Proposed German Regulations To Require Additional Security Measures for Telecom Carriers

November 14, 2019

Editor's note: CommLaw Monitor primarily addresses developments in communications and technologies in the United States. We provide this special update regarding new regulations in Germany for the benefit of U.S. and foreign service providers alike. The security issues discussed below may have implications for all service providers.

The German Federal Network Agency, Bundesnetzagentur (BNetzA), recently launched a final public consultation on its new draft Catalogue on security requirements for telecommunications service providers and operators of public telecommunications networks. The draft is revamped significantly, but follows the same vein as its predecessors to prevent disruptions and manage security risks, by requiring providers and operators to implement technical security measures and safeguards for operating telecommunications and data processing systems. The deadline for comments on this version 2.0 of the Catalogue is 13 November 2019, but the BNetzA is unlikely to make fundamental changes at this late stage. Consequently, stakeholders should consider the draft as a reliable indicator of the official version, and assess how to best satisfy the requirements.

The Catalogue will have the authority of soft law once published, because its content constitutes recommendations that the BNetzA inferred from law. Deviation from the Catalogue therefore is an option. However, any divergence will have to be necessary and reasonably justified, as audits on security measures will use it as a benchmark.

The following non-exhaustive list provides details of the expected additional security requirements:

- **Network traffic must be constantly monitored for any abnormality** and, if there is any cause for concern, appropriate protection measures must be taken (e.g. network traffic stopped, traffic to the source of interference restricted or stopped). The detection measures must be state-of-the-art.

- **Security-related network and system components (critical key components) may only be used if they have undergone IT security checks by a Federal Office of IT Security, Bundesamt für Sicherheit in der Informationstechnik (BSI), approved testing body and have been certified by the BSI.** Critical key components may only be sourced from those suppliers/manufacturers that can provide assurance of their trustworthiness in an appropriate manner. This obligation applies to the entire supply chain and is a requirement for the necessary certification of components. These requirements will be set out in more detail in the Catalogue. The underlying standards will be published by the BSI in consultation with the BNetzA. The competent ministries are drawing up appropriate legal safeguards, notably as part of the ongoing major amendments to the German Telecommunications Act, to ensure the binding nature of the requirements and to secure specific requirements legally and

unambiguously, such as the duty of certification.

- The network and system components that are security-related (critical key components) will be determined by the BSI and BNetzA by mutual agreement (when drawing up the Catalogue).
- **Security-related network and system components (critical key components) may only be used following an appropriate acceptance test upon supply and must be subjected to regular security tests.** If any deviations from the service specifications of the network operator or provider arise during the tests, these deviations must be documented and undergo a risk treatment process. Any measures taken to minimise risks from deviations that could have a significant impact on telecommunications networks and services must be notified to the BNetzA and the BSI without undue delay.
- ,**Only trained professionals with in-depth knowledge of systems may be employed for the assessment of risks and protection measures in security-related areas.** A sufficient number of such professionals must be kept available.
- Proof must be provided that the hardware tested for the selected, security-related components and the source code at the end of the supply chain are actually deployed in the products used.
- When planning and building the network, sufficient diversity must be ensured by using network and system components from different manufacturers. This requirement will be defined by the BNetzA and could vary between different networks, for example, between the core and access networks.
- Where system-related processes are outsourced, the network operator and provider must ensure that independent, professionally competent and reliable contractors are selected and that compliance with statutory requirements remains guaranteed. The network operator and provider must provide evidence of this.
- Adequate redundancy must be available for critical, security-related network and system components (critical key components). A list of particularly critical network components is being drawn up in this regard (e.g. home location register, core network, backbone, porting server).
- When implementing the security requirements, national security regulations and regulations for the secrecy of telecommunications and for data privacy protection must be met.

The Catalogue is expected to be published before the end of the year. A future law will make mandatory Annex 2 of the Catalogue, which contains additional requirements for networks and services subject to “increased risk potential.” BNetzA’s definition contains abstract and concrete parts. It encompasses all suppliers within the industry and technology sector considered prominently important to the public interest or the BNetzA. The definition also includes all mobile networks with more than 100,000 subscribers, and suppliers using critical components. Components are particularly critical if a technical compromise leads or can lead to significant data breaches (e.g., automated mass data exploitation in the sense of Big Data application); systematic exploration of telecommunications; or substantial security breaches. A list of critical components will be published in an initial form no later than 1 January 2020.

There currently is not an English text available. The German text can be found here.