Hinweis: Nachfolgende nichtamtliche Übersetzung wird nur hilfsweise bereitgestellt!

Note: The following translation is unofficial and is provided as a convenience for the reader.

Federal Ministry of the Interior, Building and Community

General order

concerning the details of the minimum requirements for the declaration of guarantee (prohibition of the use of critical components) for the telecommunications industry, to be defined pursuant to section 9b (3) sentence 4 of the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, BSIG)

of 7 October 2021

I.

In the telecommunications industry, critical components as referred to in section 2 (13) of the Act on the Federal Office for Information Security are those which fulfil the critical functions defined in section 109 (6) sentence 1 no. 2 of the Telecommunications Act (*Telekommunikationsgesetz*, TKG). The declaration of guarantee that must accompany the notification of the planned use of such a critical component in accordance with section 9b (1) sentences 1 and 2 of the Act on the Federal Office for Information Security must contain, in addition to the content required by section 9b (3) sentence 3 of the Act on the Federal Office for Information Security, the following statements in German by the manufacturer:

1. a commitment to cooperate, for as long as the critical component is in use, with the operator of the critical infrastructure, with the Federal Office for Information Security and with the Bundesnetzagentur with regard to the security of the critical component; to provide information related to the production and the operation of the critical component; to provide the necessary support; and to enable the operator of the critical infrastructure to audit the information security management system of the critical component;

2. a commitment to assist the operator of the critical infrastructure as appropriate and to the extent necessary when conducting security checks and penetration analyses of the critical components;

3. a commitment to notify the operator of the critical infrastructure sufficiently in advance of planned changes to the production and provision of security-relevant parts of the system; and, at the request of the operator of the critical infrastructure, to provide specific information about the product development of the security-relevant parts of the critical components used;

4. a commitment to notify the operator of the critical infrastructure immediately of any vulnerabilities in the critical component as soon as they are detected. This notification must be sufficiently detailed so that the operator is able to take the necessary action to contain and remedy any harmful consequences;

5. a commitment to apply a suitable information security management system for the critical components. This system must make it possible to archive the relevant firmware and software versions of the critical components so that they cannot be manipulated and can be reviewed as appropriate; a commitment to provide appropriate access to these archives in the event of a security incident. This includes in particular documenting all relevant product- and process-related information, including the firmware and software versions used and information from external sources (such as data sheets); protecting this information according to the state of the art against unintentional changes; monitoring changes; and documenting them in readable form for at least as long as the critical components are in use;

6. a declaration, whether and if so, in what way it is possible, based on the company's existing structure (shareholder structure, participating interests), for the government, government agency or military of a country that is not a member state of the European Union to influence the security, confidentiality, integrity, availability or operability of the critical infrastructure, in violation of the law applicable to the company or in fact;

7. information about the company's headquarters (including its complete business address) and about its structure; its number in the commercial register, tax registration number and EORI number, if applicable; the complete names, addresses and birthdates of the company's management team and other authorised representatives; company names must also be written in the characters used in the company's place of business;

8. an assurance of the ability in law and in fact to refuse to disclose confidential information about operating processes, confidential information gained during operating processes, and confidential information about the operator of the critical infrastructure. This includes in particular the assurance that, at the time the declaration is made, the provider of the declaration is under no obligation to disclose such information to third parties or otherwise make it available to them. This assurance does not extend to legal obligations to disclose information to German law enforcement authorities. This assurance covers obligations to disclose information to foreign intelligence services, law enforcement or security authorities or other government or private foreign entities; in case of doubt, these obligations must be reported;

9. a commitment to inform the Federal Ministry of the Interior, Building and Community and the operator of the critical infrastructure immediately if it is no longer possible to honour the declaration of guarantee due to changed circumstances or other information acquired by the manufacturer.