Draft Act from the Federal Ministry of the Interior

Draft of an act to strengthen cybersecurity[1]

Dated ...

The German Federal Parliament (Bundestag), with the consent of the German Federal Council (Bundesrat), has passed the following act:

[…]

Article 4

Amendments to the Act on Data and Privacy Protection in Telecommunications and Digital Services

The Telecommunications and Digital Services Data Protection Act, of 23 June 2021 (Federal Law Gazette I p. 1982; 2022 I p. 1045), as last amended by Article 3 of the Law, of 10 March 2026 (Federal Law Gazette 2026 I No 64), is amended as follows:

1. after Section 19, Paragraph 4, the following Paragraphs 5 and 6 are added:

(1) ‘ If a digital service provider becomes aware of a disruption emanating from one of its services during a user's use of the service, it must immediately notify the user of this, provided that the user's identity is known. Insofar as technically possible and economically reasonable, the provider must, within the scope of its respective responsibility for commercially provided digital services, inform the user of appropriate, effective and accessible technical means by which they can detect and resolve the disruption. If the provider has been notified of the disruption by the Federal Office for Information Security (BSI), the provider must forward to the user all information provided in the disruption notification that can be used to detect and resolve the disruption. The provider may redirect portions of the data traffic to and from a service being used that is experiencing a disruption, insofar as this is necessary in order to notify the user of the disruption.

(2) If a digital service provider is informed by the Federal Office for Information Security (BSI) of specific threats to information technology security emanating from or affecting a user's use of one of its services, it must immediately notify the user thereof, provided that the user's identity is known. In doing so, the provider must, in particular, forward to the user all the information contained in the notification from the Federal Office for Information Security (BSI) pursuant to Sentence 1 that enables the threats to be identified and prevented. If a digital service provider becomes aware of threats to information technology security emanating from or affecting the user's use of one of its services, it may notify the user thereof. Where technically possible and economically reasonable, the provider may advise the user of appropriate, effective and accessible technical means by which they can identify and prevent these threats.’

[…]

[1] Article 4 of this Act is notified in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council, of 9 September 2015, laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

Justification

B. Special part

Re Article 4 (Amendments to the Act on Data Protection and Privacy Protection in Telecommunications and Digital Services)

Re Point 1

With the newly introduced Paragraphs 5 and 6, digital service providers are required to inform their users about disruptions (Paragraph 5) or specific threats (Paragraph 6) emanating 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.

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 TKG. 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). 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.

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).