity risks. These have been bolstered in NIS 2 by requirements for all in-scope entities to implement a core set of policies. Required policies include (amongst others): risk analysis and incident response; encryption and cryptography; vulnerability disclosure; cybersecurity training and ICT supply chain security.

The emphasis in NIS 2 on addressing risks in entities' ICT supply chains means that businesses that are outside the direct scope of NIS 2 may also be impacted. When considering whether ICT supply chain security policies are appropriate, essential and important entities will be required to take into account the vulnerabilities to each direct supplier and service provider, and the overall quality of products and cybersecurity practices of their suppliers and services providers. Essential and important entities are encouraged to incorporate cybersecurity risk management measures into their contractual arrangements and to exercise increased due diligence in selecting their managed security service providers. Member States will also be required to adopt policies addressing, amongst other things, cybersecurity in their ICT supply chain and the inclusion of cybersecurity-related requirements for ICT products and services in public procurement.

In-scope entities must also adopt adequate technical, operational and organisational measures, proportional to "*the degree of the entity's exposure to risks, its size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact*". NIS 2 expects entities to undertake a risk assessment to determine what measures are appropriate. The risk assessment process suggests important entities may be able to adopt less stringent measures than critical entities

Management responsibility

NIS 2 imposes obligations on the "management bodies" of in-scope entities to approve the adequacy of, and supervise the implementation of, cybersecurity risk management measures, and Member States must ensure that management bodies can be held liable for infringements by the entity of provisions relating to those measures. Members of management bodies of in-scope entities will be required to follow training on a regular basis in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity.

In relation to essential entities, Member States must ensure that a natural person responsible for (or acting as a legal representative of) an essential entity has the power to ensure its compliance with NIS 2, and that it is possible to hold such persons liable for breach of their duties to ensure compliance with NIS 2.

Incident reporting

Under NIS 2, in-scope entities must submit an initial report or "early warning" to the competent national authority or computer security incident response team (CSIRT) without undue delay ***and within 24 hours*** from when the entity became aware of a significant incident (instead of simply "without undue delay" under NIS 1). This is to be followed by a fuller incident notification without undue delay and within 72 hours, and entities must then submit a final report no more than one month later. Entities will also be required to notify affected users without undue delay, where appropriate.

Helpfully, notified national authorities or CSIRTs must respond to an initial report within 24 hours with initial feedback on the incident and, if requested, guidance on the implementation of possible mitigation measures.

A further modification under NIS 2 is a simplified definition of "significant", which aims to address over-reporting of incidents. Under NIS 1, entities had to consider an expansive list of factors to determine whether an incident needed to be reported. Under NIS 2, an entity reports only those incidents which: (i) cause, or have the potential to cause, severe operational disruption of the services or financial losses for the entity concerned; or (ii) have affected, or are capable of affecting, other natural or legal persons by causing considerable material or non-material damage.

Registration

Certain in-scope entities (including providers of cloud computing services, data centre services, content delivery networks, managed services, online marketplaces, online search engines and social networking services platforms) will be required to submit certain information to competent authorities to enable the European Union Agency for Cyber Security (**ENISA**) to maintain a registry of such entities.

STRENGTHENED SUPERVISORY AND ENFORCEMENT REGIME

NIS 2 provides competent national authorities with broadened and strengthened powers to supervise and sanction in-scope entities. These can apply differently, depending on whether an entity is an essential entity or an important entity.

Supervision

Essential entities (such as providers of a certain size and providing specified services in identified sectors of "high criticality", such as banking, financial infrastructure, energy, transport, health and digital infrastructure sectors), will be subject to a fully fledged, *ex ante*, supervisory regime. Significantly, national authorities have a list of core powers to supervise essential entities, including the ability to carry out random inspections, regular and ad hoc audits, and security scans to check for vulnerabilities, as well as the ability to request certain information and evidence of compliance.

Important entities are subject to lighter, *ex post*, supervision in the event of evidence or indications of non-compliance.

Enforcement

NIS 2 provides national authorities with a minimum list of enforcement powers for non-compliance, including the power to order entities to make public aspects of the infringement, to cease certain conduct or to implement recommendations. In the case of essential entities, if the deadlines for taking action required by a competent authority are not met, the entity's certification or authorisation concerning the service can be suspended, and those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily prohibited from exercising managerial functions in that entity.

NIS 2 also harmonises the penalty regime by introducing uniform fine thresholds for breaches; the maximum fine for essential entities is the greater of EUR 10 million or 2% of annual worldwide turnover, whilst for important entities it is the greater of EUR 7 million or 1.4% of annual worldwide turnover.

ENHANCED CO-OPERATION AT NATIONAL AND EUROPEAN LEVEL

NIS 2 will retain the role of the CSIRTs and CSIRT network established under NIS 1. NIS 2 will create a new body, the European Cyber Crises Liaison Organisation Network (**EU-CyCLONe**), for the co-ordinated management of large-scale cybersecurity incidents and to ensure regular exchange of information amongst Member States and EU bodies.

Under NIS 2, ENISA will develop and maintain a European vulnerability registry to enable entities, and suppliers of network and information systems, to document vulnerabilities. Entities are encouraged to invite outsiders (often "ethical hackers") to examine their systems and identify vulnerabilities.

In-scope entities (as well as, where relevant, out-of-scope entities, such as suppliers or service providers) will be able to exchange on a voluntary basis relevant cybersecurity

information amongst themselves, for example in respect of cyber threats, near misses, and adversarial tactics. The onus is on Member States to facilitate the sharing of such information.

In addition, Member States, in co-operation with the Commission and ENISA, will carry out co-ordinated risk assessments of critical ICT supply chains at the EU level.

THE WIDER LEGISLATIVE LANDSCAPE

NIS 2 will apply alongside, and without prejudice to, certain existing EU legislation, such as the EU General Data Protection Regulation (GDPR). Notably, where competent authorities become aware of infringements of NIS 2 cyber risk management or incident reporting provisions that can entail a personal data breach under GDPR, they are required to inform the relevant data protection authorities.

Various sector-specific legislation in the EU has been considered in the drafting of NIS 2. In particular:

- NIS 2 provides that, where sector-specific EU legislation imposes equivalent requirements for essential or important entities to adopt measures or notify significant incidents, the relevant NIS provisions (and associated supervision and enforcement) will not apply;

- NIS 2 provisions would apply to all critical entities identified under the *Directive on the resilience of critical entities*, which focuses on resilience against physical risk in many of the in-scope sectors for NIS 2; and

- NIS 2 provides that any overlap with the *Regulation on digital operational resilience for the financial sector* (DORA) will be addressed by DORA being considered as *lex specialis* (i.e. a more specific law that will override the more general NIS2 provisions). (*See* our briefing on the Digital Operational Resilience Act.)

The proposed EU Cyber Resilience Act, which imposes cybersecurity requirements and incident reporting obligations on manufacturers, distributors and importers of connected hardware and software, will also feature in this evolving landscape of EU cybersecurity laws, and will complement the objectives of NIS 2 through the impact of its vulnerability disclosure and handling requirements on secure supply chain relationships where connected hardware or software forms part of the network and information systems of essential and important entities. (*See* our briefing on the Cyber Resilience Act.)

Multinational organisations will also be monitoring other regulatory reform in relation to cybersecurity and the potential impact on their compliance programmes and incident response plans – including, for example, tracking the New York State Department of Financial Services (NYDFS) consultation on amendments to the Cybersecurity Requirements for Financial Services Companies and awaiting the outcome of the UK's review of the UK Network and Information Systems Regulations 2018 SI 2018/506 (**UK NIS**), which implemented NIS 1.

TIMELINE AND NEXT STEPS

Following adoption of NIS 2 by the European Parliament plenary session on 10 November 2022 and adoption by the Council of the EU on 28 November 2022, publication of the Directive in the Official Journal is expected in December 2022.

NIS 2 will come into effect on the twentieth day following the day on which it is published in the Official Journal. Member States will then have 21 months to transpose the Directive into national law.

Timeline	
6 July 2016	NIS 1 adopted
9 May 2018	Deadline for Member States to transpose NIS 1 into national law
7 July 2020	European Commission launches consultation on NIS reform
16 December 2020	European Commission publishes proposal or NIS 2
22 November 2021	European Parliament adopts its negotiating position
3 December 2021	European Council adopts its negotiating position
13 January 2022	First round of trilogue negotiations
16 February 2022	Second round of trilogue negotiations
13 May 2022	Political agreement reached
10 November 2022	European Parliament votes to adopt NIS 2
28 November 2022	NIS 2 approved by the Council of the EU
Expected in late 2022	NIS 2 published in the Official Journal
Autumn 2024	Deadline for Member States to transpose NIS 2 into national law

KEY TAKEAWAYS

Be prepared

Companies must consider whether they are likely to fall within the scope of NIS 2 and, if so, whether they will be deemed important or essential entities.

Companies must plan for potentially significant costs associated with complying with the new requirements. According to the EU impact assessment for NIS 2, companies which were under the scope of NIS 1 should budget for an increase of up to 12% in their ICT spend for the years immediately following the implementation of NIS 2. For companies which were not subject to NIS 1, the estimate is 22%.

Review of Processes, Policies and Procedures

In-scope entities will need to review NIS 2 requirements – in particular in relation to cybersecurity risk management (such as the core set of associated policies) and incident reporting – and consider what changes need to be made to existing policies and procedures.

NIS 2 should lead to greater consistency in the implementation of cybersecurity measures across the EU. Multinational companies that were previously subject to NIS 1 may be able to streamline and harmonise certain processes and procedures to reflect the more uniform requirements across Member States. However, companies will need to be vigilant in relation to any remaining (or subsequently introduced) more stringent Member State requirements.

Spotlight on supply chain

NIS 2 (and developments elsewhere, such as proposals for UK NIS) mean that companies should be actively considering how to manage appropriately the cybersecurity risk posed by their use of managed services. As managed service providers have access to the networks of thousands of companies, a vulnerability in one such provider can expose the networks of many or all of its customers.

Overlapping obligations

Organisations should prepare for NIS 2 compliance in a holistic manner that also takes into account relevant obligations under other laws. For example, the cybersecurity policies and incident management procedures of in-scope entities for NIS 2 will need to consider all relevant requirements across applicable laws, including GDPR requirements for incident reporting and for appropriate technical and organisational measures. Organisations should not assume that a GDPR-compliant incident response process will be sufficient for NIS 2 purposes, particularly in light of NIS 2's tighter reporting timeframes.

AUTHORS

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Stephanie Phillips
Senior Associate
Amsterdam
T: +31 20 711 9769
E: stephanie.phillips@cliffordchance.com

Hannah Ovaisi
Senior Associate
London
T: +44 207006 5275
E: hannah.ovaisi@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

CONTACTS

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Frédérick Lacroix
Partner
Paris
T: +33 1 4405 5241
E: frederick.lacroix@cliffordchance.com

Gunnar Sachs
Partner
Dusseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Marc Benzler
Partner
Frankfurt
T: +49 69 7199 3304
E: marc.benzler@cliffordchance.com

Monica Sah
Partner
London
T: +44 207006 1103
E: monica.sah@cliffordchance.com

Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com

Thomas Voland
Partner
Dusseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Joanne Neenan
Director,
Public International Law
London
T: +44 207006 3754
E: joanne.neenan@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Gail Orton
Head of EU Public Policy
Paris
T: +33 1 4405 2429
E: gail.orton@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group Amsterdam
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Marian Scheele
Senior Counsel
Amsterdam
T: +31 20 711 9524
E: marian.scheele@cliffordchance.com

Carlos Zabala
Counsel
Madrid
T: +34 91 590 7515
E: carlos.zabala@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

Andrei Mikes
Senior Associate
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

Cheryl Jones
Senior Associate
Knowledge Lawyer
London
T: +44 207006 2386
E: cheryl.jones@cliffordchance.com

Mark Fisher
Senior Associate
London
T: +44 207006 1480
E: mark.fisher@cliffordchance.com

Oscar Tang
Senior Associate
London
T: +44 207006 3749
E: oscar.tang@cliffordchance.com

Lauren Sutcliffe and Ivan Panton contributed to the writing of this briefing.

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2211-003750