WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

eco main criticism of the notified draft security catalogue according to § 109 (6) TKG to the EU Commission – Notification No. 2020/496/D

Berlin, 28.09.2020

The Bundesnetzagentur (German Federal Network Agency - BNetzA) has issued the draft security catalogue in agreement with the Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security - BSI) and submitted it to the EU Commission for notification. The catalogue shall set the security requirements for the operation of telecommunications and data processing systems as well as for the processing of personal data, and the establishment of security concepts are to be based on the catalogue.

eco and its member companies share with the competent authorities the interest in improving and strengthening the IT security of telecommunications networks and services. In the context of the notification procedure, we would like to express our main criticisms regarding the draft submitted in terms of the compatibility of the security catalogue with European law and principles. In addition, we would like to refer to our detailed opinion on the draft for a security catalogue.

▪ No legal certainty due to planned changes

I. a. § 109 TKG is to be amended. Paragraph 6 of this regulation is to be the legal basis for the notified draft. The regulation is to be amended in such a way that it forms a regulatory complex together with the future BSI Act, a future general decree of the Federal Ministry of the Interior (details on written guarantee), the future list of BNetzA/BSI (draft in national consultation) and a future technical guideline (TG) of the BSI (for list and TG see no. 8 of the Notification Message). This planned regulatory complex will create significant legal and planning uncertainty for the providers concerned. This constitutes an unjustified encroachment of the freedom to conduct a business under Article 16 of the EU Charter of Fundamental Rights.

▪ Compatibility with Cyber Security Act questionable

eco considers that it is possible that the application of the notified draft will not be in accordance with the Cyber Security Act (CSA), EU Regulation 2019/881. The BNetzA and the BSI have a very wide scope for interpretation and application outside the CSA. In addition, global and international standards, such as 3GPP, are not taken sufficiently into account.

▪ Breach of the EU Single Market Principle

eco sees the requirements of Annex 2 of the security catalogue as representing a breach of the freedom to provide services in accordance with Art. 62, Art. 53(1) TFEU, specified in greater detail by Directive 2006/123/EC. The strict requirements of BNetzA represent very high obligations for 5G providers who operate or plan to operate across the EU to purchase technical components in accordance with German requirements, although other Member States impose different requirements. The products and services of the German 5G network operators would

become more expensive throughout Europe, as companies are in fact forced to install and use components in their telecommunications infrastructures throughout Europe that meet German security requirements. This also distorts competition, as 5G providers from other EU Member States with significantly lower security requirements can offer their services at significantly reduced rates. A factual justification of this indirect discrimination is not apparent, as the requirements of BNetzA exceed the necessary measure.

- **Impact of international trade not sufficiently taken into account**

Contrary to the national authorities' assessment, the draft submitted violates the Agreement on Technical Barriers to Trade Agreement, see No. 16 Notification Communication. It is a protectionist measure whereby manufacturers are excluded from the German market in the event that the specifications of the catalogue and its systems are not complied with. The scheme is based on presumptions regarding certain producers and no actual evidence. Principles of the rule of law require that conjecture cannot be the basis for the withdrawal of trust, especially geostrategic, commercial, geopolitical, foreign policy, or other political considerations, which are all extraneous to the topic.

- **Declaration of trustworthiness infringes General Principles of EU law**

Terms such as third parties, security authorities, confidential information are too indeterminate. Some points cannot be signed or guaranteed by any manufacturer, and are therefore legally impossible. This is an infringement in the freedom to conduct a business that goes beyond what is absolutely necessary. The requirements are also not in line with the objectives of the planned E-Evidence Regulation. However, Member States are also obligated to respect the Effet Utile, if they can foresee that national rules are incompatible with an EU regulation that has already adopted concrete forms, as e-evidence has done. In this case, the EU Member States are obliged to take the forthcoming regulation into utmost account.

- **Breach of notification obligation or national law**

The List of the BNetzA/BSI and Technical Guideline of the BSI are either a legal part of the Security Catalogue (administrative act in the form of the General Decree), in which case, there would be at least one legal basis with § 109 (6) TKG, and they should have been notified. As this was not done, the BNetzA would, in this case, have infringed the TRIS-Directive EU/2015/1535. However, if both are not legal part of the security catalogue, there is no legal basis for either of them, either in EU or national law. This is a clear violation. In this case, the EU Commission is required to request Germany to amend or withdraw the notified draft. Otherwise, the TRIS procedure would be conducted ad absurdum. It would have to be carried out again after the draft has been repealed. The adoption by the EU-Commission of a draft manifestly contrary to national law would also not correspond to the Effet Utile pursuant to Art. 4 (3) TEU with regard to Directive EU/2015/1535.

- **Protection of confidence not guaranteed**

There is no sufficient legal basis in EU or German law for the obligation to remove individual components from the network (2.4 of the draft, p. 66), if the certification is subsequently withdrawn on the basis of an official decision. Such a legal basis would also have to comply with

the Parliament's reservation of intervention. Furthermore, it remains open how to grant legal protection to affected network operators if they are to be obliged to replace individual components, should the certification of the component cease after installation. The network operators are not the addressees of the certification obligation, but the manufacturers. The decisions that could lead to the elimination of certification are also not readily accessible to network operators. The comprehensibility of the administrative action of the certifying authority is also open, because often intelligence information that is inaccessible to the authority is likely to play a role. In addition, this is an interference in the ownership of the network operator, for which the operator has given no cause and is not responsible. For this purpose, the network operator concerned must be compensated by the State, as in the case of an equal measure of expropriation. Such a compensation rule has not yet been provided for.

- **Hearing did not take place**

There has been no hearing for the draft notified here. The only hearing that has taken place was on a draft security catalogue, held in autumn 2019. However, that draft differed in substantial ways and to a considerable extent from the notified draft. Therefore, there was no consultation on the draft submitted for notification before it was notified. This constitutes a violation of Article 41 (2) lit. a) of the EU Charter of Fundamental Rights.

- **Longer implementation deadlines offered for OTT providers**

With the implementation of the EECC into national law, it is already foreseeable that the number of parties subject to obligations with regard to the security requirements as set out in § 109 paragraphs 6, 4, 2 and 1 TKG is going to increase significantly, e.g. to OTT providers. The BNetzA grants traditional telecommunications companies one year from the publication of the catalogue, e.g. on page 65. This deadline is aimed at traditional telecommunications companies that already have practical experience and knowledge regarding security requirements. On the other hand, this does not apply to the OTT providers facing their first obligation in this regard. The predetermined security requirements are complex, comprehensive and difficult to implement. Accordingly, the OTT providers must first develop a sufficient understanding of the technical requirements and develop a corresponding implementation concept which is adapted to their individual requirements and circumstances. This requires an appropriate deadline for implementation. We propose a deadline until 31.12.2025, as on page 65 of the notified draft. In the opinion of the eco, this requires the principle of proportionality in accordance with Article 52 (1) sentence 2 of the EU Charter of Fundamental Rights.

About eco: With over 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. eco's key topics are the reliability and strengthening of digital infrastructure, IT security, and trust, ethics, and self-regulation. That is why eco advocates for a free, technologically-neutral, and high-performance Internet.