Ministry of Resilience and Preparedness

14. October 2025

The Danish Government's response to the Commission's call for evidence for the Digital Omnibus as regards cybersecurity

Need for continued high level of cybersecurity
Denmark supports the overall ambition to simplify EU legislation. However, it is vital that any simplification efforts regarding cybersecurity legislation maintains the current objectives of a high-common level of cybersecurity across the EU. The digital omnibus should therefore focus on clarification, increasing consistency and complementarity when it comes to cybersecurity legislation and its relation to other digital legislation.

Short term: Streamlining of reporting obligations
On the short term, we believe the most effective way forward is to streamline reporting requirements across digital legislation. Incident reporting should be streamlined across cybersecurity regulations, so that the same criteria are used to assess the relevance and impact of incidents for the purposes of reporting. This could be in relation to reporting formats and guidelines that ease the burden of compliance.

Some reporting obligations (such as from NIS 2 and CER) can easily be merged due to their similar nature. We see practical and legal challenges for reporting obligations where reporting frequency, purpose, mandate and responsibilities vary.

To this end, an impact assessment for streamlining cybersecurity legislation should be fast-tracked.

Public authorities and private companies are required to comply with multiple, parallel regimes when deploying digital technologies and handling sensitive data. Although these regimes' objectives are complementary, their operational requirements, risk assessments, reporting duties, and supervisory oversight, are fragmented. This can create unnecessary duplication and increase the likelihood of non-compliance.

An example: A single incident, such as a ransomware attack affecting availability, integrity and confidentiality, may trigger:

- **Article 23 NIS 2**: notification to CSIRTs within 24 hours.
- **Article 33 GDPR**: personal data breach notification to the Data Protection Authority within 72 hours.
- **Article 62 AI Act**: reporting of serious incidents involving AI systems.

Each obligation is legitimate in isolation, yet together they generate a resource-intensive and fragmented compliance landscape.

From a legal perspective, divergent deadlines, thresholds and procedural requirements increase the likelihood of premature or incomplete reporting, or even outright non-compliance. This not only jeopardises regulatory conformity but can also create legal uncertainty, which in turn complicates the ability of authorities to demonstrate accountability.

From a security perspective, fragmented duties risk diminishing the overall capacity to contain and remediate breaches, thereby conflicting with the core objectives of NIS 2. Consequently, operational resilience, which depends on clarity, coherence and timely intervention, can be impaired.

Moreover, reporting obligations should be evaluated as to what purpose they serve. Currently, a number of the objectives – including knowledge gathering, legal requirements, and operational requirements – are served by the same reporting scheme (this is the case under NIS 2). This leads to the scope of the reporting increasing drastically, as each reporting scheme has to fulfill several objectives. These schemes should be disaggregated and their contents streamlined according to the specific purposes that they serve. In this way the extent of incident reporting can be streamlined and administrative costs lowered substantially. It should be clear if the objective is to ensure effective incident handling or to gather information or to ensure compliance. The objective should then be reflected in both the deadlines for reporting (if it is to ensure compliance, is it then needed within 24 hours?) and the type of information requested in the report.

The provision of reports at different times after an incident should be changed so that only the reports expressly needed to fulfill the legal requirements and operational needs are retained. Additionally, the reporting times should be the same for all of the relevant digital legislations.

Additionally, under NIS 2, lex specialis and implementing acts have been introduced. These can have slightly different approaches to incident reporting. All incident reporting in current or future lex specialis as well as implementing acts should be streamlined to follow the provisions in NIS 2. This will minimize confusion amongst NIS 2 entities and allow clear divisions of responsibility between actors at national and EU levels.

Long term

The streamlining as described above will lay the ground work for further simplification, including the possibility of a common reporting platform.

To facilitate this, the reporting platform that ENISA will launch for the Cyber Resilience Act could be expanded to function as a single reporting platform or a platform to forward incidents for all digital incidents, given these criteria are fulfilled:

- The national CSIRT still receives cybersecurity incidents directly to maintain national situational awareness.
- The platform is built in a decentralised manner that maintains a high level of security and avoids a Single Point of Failure or a single access point for malicious actors.

- The platform is calibrated to work with existing national Single Reporting Platforms (for example the Danish platform at virk.dk). This could be by having national endpoints to access the platform that would forward (but not keep the data) to relevant authorities.
- The reports must be made in a machine-readable format.

Such a platform will most likely take time to develop. For a more short-term solution ENISA could link all national reporting platforms on their webpage.

From our national experience having had a Single Reporting Platform since 2018, we have built it as a platform where incidents related to cybersecurity and digital legislation (from NIS 2, GDPR, eIDAS, DORA, PSD2 and the National Law Enforcement Act) can be reported once – in either English or Danish – based on a dynamic template that changes depending on the type of incident. The platform then forwards the report to the relevant competent authorities and only keeps an encrypted version of the report for 90 days. That way the platform is not as interesting a target for malicious actors. The report is handled by the national CSIRT and the relevant competent authorities in their own secured systems.

Regarding the Net and Information Systems Directive (NIS 2)

Information needed for registration: In Article 27 there is an obligation for competent authorities to maintain a register of entities within the scope of the Directive. This register is intended to support oversight, incident response, and risk management. However, the information currently required for inclusion in the register could be reviewed as to its necessity e.g. IP-intervals. IP-intervals has proven harder to acquire for some entities than expected and created a degree of delay in the registration process.

Interpretation of sector definitions While the Directive rightly seeks to strengthen the overall level of cybersecurity within the Union, certain sectoral definitions — for instance within the digital sector — are broad and to some degree ambiguous. In particular, the categories of cloud computing service providers, managed service providers, and managed security service providers would benefit from more precise delineation. At present, the Directive leaves room for interpretation, and providing alignment in interpretations among member states would be a contribution of significant value.