Message 301

Communication from the Commission - TRIS/(2024) 2490

Directive (EU) 2015/1535

Notification: 2024/0420/DE

Request for supplementary information from the Commission.

Request for supplementary information - Demande d'informations complémentaires - Žádost o doplňující informace - Ersuchen um ergänzende Informationen - Искане за допълнителна информация - Žádost o dodatečné informace - Anmodning om supplerende oplysninger - Αίτηση συμπληρωματικών πληροφοριών - Solicitud de información complementaria - Lisateabe edastamise palve – Lisätietopyyntö - Zahtjev za dodatne informacije - Kiegészítő információ kérése - Domanda di informazioni complementari - Prašymas pateikti papildomos informacijos - Papildu informācijas pieprasījums - Talba għal tagħrif addizzjonali - Verzoek om aanvullende inlichtingen - Prośba o uzupełnienie informacji - Pedido de informações complementares - Solicitare de informații suplimentare - Žiadosť o ďalšie informácie - Zahteva za dodatne informacije - Begäran om kompletterande upplysningar - Iarraidh ar fhaisnéis fhorlíontach

MSG: 20242490.EN

1. MSG 301 IND 2024 0420 DE EN 24-10-2024 17-09-2024 COM INFOSUP COM 24-10-2024

2. Commission

3. DG GROW/E/3 - N105 04/63

4. 2024/0420/DE - SERV60 - Internet services

5.

6. In the context of the notification procedure under Directive EU 2015/1535, the German authorities have notified the Commission the Draft Act transposing the NIS 2 Directive and regulating essential features of information security management in the federal administration (NIS 2 Transposition and Cybersecurity Enhancement Act).

In that regard, the Commission would like to better understand the relationship between § 41 of the draft BSI Act and the recently agreed Cyber Resilience Act (CRA). The CRA follows the principle of maximum harmonisation, preventing Member States from impeding, for the matters covered by the CRA, the making available on the market of products with digital elements compliant with the CRA. § 41 (2) of the draft BSI Act provides for the possibility to prohibit the use of critical components in certain cases. In addition, § 41 (2) requires manufacturers to make a declaration of trustworthiness (‘Garantieerklärung’) to the operator and also includes an empowerment for the Ministry of the Interior to define minimum requirements for the declaration of trustworthiness. The Commission would therefore greatly appreciate the following clarifications:
1) How are products with digital elements designated as critical components? Do designations only relate to a narrow set of operators or do they cover wider parts of the national market of those products?
2) To which extent does a prohibition to deploy a product with digital elements as critical component affect the ability of the manufacturer to place that product on the German market? How does § 41 (2) interact with Article 4 (“Free movement”) of the CRA, which prevents Member States from impeding the making available on the market of products with digital elements which comply with the CRA?
3) What types of minimum requirements can be imposed by the Ministry of the Interior in relation to the declaration of trustworthiness? Can these requirements exceed the obligations and essential cybersecurity requirements laid down in the agreed Cyber Resilience Act?

Moreover, the Commission would appreciate clarifications concerning the transposition of the Directive (EU) 2022/2555 (NIS 2 Directive) with regard to the following provisions:

4) Article 6(29) of the NIS2 Directive contains a definition of Domain Name System (DNS). While the implementation in § 2 of the draft BSI Act takes up all DNS-related definitions, this definition seems to be missing. What is the reasoning behind? Is it defined in any other legislation that is quoted in the text?
5) Article 28(5) of the NIS2 Directive requires that a response to all access requests is given in all cases and within 72 hours; it further specifies that access to data shall be granted to legitimate access seekers. Article 50 (1) of the draft DE law imposes replies within 72 hours to legitimate access seekers. How would the replies to other requestors who are not listed as legitimate access seekers be covered under this obligation?
6) Article 50 (1) of the draft DE law specifies that "if the requested information is not available, this shall be notified within 24 hours of receipt of the request for access." How would the obligation to provide access to legitimate access seekers be fulfilled in these cases?
7) In the "explanatory note" Re Section 51 (Obligation to cooperate) implementing the Article 28(6) of the NIS 2 Directive it is stated: " Registration data shall not be collected, verified and stored twice. The obligation to cooperate ensures the fulfilment of the obligations without duplication of databases. An obligation to run double databases would lead to a significant outflow of registration data to non-EU countries, as a large number of registries and registrars are based there". While it is clear that there is no obligation for TLD registries and entities providing registration services to have separate databases, is it the intent to forbid ex ante the possibility to have separate databases? Under this circumstance, would the entity that does not have a database be allowed to access the database for the purpose of addressing access requests?

The German authorities are kindly requested to respond by 27 September 2024.

****

Mary Veronica Tovsak Pleterski
Director
European Commission

Contact point Directive (EU) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu