Message 001

Communication from the Commission - TRIS/(2026) 1353

Directive (EU) 2015/1535

Notification: 2026/0248/DE

Notification of a draft text from a Member State

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta’ dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20261353.EN

1. MSG 001 IND 2026 0248 DE EN 19-05-2026 DE NOTIF

2. Germany

3A. Bundesministerium für Wirtschaft und Energie, Referat EB3

3B. Bundesministerium des Innern, Referat CI 1

4. 2026/0248/DE - SERV60 - Internet services

5. Act to Strengthen Cybersecurity (Article 4 – Amendment to Section 19 of the Telecommunications, Digital Services Data Protection Act)

6. Digital service providers are obligated, in addition to the existing regulations for telecommunication service providers in the Telecommunications Act (TKG), to inform their users about disruptions (Paragraph 5) or specific threats (Paragraph 6) emanating from one of their services.

7.

8. With the newly introduced Paragraphs 5 and 6 of Section 19 of the Telecommunications, Digital Services Data Protection Act (TDDG), digital service providers are required to inform their users about disruptions (Paragraph 5) or specific threats (Paragraph 6) arising from one of their services, and to pass on information from the Federal Office for Information Security (BSI) about specific threats affecting the providers' customers to their users, insofar as this information is known and notification is possible.
Paragraphs 5 and 6 only cover those disruptions or threats emanating from a service during the user´s use of that service. This refers to cases where a user, for example, uses a hosting service to operate a website or email service, and the website or email service for which they are responsible is compromised and misused in order to distribute malware or phishing emails. It therefore concerns disruptions and threats that affect a user when they are using a service. Possible examples of relevant disruptions include a compromised email account used to send spam; a compromised server used for DDoS attacks; or a compromised website used to distribute malware.

The purpose of this obligation is to prevent damage caused by vulnerable or already compromised services. This kind of damage can occur to the user themselves as well as to other internet users if they are attacked via the affected services (e.g. malware, phishing or DDoS attacks). In addition, digital service providers are obligated to notify those users whose use of the services are causing a disruption or for whom there is a threat – insofar as this is known – and to forward to these users any information transmitted by the Federal Office for Information Security (BSI).

9. The obligations in Paragraphs 5 and 6 essentially correspond to those already existing for telecommunications service providers in Section 169, Paragraphs 5 and 6, of the Telecommunications Act (TKG).

9a. The existing obligations of telecommunications service providers under Section 169, Paragraphs 5 and 6, of the TKG leave gaps in addressing corresponding threats, as systems whose operators are not subject to the TKG are regularly affected. However, the Federal Office for Information Security (BSI) processes on a daily basis numerous findings on vulnerable or compromised systems (hosting providers, cloud computing service providers, data centre service providers, content delivery network operators, managed service providers, managed security service providers).

9b. Although these findings are currently forwarded to the providers, they are very often not passed on to the affected users by the service providers due to a lack of legal obligation. The existing threat cannot therefore be regularly effectively addressed.

9c. No, the prevention of excessive burden is addressed through the limitations on technical feasibility and economic reasonableness in the regulatory framework.

10. Reference to the basic texts: No basic text available

11. No

12.

13. No

14. No

15. No

16.
TBT aspects: No

SPS aspects: No

****

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