knowledge 16 July 2024 | 2 min read

Have Your Say on Upcoming NIS 2 Cybersecurity Obligations

The NIS 2 Directive (Directive EU 2022/2555) was adopted by the European Commission (the **"Commission"**) on 16 January 2023 and aims to ensure a common high-level security of network and information systems across EU Member States and to update cybersecurity obligations (see detailed briefing here (https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/impending-cybersecurity-obligations-are-you-subject-to-nis-2?_gl=1*6nc60c*_up*MQ..*_ga*OTYzNzc0Mjg5LjE3MjEyMDQ4OTQ.*_ga_E6XJ6TZ4XQ*MTcyMTIwNDg5My4xLjAuMTcyMTIw

The European Commission has published a draft implementing regulation (the **"Draft Regulation"**) which provides further details on cybersecurity risk management measures which are applicable to certain essential and important entities, as well as providing further detail regarding when an incident is considered to be 'significant' for the purposes of reporting obligations for those categories of entities. The Draft Regulation is open for public feedback until 25 July 2024.

What does the Draft Regulation cover?

Article 21 of the NIS 2 Directive imposes obligations on essential and important entities to put in place cybersecurity risk-management measures, while Article 23 imposes obligations on such entities to report 'significant incidents' to the Computer Security Incident Response Team (**"CSIRT"**).

The NIS 2 Directive requires the Commission to adopt certain implementing acts by 17 October 2024, laying down:

a. the technical and methodological requirements of the applicable cybersecurity risk-management measures, and
b. further details regarding the cases in which an incident will be considered 'significant', applicable to certain specified essential and important entities.

Who does the Draft Regulation apply to?

The Draft Regulation applies to the following essential and important entities:

domain name system (**"DNS"**) service providers;
top-level domain (**"TLD"**) name registries;
cloud computing service providers;
data centre service providers;
content delivery network providers;
managed service providers;
managed security service providers;
providers of online market places, of online search engines and of social networking services platforms, and
trust service providers (the **"Relevant Entities"**).

What does it say about “technological and methodological requirements” of cybersecurity risk management measures?

The Annex to the Draft Regulation sets out the technical and methodological requirements of cybersecurity risk management measures as applicable to the Relevant Entities in significant detail. This includes detailed requirements for:

a. A policy on the security of network and information systems;
b. A risk management policy;
c. Incident management;
d. Business continuity and crisis management;
e. Supply chain security;
f. Security in network and information systems acquisition, development and maintenance;
g. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
h. Basic cyber hygiene practices and security training;
i. Cryptography;
j. Human resources security;
k. Access control;
l. Asset management; and
m. Environmental and physical security.

What does it say about significant incidents?

The Draft Regulation lays down criteria which, if one or more are fulfilled, dictate whether an incident should be considered significant for the purposes of reporting obligations under the NIS 2 Directive.

This includes criteria such as specified levels of financial loss, considerable reputational damage, the exfiltration of trade secrets, the death of or damage to a natural person, or the occurrence of successful, suspectedly malicious and unauthorised access to network and information systems. The Draft Regulation also sets out criteria for ‘recurring incidents’, and specific criteria to be considered by each of the Relevant Entities.

What is the timeline for feedback?

The European Commission published the Draft Regulation on 27 June 2024 (here (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en)) and has stated that it is open for feedback for a period of 4 weeks until 25 July 2024. Organisations which fall within the categories of Relevant Entities and will be subject to the finalised implementing regulation should review the Draft Regulation and consider whether they would like to provide feedback on any particular aspect.

Also contributed to by Lisa Leonard

This document has been prepared by McCann FitzGerald LLP for general guidance only and should not be regarded as a substitute for professional advice. Such advice should always be taken before acting on any of the matters discussed.

Key contacts

Paul Lavery
Partner