European Data Centre Association

Feedback on the draft implementing regulation on Cybersecurity risk management & reporting obligations for digital infrastructure

Executive Summary

The European Data Centres Association (EUDCA) has been representing the interest of data centre operators in Europe since 2011. The EUDCA is the voice of the data centre industry, with a diverse membership which includes European and international operators, vendors, and a network of national trade associations. The EUDCA welcomes the specifications, that the European Commission has laid out, on the NIS2 reporting requirements and risk-management measures that data centre operators will need to incorporate into their operations but is under the impression that both have the potential to lead to an increase in the administrative burden for data centre operators. Additionally, the current implementing regulation does not specify the differences between the different data centre business models and thus colocation data centre operators are at risk to breach the confidentiality agreements with their clients.

Thus, the EUDCA requests the Commission to

- Align the risk-management measures laid out in the Annex of the Implementing Regulation with international standards, such as ISO 27001;
- Provide a guidance statement and mapping tool for the organisations' reference and usage to check common control requirements and focus on the gaps which are not covered as a part of existing ISO 27001 certification scope;
- Implement the existing definition for co-location data centres of the delegated regulation C(2024) 1639;
- Issue clarification documentation for Art. 8 a), b), c) to limit the scope of reporting incidents to severe infractions of customer SLAs.
- Remove the reporting requirement under Art. 8 d) for colocation data centre operators.

Feedback on the different articles

Technical and methodological requirements – Art. 2 and Annex

The EUDCA welcomes the clarification of the Technical and methodological requirements for the purpose of Art. 21 II a) to j) of the NIS2 Directive. The requirements that the Commission has laid out are very detailed and specify many of the already existing security measures that data centres have already put into place. The measures laid out in this regulation have the potential to lead to a doubling of the administrative procedures, as data centres often are already required by their customers to certify against existing international cybersecurity standards. The most pertinent certification in this area, that European data centres are receiving third-party verification for, is ISO/IEC 27001, a standard laying out a structured risk management framework and reporting procedures. The ISO norm establishes guidelines on how to develop, maintain, operate and improve an Information Security Management System (ISMS), which has a comparably extensive scope as laid out in the implementing regulation at hand. The norm focuses on identifying and mitigating reasonably foreseeable threats to create a robust and reliable digital infrastructure.

Additionally to the ISMS, ISO 27001 also includes a reporting policy for security incidents. Whilst the standard does not introduce a reporting requirement to any authorities, it lays out a structured response plan. This plan needs to include clear guidelines for identifying, containing, reporting, and recovering from cybersecurity incidents. This plan can be the basis of the technical and methodological requirements. To limit the administrative burden on operators, the European Commission has the possibility to adopt ISO 27001 and similar standards as equivalent to the requirements of the annex of this implementing regulation and develop a guidance document on the gaps that operators will need to address before fully complying with the requirements of this regulation.

- Align the risk-management measures laid out in the Annex of the Implementing Regulation with international standards, such as ISO 27001;
- Provide a guidance statement and mapping tool for the organisations' reference and usage to check common control requirements and focus on the gaps which are not covered as a part of existing ISO 27001 certification scope;

Reporting of significant incidents for data centre providers – Art. 3 and Art. 8

As a fundamental part of Europe's sovereign digitalisation strategy, colocation data centre operators have established a strong and secure digital infrastructure that its clients can reliably and anonymously utilise across Europe, whilst remaining in full control of their data and IT equipment. In their contracts, colocation data centre operators guarantee the anonymity of the data and IT processes of their clients and do not interfere with the data transmission process. They guarantee that at no point they will access the servers and have no ability to collect data related to the clients' processes. Most of the reporting requirements laid out in Art. 8 for data centre providers (Art. 8 b), c), e)) can be tracked and reported to the respective national authorities. However, the current phrasing of this article (Art. 8 a), b), c)) encompasses all infractions regardless of size and impact. It should be clarified that only severe deviations from key obligations under the customer service level agreement trigger the incident reporting obligation to avoid an unnecessary burden on the operator.

Additionally, the requirement on reporting compromised data traffic or storage (Art. 8 d)), due to a digital security failure, is outside of the scope of observation for colocation data centres. The definition utilised for "data centre services" in the NIS 2 directive unfortunately does not add a differentiation for colocation data centre operators and treats them the same as other data centre operators, which are in control of the IT services. This leads to a lack of distinction between incidents stemming from either infrastructural or digital issues. This is eventually bound to create a significant and unenforceable administrative burden, by forcing operators to report incidents, which do not impact the security of the data. Furthermore, this has severe implications on the legality of reporting incidents and enforceability.

Due to the contractual relationship between colocation operators and its clients, operators are unable to force their clients to report such incidents to them and are often even unaware of the incidents happening on the digital service level. As the regulation currently stands, the reporting obligation would however fall on the data centre operator to report these. Thus, we would like to reiterate our strong conviction that regulations should not require data centre operators to report matters outside of their control. Due to the anonymity of a client's operator and the strict separation of the colocation operators from the clients' servers, colocation operators are unable to enforce the incident reporting from significant incidents, occurring in the IT equipment and during the operation of IT services. To avoid any national legal conflicts and stay consistent with other existing European legislation, the EUDCA proposes to introduce a distinction for colocation data centre operators, by utilising the definition of colocation data centres from the delegated regulation C(2024) 1639 and removing their requirement to report on Art. 8 d).

- Implement the existing definition for co-location data centres of the delegated regulation C(2024) 1639;
- Issue clarification documentation for Art. 8 a), b), c) to limit the scope of reporting incidents to severe infractions of customer SLAs.
- Remove the reporting requirement under Art. 8 d) for colocation data centre operators.