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

eco

eco Opinion for the EU Commission on the notified Security Catalogue Pursuant to § 109 (6) TKG – Notification No. 2020/496/D

Berlin, 28.09.2020

The Bundesnetzagentur (German Federal Network Agency) has issued the draft of a security catalogue. It is intended as a specification of the security requirements for the operation of telecommunications and data processing systems as well as for the processing of personal data. It is to be considered when designing security concepts.

eco and its member companies share the interest in improving and strengthening the IT security of telecommunications networks and services with the competent authorities.

I. In General

In the following, we would like to take the opportunity to address in detail the essential aspects of the revised draft security catalogue once more, which has been submitted to the European Commission for notification.

eco regards it as positive that the Bundesnetzagentur (BNetzA) has chosen a more appropriate approach with more differentiation than first proposed in the autumn 2019 draft. However, it is to apprehend that the obligations for all telecommunications network operators and providers of such services will become even stricter in the foreseeable future. In the course of implementing the European Code of Electronic Communications (EECC), the German Telecommunications Act (TKG) is to be revised entirely. As far as currently known, this includes a revised version of § 109 TKG, whose paragraph 6 is the legal basis of the draft in the notification procedure. This revision provides clear aggravations. I. a., for a significantly stricter framework. A very complex set of regulations on various laws in addition to TKG is envisaged, inter alia, including a general decree of the German Federal Ministry of the Interior (BMI) and further other administrative regulations. With regard to these proposed legal changes, it seems that the notified draft intends to take these (amendments) into account in advance, e.g. a Technical Guideline of the German Federal Office for Information Security (BSI), see Section IV below.

eco considers the adoption of the catalogue of security requirements prior to the entry into force of related new regulations, which are to be concretised by the catalogue and which form the legal basis for the catalogue, to be inadmissible. This approach does not provide the network operators and service providers any certainty in relation to planning, investment, and legal considerations. eco, therefore, demands the publication of all planned new regulations, so that a holistic assessment and commentary can be made by the companies concerned. Furthermore, we consider the draft to be an unjustified infringement of the freedom to conduct a business in accordance with Article 16 of the EU Charter of Fundamental Rights,

thus the planned requirements go far beyond what is necessary to ensure the security of telecommunications systems and services and are partly based on considerations out of topic.

II. Scope unclear

The draft uses the term “increased criticality”. The draft list (see No. 16 Notification Message) speaks of, on the other hand, refers to “increased risk potential”. It should be clarified whether these two different terms are intended to refer to different areas of application. If that is not the case, it would be useful to use the same term in both documents. Also, the titles of Annex 2 of the Security Catalogue and the associated draft list are unclear. Both use the terms “increased risk potential”. Nor is it clear from the scope of the draft list to what it refers. It is only in the overall view of the draft Security Catalogue that it becomes clear that the section “increased criticality”, p. 37f, 5.1.3, in Annex 2 and the draft list addresses only 5G network operators. Linking and entangling these concepts thus so that the scope can only be understood after reading three separate pages is both unnecessary and unhelpful.

III. Compatibility with Cyber Security Act questionable

In eco’s opinion, the application of the notified draft can be inconsistent with the Cyber Security Act (CSA), EU Regulation 2019/881. Where certification schemes under the CSA are not available, there is a proviso that “mandatory network operators and service providers must temporarily take other appropriate and reasonable technical and other security measures when using critical components to avert risk”, see p. 65, 2.4. These are further very vague terms which the Bundesnetzagentur may interpret in addition to those of Section 109 TKG. However, the indeterminate legal terms in § 109 TKG are supposed to be concretised by the Security Catalogue. Moreover, the term of “danger defence” is not sufficiently limited to the purpose of § 109 TKG, which are technical protective measures for networks and telecommunications services. Also, global and international standards, such as 3GPP, are not taken sufficiently into account.

The BSI shall be authorised to adopt a Technical Guideline (TG) on components in networks with increased criticality, see Notification Message no. 8: “This (TG) contains requirements for the certification of critical components, including requirements for the operational environment and operation as a prerequisite for the validity of certificates. It also describes requirements for the certification of certificates according to European certification schemes (CSA).”

Given this, eco considers it very important that the EU Commission and ENISA carry out their monitoring tasks with regard to EU-compliant application by Bundesnetzagentur and BSI.

IV. Breach of the EU Single Market Principle

eco considers the requirements of Annex 2 of the Security Catalogue to be a violation of the EU single market principle, in the sense of unjustified infringement of the freedom to provide services according to Art. 62 in conjunction with Art. 53 (1) TFEU, concretised by Directive 2006/123/EC. By imposing such high requirements on 5G providers, all of which are active or planning to be active throughout the EU, the Bundesnetzagentur is effectively forcing these providers to purchase technical components in line with German requirements, even though other Member States have different or lower standards. In eco's opinion, this constitutes a discriminatory requirement as provided for in Art. 14 (1) of Directive 2006/123/EC. The Bundesnetzagentur is aware that the providers carry out purchasing on a group-wide basis in order to operate economically and stay competitive. In doing so, the agency is indirectly exploiting the factual constraints imposed by the market principles in question. This leads to indirect discrimination against German 5G providers. This unequal treatment is also not objectively justified. For this purpose, overriding reasons of general interest such as public safety would have to justify this indirect discrimination, see Art. 16 (1) lit. b) of Directive 2006/123/EC.

eco recognises the Bundesnetzagentur's efforts to increase public safety in electronic communications networks through the provisions in the notified draft. However, in many points and to a greater extent than required, e.g. the duty of notification regarding the installation of individual critical components (see section VIII below) and the obligation to remove them (see section IX below). Finally, in addition to ENISA's 5G Toolbox, the "IT-Grundschutzkompendium" of the BSI, and the list of the Bundesnetzagentur and the BSI, companies now should also observe the Technical Guideline of the BSI. This conglomeration of requirements is no longer manageable and does not serve security purposes.

Besides, the products and services of German 5G network providers are becoming more expensive across the EU, as companies are effectively forced to use components throughout the EU that meet German security requirements. The requirements set out by the Bundesnetzagentur are only intended to ensure that German 5G networks are secure. They must not, however, lead to a significant increase in the costs of network development throughout the EU, not even indirectly. This also leads to a distortion of competition, as 5G providers from other EU Member States with significantly lower security requirements can offer their services at significantly lower prices. There is no apparent objective justification for this indirect discrimination, as the Bundesnetzagentur's requirements exceed what is necessary, see the previous paragraph.

Ultimately, manufacturers of components who do not wish or are unable to comply with the requirements of the catalogue will be excluded from the German market without any objective justification for the exclusion. Indeed, as stated above, the requirements are not necessary, or not to the extent required, to ensure security.

V. Effects of international trade not sufficiently taken into account

In point 16 of the Notification Message on the notified draft, the German Federal Ministry for Economic Affairs and Energy (BMWi) concluded that there would be no impact on international trade. Specifically, this involves compliance with the World Trade Organization's "Agreement on Technical Barriers to Trade" (TBT Agreement). It aims, inter alia, to prevent unnecessary technical barriers to international trade and to prevent the adoption of protectionist measures. The notified draft does not meet this requirement. The draft provides for the point of trustworthiness together with many sub-aspects to be examined.

eco considers trustworthiness to be an important point in principle. However, this aspect plays a central role at a much earlier stage, namely before the conclusion of the contract between 5G mobile network operators and the manufacturers. None of these network operators would enter into a contract with a manufacturer they did not consider trustworthy, as network operators are very conscious of their responsibility towards customers and society.

With regard to the prevention of the adoption of protectionist measures, the rule of law dictates that assumptions cannot be the basis for the withdrawal of trust, and certainly not extraneous geostrategic, trade, geopolitical, foreign policy or other political considerations. Exclusion of an undertaking from a market must be based on verifiable facts, regardless of whether the State excludes the company itself or by imposing on network operators such strict conditions on manufacturers and suppliers that network operators refrain from using components from certain manufacturers. Unfortunately, eco sees this as a real imminent possibility in Germany.

VI. Declaration of trustworthiness causes concerns

The notified draft has unfortunately retained all the points from the draft of autumn 2019 unchanged, contrary to the justified criticism and the need for clarification. In eco's opinion, the draft therefore still does not sufficiently take into account that the legal framework of a country applies independently of individual manufacturers. This raises the question of whether such checks should not rather be carried out by a central authority. From eco's point of view, there is still a need for further clarification with regard to several terms and the concrete content of some subitems.

- To 3 No. 2: "No information from contractual relationships to third parties". Are customs and tax authorities of the country in which the source of supply is subject to custom duties and/or taxed to be considered third parties? eco suggests that an explicit clarification be made in the text that legal obligations to provide information, for example, regarding tax and customs, remain unaffected.

- As regards 3 Nos. 3ff: "confidential information". What is covered and what is not? eco suggests that the abstract wording should be substantiated by appropriate explanations, justification and concrete examples.

- Total at 3 No .4: In our view, no manufacturer can make this undertaking regarding the wording of this sub-item. Even in other European countries, unlike in Germany, there is no rule of separation between the police and the secret services, for example, in most of the Scandinavia countries, Switzerland, Austria and France. Outside the EU, none of the home countries of the large technology concerns, such as the USA or China, have such separation in law.

This means that it cannot be excluded that information which a manufacturer communicates to the competent law enforcement authorities for criminal prosecution purposes because of its statutory duty to provide information is not also accessible to the respective intelligence (secret) services. In addition to the above-mentioned legal obligations to provide information on customs and tax matters, there are many other legal obligations that are mandatory under European and international law, e.g. danger defence.

It is clear that almost all companies in the world, including European and American companies, are obliged to inform the secret services of their headquarters by order.

We refer exemplarily to the German legislation, which treats certain types of enterprises

— the BND pursuant to § 8 BND-G (https://www.gesetze-im-internet.de/bndg/__8.html),

— the BfV according to §§ 8, 8a, 8d BVerfSchG (https://www.gesetze-im-internet.de/bverfschg/)

— the LfVs (Bay.LVerfSchG, Art. 14-16 (https://www.gesetze-bayern.de/Content/Document/BayVSG)

— and the MAD pursuant to §§ 4a, 4b MAD-G (https://www.gesetze-im-internet.de/madg/)

obliged accordingly.

In Switzerland, the special obligation to provide information applies to companies in accordance with Art. 25 icw. m. Art. 19 of the Swiss Intelligence Act

(https://www.admin.ch/opc/de/federal-gazette/2015/7211.pdf, p. 9)In Austria pursuant to § 11 (1) no. 5 icw. m. § 6 of the Austrian Police State Protection Act – PStSG(https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2016_I_5/BGBLA_2016_I_5.pdfsig, p. 4).

In the context of the lack of the rule of separation in the above-mentioned states, we would also like to refer to the European legislative procedure for the so-called" e-Evidence Regulation". This planned set of rules is intended to give investigating authorities cross-border access to data. This would mean that, in view of the planned e-Evidence Regulation, no one would be able to fulfil the requirement of No. 4 in the future. In our opinion, there is already a general legal impossibility. In this respect, the term "security authorities" used in point 4 is far too vague. There is no legal definition of "security authorities" in the TKG. No matter what, this would not be sufficient, as the manufacturers in question are not subject to the TKG. This inaccuracy prevents obligated telecommunications companies from issuing a declaration of trustworthiness and also prevents the respective manufacturer from signing it.

A regulation which, however, does not allow any of the potential suppliers of suitable system components to make a legally compliant declaration is to be rejected, in eco's opinion. With regard to the advanced negotiations on an e-Evidence Regulation, eco also believes that Germany is prevented from issuing regulations that contradict the objectives of the proposed Regulation. This follows from the EU treaties, and in particular the Effet Utile pursuant to Art. 4 (3) TEU.

Besides, point 4 requires manufacturers to integrate technical methods/procedures into their products that enable operators to verify the integrity of the products. The inspection of the product should be carried out and documented during its entire life cycle. eco, therefore, doubts the appropriateness according to § 109 (2) TKG and the feasibility of this requirement due to the number of network and system components and their development dynamics.

An implementation of this requirement, which is currently not included in any product, would, for example, result in the complete, new development of core network components and management systems by every manufacturer and is estimated to take several years. At the same time, the effects on the existing processes customary in the industry with regard to delivery, storage, commissioning and replacement of components would be equally serious, as these would have to be developed from scratch and would also have to be reflected in the existing contractual relationships.

Accordingly, eco still considers a re-wording of 3 (4) to be urgently necessary, so that affected telecommunication companies can also actually and legally prepare a declaration of trustworthiness and the respective manufacturers can sign this declaration.

Finally, the aspect of the declaration of trustworthiness does not refer back to the deadlines specified in point 2.4 of the draft, p. 66. Because these two aspects are interconnected, there should be a link between them in the catalogue.

VII. Breach of notification obligation or national law

No. 8 of the Notification Message states that the Bundesnetzagentur and the BSI intend to jointly publish a "list of critical functions for public telecommunications networks and services with increased risk potential (supplement to Annex 2 of the Catalogue of Security Requirements)". In addition, the BSI is to issue a Technical Guideline on the "Certification of Telecommunications Components", since "security certification" by a recognised body is a particularly important component.

However, neither the draft list nor the BSI Technical Guideline were submitted to the EU Commission for notification.

a) List

Either the list is a legal part of the administrative act "Security Catalogue" (in the form of a general decree). If the list is part of this general decree, it is, like the Security Catalogue, subject to notification as a technical regulation under Directive EU/2015/1535. The fact that

the Bundesnetzagentur regards the list as part of a binding, concrete regulation of the individual case in the sense of a general ruling is shown by the many obligations of 5G network operators in Annex 2, e.g. the obligation to notify the installation of critical components, obligation by revoked certification after installation, etc., which BNetzA can order, but without the list there would be no subject to that order.

If, on the other hand, the list is not part of the general decree “Security Catalogue”, § 109 (6) TKG is not a legal basis for the adoption of the list. Moreover, there is no other legal basis for this list in the TKG. It was, therefore, a manifest infringement of national law. In this case, the EU Commission is obliged to request Germany to amend or withdraw the notified draft. The procedure for notifying technical regulations would be taken ad absurdum if the EU Commission were to accept obviously illegal national law of the member states. Following the repeal of the unlawful national act, the draft Security Catalogue would have to be notified again.

The adoption by the EU Commission of a draft that obviously violates national law would also not be in accordance with the Effet Utile pursuant to Art. 4(3) TEU in regard to Directive EU/2015/1535. The Effet Utile also binds the EU Commission under Art. 4(3) in conjunction with Art. 17(1)(2) TEU. It requires the enforcement of EU law in the way that best serves the purpose of the law in question. It is contrary to the purpose of the notification procedure of Directive EU/2015/1535 if manifestly unlawful national provisions are adopted without contradiction since this notification procedure would foreseeably have to be repeated for the same technical regulation.

b) Technical Guideline of the BSI

The same applies to the BSI Technical Guideline referred to in point 8 of the Notification Message. Either it is subject to notification because it is either part of the Security Catalogue or it is in obvious breach of national law. This is because § 109 (6) TKG is not a legal basis for the BSI to be allowed to issue a Technical Guideline on components in networks with increased criticality. This section only authorises the Bundesnetzagentur to issue the Security Catalogue. Even then, it would be necessary for the EU Commission to request Germany to amend or withdraw the draft in order to not draw out the TRIS procedure ab absurdum and to take the Effet Utile into account, see the previous point.

VIII. Obligation to notify installation of critical components illegal

In eco’s opinion, the obligation to notify the installation of critical components in 2.3 of Annex 2, p. 65 is illegal; both with regard to national law and EU law. Such an obligation to notify is to be regarded as an infringement in the sense of the national and European law, as the 5G network operators are considerably restricted and burdened in their entrepreneurial freedom by the notification of each affected component to both the Bundesnetzagentur and the BSI in their freedom to conduct a business the same time, as there are likely to be a very large number of components. These are encroachments on occupational freedom (Art. 12(1 GG), in conjunction with Art. 19 (4) GG, and on the right to an established and operating business

under Art. 14 (1) in conjunction with Art. 19 (4) GG, as well as the fundamental right, the freedom to conduct a business according to Art. 16 EU Fundamental Rights Charter.

Significant infringements by the state intervention must be based on a law passed by parliament (theory of materiality and parliamentary scrutiny reservation). As the obligation to notify does not fall within the competence of the EU, there is no EU legal basis, see Recommendation of the EU Commission 534/2019, 26.03.2019. The TKG does not provide a legal basis for an obligation to report the installation of critical components. At best, Section 109 (4)(5) TKG could be used for this purpose (Section 109 (6) TKG is the basis of the Security Catalogue).

However, § 109 (4) sentence 5 TKG only provides for the authority to request the Bundesnetzagentur to remedy deficiencies in the security concept or its implementation. This is an ex-post control. Either the security concept already exists and is being examined by the authorities, or its implementation is being monitored by the authorities. An advance (ex-ante) indication of individual components cannot be derived from this rule, and such an interpretation would violate the wording of § 109 (4) sentence 5 TKG. A historical interpretation also makes this clear. The reasoning of the law, when the rule was first introduced, states: “The regulatory authority may require rectifications if it recognises deficiencies,” see BT-Drs. 13/3609;P. 54.The BSI is not mentioned at all in § 109 (4) sentence 5 TKG.

In eco`s view, the EU Commission is also required with regard to this aspect to ask Germany to amend or withdraw the draft in order not to lead the TRIS procedure ad absurdum and to take account of the Effet Utile, see in detail above.

IX. Protection of confidence regarding built-in components not guaranteed

eco is very critical of the obligation to dismantle critical components in the event of subsequent revoking of certification by the authorities. A network operator concludes a contract for the supply of network components only with a manufacturer it trusts. The latter represents the basis for investment and for the installation of the components. However, the obligation in 2.4 of the draft, p. 66, means that network operators must remove individual components from the network in the event that certification is subsequently revoked due to an official decision. The draft also expressly points out that this requirement also applies to inventory components. Such an obligation to replace existing components constitutes an even more intense infringement than the obligation to notify (see point before) in the above-mentioned fundamental rights of companies.

The appropriate planning to maintain the operation of the networks, the installation of the replacement components – these are all very drastic measures which have a direct impact on the business and operational processes of the companies concerned. This is an “enteignungsgleicher Eingriff” similar to expropriation. Consequently, the regulatory authority must ensure adequate economic compensation in the event of a prohibition of the operation

of previously approved technical components, as the network operators do not give cause for the revoking of a certificate and reasons for this are not within its sphere of responsibility.

There is no legal basis in European law due to a lack of regulatory competence. Under certain circumstances, § 109 (4) sentence 5, second alternative TKG, could be a possible legal basis in national law. According to this, the Bundesnetzagentur can demand the immediate rectification of deficiencies if it detects such (deficiencies) in the implementation of the security concept. In turn, the security concept is to be issued by network operators on the basis of the Security Catalogue, see § 109 (4), (6) TKG. Both, the list of BNetzA/BSI and the technical guideline of the BSI (No. 8 Notification Message) are either could be considered part of the Security Catalogue.

If § 109 (4), (6) TKG were to be the legal basis, the list of Bundesnetzagentur and BSI, as well as the Technical Guideline of the BSI, would have had to be notified at the same time as the draft of the latter. However, § 109 (4) sentence 5 TKG does not contain any conjunction to the certification or an obligation to do so. As a result, there is no national legal basis for List and Technical Guideline in order to establish binding regulations for network operators. A legal basis would have to fulfil the parliamentary scrutiny reservation in regards to its intensity of intervention.

Finally, the occurrence of the specific obligation to replace a component is in no way foreseeable for the network operator. This significant intervention, which is planned by the state, jeopardises the operation of the critical infrastructure itself and entails at least restrictions on use, or may result in the complete failure of network elements and services.

It also remains open how legal protection will be granted to affected network operators if they are to be obliged to remove individual components because the certification of the component is revoked after installation. The network operators are not the addressees of the certification obligation, but the manufacturers. The decisions that could lead to the revoking of certification are also not readily available to network operators. The traceability of administrative actions is also part of this. The network operators will only be aware of this if they are notified of the complete official decisions on the revoking of certification. However, the administrative procedure to be followed for this only concerns the certifying authority and the manufacturer.

This is aggravated by the fact that in the 5G sector a considerable amount of information which could lead to the withdrawal of certification may come from intelligence (secret service) sources, so that the authority withdrawing the certificate may just receive instructions to withdraw it without knowing the objective reasons. This would in no way ensure the traceability of the administrative action, even with regard to the obligation to expand, and would make effective legal protection impossible. This is neither compatible with EU law nor with national law. Moreover, the network operators have no influence on the creation and maintenance of the certification requirements.

X. No hearing

No hearing pursuant to § 109 (6) TKG has taken place on the draft submitted for notification. Just a single hearing on a draft of the Security Catalogue was carried out in autumn 2019. However, this draft differed substantially and to a considerable extent from the draft submitted in the notification. In eco's view, the Bundesnetzagentur/BSI list and the Technical Guideline are legal components of the Security Catalogue. They should, therefore, both have been notified at the same time as the current draft. The draft list is currently under national consultation. Nothing is known about a hearing on the Technical Guideline of the BSI.

In eco's opinion, hearings that were held too late or not at all constitute violations of Art. 41 (2)(a) in conjunction with Art. 16 of the EU Charter of Fundamental Rights. The right to good administration includes, in particular, the right of each undertaking to be heard before any individual measure adversely affecting it is taken. (For the sake of completeness, it is again pointed out that, as far as the list and the Technical Guideline are not regarded as part of the Security Catalogue, there is no legal basis for both.)

XI. Longer implementation deadlines for OTT providers required

Once the EECC has been transposed into national law, it is already foreseeable that the group of obligated parties with regard to security requirements § 109 (6), (4), (2) and (1) TKG will be significantly expanded. This includes, among others, OTT providers. At several points in the notified draft, the Bundesnetzagentur grants providers a period of one year from the publication of the Catalogue, e.g. on p. 65. This period is aimed at traditional telecommunications companies that already have practical experience with and knowledge of the security requirements. In contrast, this does not apply to the OTT providers who will be affected for the first time. The specified security requirements are complex, extensive and difficult to implement. The affected companies must first develop a sufficient understanding of the technical requirements and, based on this, develop a corresponding implementation concept that is tailored to their individual requirements and circumstances.

eco requests an appropriate implementation period, e.g. until 31.12.2025, as stated elsewhere in the draft, p. 66. Added to this are the challenges of implementing the necessary technical precautions. Here too, there is a lack of relevant experience and standardised solutions and concepts. The existing technical systems of the companies affected for the first time are themselves complex. Implementation processes on this scale are very demanding and must be planned, prepared and counter-tested in the best possible way.

The OTT providers concerned will only have some of the required personnel available to install the necessary technical arrangements, adapt them to the existing systems, operate and maintain them. This leads to a new, previously non-existent need in staff recruitment, which is difficult in such a specialised field and requires time to prepare for adequately. This also applies if parts of the processes required for implementation are to be outsourced to third parties, as there are only a few providers in this area and therefore a backlog of orders

is foreseeable, which must be taken into account when longer implementation periods are set.

In the opinion of eco, this demands consideration of the principle of not treating what is not equal equally, Art. 20 in conjunction with Art. 16 EU Charter of Fundamental Rights, and the principle of proportionality under Art. 52 (1)sentence 2 EU Charter of Fundamental Rights. OTT providers are not equal to the traditional telecommunications companies in being placed under such obligations for the first time, as they lack knowledge, experience and best practices. It is therefore proportionate to allow these providers longer implementation times.

About eco:

With over 1,100 member companies, eco is the largest association of the Internet industry in Europe. Since 1995, eco has been instrumental in shaping the Internet, promoting new technologies, creating framework conditions and representing the interests of its members vis-à-vis politics and international bodies. The reliability and strengthening of the digital infrastructure, IT security and trust as well as an ethically oriented digitalisation form the focus of the association's work. eco is committed to a free, technology-neutral and powerful Internet.