Position Paper

Bitkom views concerning the catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data – pursuant to § 109 of the Telecommunications Act (TKG) Version 2.0

October 5, 2020

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Nick Kriegeskotte
Head of Telecommunications Policy
n.kriegeskotte@bitkom.org

Sebastian Artz
IT Security
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Preliminary remarks

On August 4, 2020, the German Federal Network Agency submitted an amended security catalogue for notification to the European Commission. As Bitkom, we actively contributed to the comments on the security catalogue with our statement of November 18, 2019. However, the results of the consultation at that time were not included to the necessary extent in the security catalog now submitted for notification. While on the one hand it is to be welcomed that important political processes have been initiated, on the other hand it is to be regretted that the industry has not been given the chance to provide further feedback. In its current version, the security catalogue still has some unclear wording and is therefore, in fact, difficult to subsume. This is problematic because the appendix, due to its legal construction, appears almost like a law, since the network operators are ultimately restricted in their choice of contract partners. Consequently, there is an internal market relevance of the present catalogue that cannot be dismissed out of hand and which must now be considered at European level. For this reason, we would like to emphasize our perspective and position at the European level as well. The document is in line with our German position of November last year. In addition, the Annex (page 14) selectively addresses certain amendments of the current version of the catalogue. In general, Bitkom proposes and promotes the unified application of comparable criteria across the common market. Bitkom wishes to emphasize that individual national pockets of regulation should not be created to circumvent the common market. Bitkom therefore promotes a unified approach in the EU.

A. General considerations

4G and 5G mobile communications and digital infrastructures in general are becoming the backbone of the digital economy, society and administration. The aim is to set up efficient, affordable and secure 5G networks in Germany as quickly as possible and to consolidate and upgrade 4G networks. The growing importance of communications networks for the functioning of our society means that more ambitious demands are being placed on communications infrastructure in every respect. At the same time, the

debate on trustworthy infrastructures is also giving rise to further requirements for the shaping of Europe's digital sovereignty.

In order to achieve these goals, fair and innovation-stimulating competition with the same rules for the same services and offerings and the diversity of technologies and providers are essential so that, as intended, high-performance, affordable and secure 5G networks can be established in Germany as quickly as possible.

However, in order to satisfy the claim to sovereignty, in addition to the necessary speed of market development, policy-makers are called upon to design the legal framework and its implementation in such a way that the networks guarantee the highest possible level of security, including availability, at all times and cannot be compromised. As a general principle, all manufacturers - regardless of their products and offers and regardless of their origin - ideally have to apply at least the same product- and offer-specific test criteria, rules and procedures throughout Europe. At this point, we would also like to point out that a clear and technology-neutral approach that promotes the use of effective encryption must not, on the other hand, be thwarted by government activities to weaken encryption.

The legislator must also clearly address the requirements it imposes to ensure an appropriate level of IT security. Here, the Cybersecurity Act, the IT Security Act and the NIS Directive as a horizontal regulation play an important role. The discussion on § 109 TKG should also be seen in this context.

In principle, the following four principles must be observed:

1. Transparency is the basis for trust. This requires a cooperative approach with clearly defined rules for all sides. This lays the foundation not only to secure the respective product but also to strengthen the knowledge in the secure development life cycle for future products. All stakeholders should ensure that they are free from undue governmental influence and that they are in line with the standards and objectives of the OECD Principles of Corporate Governance.

2. Testing and certification: Innovation will secure tomorrow's prosperity. Innovation in the ICT sector is increasingly becoming the driving force behind economic and social development. Innovation-friendly regulation is crucial to this. The state should above all define the objectives and requirements of the proposed measures. A risk-based approach should be adopted. In the context of certification, mutual recognition should be established at least at European level. This, as well as the issue of transparency, implies that any verification of source code and other relevant materials required by the competent authorities should be carried out at a safe place in Europe under the control of the manufacturer. Germany, not least because of its economic strength, has a model function for states worldwide of which we should be aware.

3. Responsibility: Government bodies and those acting on behalf of governments, network operators and manufacturers each bear their share of responsibility for secure networks and must take all necessary measures in accordance with their respective roles and responsibilities. At the same time, users must be made aware of their contribution to the security, integrity and availability of data, and of the need to use encryption consistently, for example for critical data.

4. European Single Market: The European Single Market is a success story for economic development in Germany. Germany and the German economy have a vested interest in strengthening this internal market and sharing in its innovative strength. Therefore, any definition of security requirements, including the certification of components to be assessed as "critical", must take place within a European framework and the certification by national testing bodies based on this must be recognised throughout Europe. Going it alone at national level weakens economic development and slows down innovation.

These principles will make a decisive contribution to meeting the demand for secure communications networks.

B. Details of the draft version 2.0 security requirement catalogue

Bitkom welcomes the fact that the Federal Network Agency has published the update of the catalogue of security requirements pursuant to § 109 (6) of the Telecommunications Act (TKG) and that the approach described there implies that security requirements apply equally and in a technology-neutral way to all network operators, manufacturers and service providers. Proposed principles, such as permanent network operation monitoring, are already common practice today. The required avoidance of monocultures is also a reality today as part of the multi-vendor strategy of network operators. Furthermore, redundancies in the network are a suitable measure to increase its security.

The security of the networks has top priority. The idea of a comprehensive security architecture, as proposed by the Federal Network Agency, fits in with this. It would be desirable if such ideas could also be implemented throughout the EU. Germany should work towards this. Instead of special national routes with additional costs, efficiency gains in the European internal market could be raised. Moreover, it must also be clear that network operators alone are not responsible, but that manufacturers must also play their part.

1 Regarding 3 “Security requirements for the operation of telecommunications and data processing systems and for the processing of personal data”

1.1 Regarding 3.3.1 “Secure handling of sensitive data and information”

In the field of telecommunications, inventory data, and in particular traffic data, are highly sensitive data. They are subject to data protection and the protection of telecommunications secrecy. Regulations must therefore be established for the secure handling of such data and information. The following applies in particular:

- Implementation of appropriate organisational and technical precautions according to the state of the art,
- Implementation within the framework of a management system, e.g. information security management system (ISMS).

1.2 Regarding 3.3.2 “Physical and elementary protection requirements”

It identifies nine bullet points as the minimum number of measures to be implemented. These appear arbitrary and do not correspond to the basic logic of an ISMS with risk management, in which one determines which measures are to be followed and which are not. For this purpose, the economy or the scope of application of the respective operator is too heterogeneous to make general minimum statements. Here it is more suitable to refer to the existing security standards including the so-called state of the art and an ISMS, e.g. the BSI Grundschutz-Kompendium or ISO 27001.

These listings are to be found throughout the document, especially of course in section 3.3.

1.3 Regarding 3.3.4 “Access and access control on network and information systems”

In the past, "secured areas" were switching centres or IT server rooms which were protected by a central access, but inside were system cabinets without doors and further access protection. For these, the requirement from 3.3.4 is targeted. Today, on the other hand, there are more complex physical infrastructures, e.g. central computer centres, in which various protection requirements with different levels of protection are accommodated in common rooms. For adequate separation, there are separate cage areas for this purpose or at least separate locked server cabinets which are protected against unauthorised access

by individual key or card systems. However, these safeguards are not separate "secure areas" but "secure technical installations" (as a more general term). Through a suitable security concept (24/7 security service, camera surveillance, etc.) it is nevertheless ensured in such environments that access is possible for persons with a legitimate interest.

2 Regarding Annex 2: Further security requirements for operators of networks with increased risk potential

2.1 Preliminary remark

In order to strengthen the establishment of the European (Digital) Single Market and the development of cross-border 5G-based applications, European rather than national approaches should be increasingly targeted. Instead of the planned declaration of trustworthiness, a binding Europe-wide Cybersecurity Scheme for 5G network components based on the EU Cybersecurity Act is therefore needed. In addition, the implications of the IT Security Act 2.0 for the current procedure must be taken into account vice versa.

The aim of the revision of the catalogue of requirements, as well as of further initiatives such as the TKG amendment for the implementation of the European Code of Electronic Communications or the current revision of the IT Security Act, must be to create legal certainty for the telecommunications industry and at the same time to involve the companies, which for their part are indispensable for more secure infrastructure equipment. At the same time, general political questions must not and cannot be answered by technical-regulatory definitions of requirements, nor can they be answered by companies operating in the private sector.

The envisaged procedure provides for two pillars: technical verification and trustworthiness. In addition to the technical inspection of components, the assessment of the trustworthiness of manufacturers should also be a state task and must not be delegated. Neither the draft of the security catalogue according to §109 TKG nor the TKG can fulfil this task, since only operators, but not suppliers, are addressed. A corresponding legal basis, which, among other things, regulates the appropriate allocation of responsibility, must be created.

In order to avoid legal uncertainty among operators, it must also be clarified how the security and trustworthiness of third parties can be verified and guaranteed. The regulator must answer the question of which further processes he is triggering with this.

2.2 Regarding 1. Field of application

The definition of the scope of application or the definition of "increased risk potential" for the determination of the addressees of the further security requirements mentioned be-

low lacks concrete criteria for the determination - apart from the mobile network operators obviously covered. In the interests of legal certainty for the network operators and service providers concerned, more specific information should be provided here.

Furthermore, we would like to point out that the scope of application of the security catalogue must also be considered in a broader context:

1. The scope of application of the TKG and the security catalogue according to §109 TKG is mainly directed at the operators. At the same time, security requires a cooperative approach with obligations and allocation of responsibilities for all actors.

2. The maintenance and strengthening of harmonised regulations between the EU Member States requires a European approach with at least European, if not global standards. Otherwise the harmonisation achieved so far will weaken competition and security. Nevertheless, we welcome the intention to pursue the further development of the security requirements as quickly as possible if a German further development does not lead to a special path but to a coordinated and exemplary European solution.

2.3 Regarding 2. Certification of critical components

First of all, it needs to be clarified together with industry which network and system components are classified as "critical". A complete evaluation of the catalogue cannot be made without such a determination. Furthermore, it must be clarified how an assurance of trustworthiness is to be provided in a suitable manner and in a legally secure manner.

This and a certification of critical components should at least refer to European, ideally international, recognised standards and take existing bodies into account as far as possible. The regulation and, in particular, a possible certification should not lead to a detached national special solution that delays the introduction of 5G in Germany and burdens it with additional costs.

Furthermore, we would like to point out that network and system components are subject to a high development dynamic. Testing and certification procedures must not constitute a bottleneck and, especially in the event of staff shortages in the testing and certification bodies, must not lead to a delayed deployment of critical components. Especially software-technical adaptations that include security-critical components must be introduced promptly. Here, European or international IT management standards could serve as a template to prioritise the audit effort in a risk-oriented way or to keep the effort in an appropriate frame - the goal cannot be that every update leads to a re-certification.

Bitkom therefore welcomes the fact that the catalogue provides for a broader base of test centres to be certified by the BSI in order to effectively counteract possible bottlenecks on the part of the authorities. Corresponding security checks by test centres certified by the BSI are provided for under §2 para. 7 of the BSI Act: Certification within the meaning of this Act is the determination by a certification body that a product, process, system, protection profile (security certification), person (personal certification) or IT security service provider meets certain requirements. Test procedures for "critical" components should be carried out at a safe place in Europe under the control of the manufacturer.

In this context it should be noted that a framework for mutual recognition within Europe is necessary to ensure scalability, effectiveness and efficiency. Approval authorities should be designated which apply a mandatory, robust test method – such as BSI and ANSSI. Without this, each country will be able to repeat tests at high cost and will not be able to meet the requirements for timely testing of new technologies. The BSI law provides the means for such mutual recognition in the European context. §9(7) clarifies that in principle "security certificates issued by other recognised certification bodies from the European Union area are recognised by the Federal Office".

From our point of view, a certification of critical components must be based on European or global standards, since standardisation also takes place at supranational level. Here we welcome the reference to Regulation (EU) 2019/881 (Cybersecurity Act) of 27.06.2019, which introduced a uniform European framework for cyber security certification, in which the recognition of European schemes for cyber security certification is regulated. With regard to the participation of manufacturers, associations of operators of public telecommunications networks and associations of providers of publicly available telecommunications services, Annex 2, point 2.3, refers to the opportunity for comments.
Bitkom recommends active participation by industry in the preparation and updating of the document in order to be able to submit proposals or submissions. In the course of this active participation, the components to be recorded should be identified and named in a uniform manner for the industry.

In order to ensure the operation and further development of new technologies (e.g. the 5G mobile network), we consider it useful to specify the present draft in such a way that exceptions and special cases are taken into account. For example, 5G technology will require software updates at short intervals. Here it should be defined which category of software updates must be subject to recertification or re-testing. From our point of view a certification of every software update is not reasonable and cannot be reproduced in operation. We also see a considerable influence on the availability of resources of the BSI. In general,

we believe that, in addition to the standard certification process for exceptional or emergency cases, there should be the possibility of an alternative, accelerated testing/certification procedure, which, for example, enables the operation of a critical component at short notice and provides for a parallel or downstream testing/certification procedure.

Furthermore, it should be clarified how to deal with critical components of existing technologies (e.g. 2G/3G). From Bitkom's point of view, a certification obligation can only extend to newly commissioned system components and cannot have any retroactive effect.

In this context, the question must also be clarified what happens if certification is subsequently withdrawn, e.g. due to non-availability of software updates. Who bears the costs of this?

2.3.1 Regarding 2.3 and 2.4 Identification and Certification of critical components

In general, we welcome the acceptance and consideration of international standards and analyses such as ENISA or BEREC, in particular in developing and updating the list of "critical functions and components". We also welcome the procedure to define the critical components in accordance with the definition of critical functions that the components serve. This is helpful, as the resilience of the overall system is indicated by favorable results related to security. Basic standard functions need not be considered as critical functions.

Critical components must be clearly identifiable. Undifferentiated designations, as currently used in part in the BSI-KritisV, are not precise enough. We propose to involve operators of telecommunication networks and services in the definition and to form a joint working group of authorities and telecommunication companies under the leadership of the BNetzA or to use the sector working group telecommunications (BAK TK) in the UP KRITIS.

In Annex 2, point 2.2, the operators of telecommunications services will also be given the opportunity to submit comments. Here we expect not only the possibility to submit comments but also the possibility to participate in the preparation and consideration of our submissions.

In terms of transitional regulation, the legal basis must be created so that the manufacturer/supplier of these components initiates the certification process at an early stage in the same way as for new components. It has to be taken into account that, starting from

the operator, this is not possible within the framework of existing contracts and can thus represent a considerable risk factor for the maintenance of operation.

2.4 Regarding 3. Trustworthiness of manufacturers and suppliers

Manufacturers and suppliers are already making a major contribution to a secure network infrastructure. We support the fact that the present draft according to section 3 provides for this responsibility to be certified in writing in accordance with the requirements listed here.

The trustworthiness of a manufacturer/supplier is likely to be determined primarily by the quality of a transparent and open information policy which a manufacturer/supplier displays with regard to the implementation of the above-mentioned regulations and laws, as well as corresponding knowledge and experience from the past. Also in the context of trustworthiness it remains open what happens if a supplier loses his trustworthiness although his technology is already part of the infrastructure. Clear responsibilities, exit scenarios and transitional periods must provide legal certainty.

If a manufacturer/supplier already in use is deprived of its trustworthiness, it must be ensured that the burden of proof for the reason for the deprivation is not placed on the network operator, but on a state institution/authority, ideally at European level. This includes, for example, possible corrections of the network and the restoration of security in this operational network.

In order to remove the legal asymmetry between technical certification and the declaration of trustworthiness, it is necessary that the assessment of trustworthiness is also carried out by independent governmental bodies. Leaving the evaluation of trustworthiness to the network operators releases the state from the obligation to make such a political and factual evaluation.

2.4.1 On point 4:

Here the obligations of manufacturers should be clarified. The present version leads to an unsolvable situation and contradicts, for example, the approach of the EU Commission to enable European law enforcement and judicial authorities to secure electronic evidence under the E-Evidence Directive.

2.4.2 On point 10:

Here the term "immediately" should be further clarified. It is necessary that manufacturers inform all customers or users about security risks in good time and at the same time and thus on an equal footing. Notifying operators before a vulnerability has been prioritised by

the vendor in terms of importance, impact and exploitability, and allowed to be repaired, worked around or contained, would result in a less secure situation.

2.5 To 4. Product integrity

Newly procured critical components are subject to testing and certification by the BSI. In this respect, we generally assume that the delivery condition of hardware or software corresponds to the tested and certified condition.

With regard to the named critical phases of the life cycle of a component, we support the obligation of the manufacturers to integrate technical methods/procedures for testing product integrity into the product and to document the approach for carrying out the verification to the operator in a suitable manner. We also welcome the further obligations of the manufacturers to cooperate, which, however, must be clearly anchored in the regulations, including the necessary protective measures. We welcome the development of such an approach, but point out that such a complex instrument will require several years of development.

Similarly serious are the effects on the existing processes customary in the industry with regard to delivery, storage, commissioning and retirement, which would have to be completely redeveloped and would also have to be reflected in the existing contractual relationships. Especially against the background that certification/testing, coupled with the control mechanisms listed here, represents a preventive control which guarantees the use of integral products and would thus be preferable from a risk perspective.

In cooperation with trustworthy suppliers/manufacturers, it should rather be assumed that the critical components certified by the BSI are used precisely in the tested and certified hardware and software combination. A further obligation to provide evidence does not appear practicable in the application. In order to ensure that the software running on the network infrastructure corresponds to that supplied by the manufacturer, the concept of binary equivalence is a fundamental test. This is a challenge – it is necessary to consider whether the vendor must provide the tools to allow the operator to independently verify this.

The cycle, content and form of the periodic security reviews must be defined, ideally with longer intervals for critical components compared to particularly critical components (cf. redundancy requirement). Any form of additional acceptance tests and regular security reviews tie up new resources at the obligated companies. The specifications for this should therefore follow the principle of appropriateness of the TKG. The content and form of the acceptance tests should also be coordinated with the test contents for BSI certification so that the focus is only on those points for acceptance which have not already been checked.

In principle, there are doubts about the appropriateness (cf. § 109 (2) TKG) and feasibility of this requirement due to the complexity and diversity of the network and system components and the development dynamics in the different technologies.

2.6 Regarding 5. Security requirements during operation

2.6.1 Regarding 5.1. Security monitoring

This requirement focuses on all types of internal and external monitoring to detect attacks or errors. In principle, network traffic via the network and system components is already being monitored for abnormalities. It must be specified which special features an MI (monitoring infrastructure) has. Sector-specific specifications already exist for this. It should be noted that detection must be implemented according to the type of fault or attack, e.g. communication of infected terminals, use of hacked telephone systems and calls from foreign or fake infrastructure components.

The legal requirements for the protection of telecommunications secrecy in particular are likely to make it difficult in practice to detect unauthorised and targeted taps of communications data when concealment techniques are used. For this reason, the MI now demanded appear in part to be difficult to implement and disproportionate. It would make more sense to have security monitoring which is oriented towards the protection goals. In principle, it must also be ensured that no state tasks are delegated to the operators within the scope of monitoring.

2.7 Regarding 6. Instructed specialist personnel

Since the version here clarifies for which type of qualified personnel this requirement is to apply (to maintain the operation of the critical components), we suggest to introduce the requirement in Appendix 2 item 6 as basic conditions in a role profile.

It is also to be described in more detail for which legal requirements there is an obligation to provide verification, who is obliged to provide the verification and to whom the verification is to be submitted. In this context, a more precise, specified definition of sanctions is also necessary.

Depending on the nature of the outsourced system-relevant processes, it must be noted that supplier/manufacturer-independent contractors can also be considered. However, it cannot be assumed that the operators of the outsourced processes are basically independent of the telecommunication companies. This is not the case, in particular, if the telecommunications company – located in Germany and subject to obligations under the TKG – and the contractor belong to a group of companies.

It is questionable whether a contractor is automatically considered "reliable" or only if he is "trustworthy" in the sense of this regulation. This also requires clarification.

2.8 Regarding 7. Redundancies

For protection against disturbances or failures of critical components, the creation of redundancies is named as a possible preventive measure. Here, Bitkom welcomes the fact that the creation of redundancies is to be subject to an appropriate, company-internal risk assessment and is not demanded as a single measure for all critical components. A blanket demand would result in a not inconsiderable increase in operating expenses and maintenance costs.

2.9 Regarding 8. Diversity

Clarification is needed as to what the demand "for sufficient diversity by using network and system components from different manufacturers" refers to.

Basically, with the implied demand for a multi-supplier strategy, it should be noted that such a constellation leads to increased system complexity and thus to new sources of functional instability and security weaknesses. This means that a decision on the use of one or more manufacturers for the realisation of critical network functions requires a detailed consideration of functional, operational and security-related aspects and must be made separately in each individual case.

The network operators active on the market are already pursuing a "multi-vendor" strategy. By updating these operator strategies, the risk of unilateral dependencies can be avoided even in the 5G context. However, a multi-vendor strategy alone does not lead to more security. If the products of all vendors are not equally trustworthy, the logic of a risk-based approach may indeed lead to the opposite effect and limit the number of vendors available for sensitive parts of the network. The requirement for a "multi-vendor" approach in certain areas of architecture, such as the core packet network or parts thereof, could make implementation less secure and much more complex from an architectural and operational point of view. It would increase the number and expertise of skilled personnel that would be required to maintain the network - which is difficult in times of skill shortages - and increase operational costs. Moreover, it is already being implemented today.

In this context, we are also critical of the general requirement to use at least two manufacturers in the core/access network. In addition to operational problems resulting from the operation of network and system components from different manufacturers, we see risks for the secure operation of the network arising from such a rigid requirement. Practi-

cal experience shows that despite international standardisation, the configuration of different manufacturer components is complex and susceptible to faults.

The diversity distribution 1:2 according to number 8, however, seems arbitrary and does not meet the needs of functional network architecture planning. This division should be a guideline or recommendation. Moreover, in order to avoid monocultures in principle, the definition of a percentage is dispensable.

In principle, it should also be specified at this point whether these requirements refer exclusively to the use of components defined as critical or whether they cover all network and system components in a general way.

Annex (05.10.2020)

With regard to the already initiated notification at European level, we would like to explicitly emphasize that we, as Bitkom, advocate and support the uniform application of comparable criteria throughout the entire internal market. Individual national pockets of regulation should not be created to circumvent the common market. Bitkom therefore promotes a unified European approach.

Furthermore, we call for a comprehensive consultation of all applicable legislative projects and draft regulations. If this consultation were to be subdivided into artificially created smaller cells, or were not to include relevant parts of ancillary legislation – examples include section 109 of the German telecommunications act, the reform of the telecommunications act, and changes introduced through the IT security act – this will lead to an incomplete and perhaps skewed assessment of the legislative framework, leading to legal and investment uncertainties. This must be definitely avoided.

Planning, investment and legal security result from the interaction of a stringent and clear set of rules, sufficiently defined standards and the realization of a protection of confidence with regard to the use of certified components installed and approved by the authorities. So far, this interaction does not function to the required extent. Furthermore, the obligations to take risk-mitigation measures must correspond to the actual dangers for networks, services, providers and users.

Regarding 2. Certification of critical components

Certification of critical components must be based on European or global standards, since standardization also takes place at supranational level. Here we welcome the reference to Regulation (EU) 2019/881 (Cybersecurity Act). However, the amendment: "*If no corresponding certification schemes are available, obligated network operators and service providers must temporarily take other suitable and appropriate technical precautions and other hazard prevention measures when using critical components*" leaves room for interpretation and, hence, causes concerns of legal uncertainty. The current draft of the catalogue lacks a clear commitment to the use and acceptance of international standards.

Regarding 3. Trustworthiness of manufacturers and suppliers

Criterion 3 reads: *"Obligation of the supply source to ensure, through organisational and legal measures, that confidential information from or about its customer(s) does not end up abroad at its own initiative or at the initiative of third parties or that foreign agencies in Germany become aware of it."* If interpreted literally, criterion 3 seems to be a data localization requirement. If this is indeed the case, it must be clearly stated as such, especially with regard to the European level and the unsolved question of whether such a requirement would be permissible at all – especially at the sub-legal level. In addition to this, the second half of the sentence refers to "*foreign agencies in Germany*". This suggests a reference to government data access, which also makes the relationship to criterion 4 questionable. This must be considered separately below. Bitkom advises that a renewal of section 92 of the German telecommunications act, as abolished in 2012, should not be intended. Cross-border processing of data will remain permissible in accordance with the generally applicable regulations, especially the GDPR. It is unlawful access by way of interference or outside lawful processing that must be safeguarded against.

Criterion 4 reads: *"Assurance from the supply source that it is legally and actually able to refuse to disclose confidential information from or about its customers to third parties. In particular, at the time the declaration is made, there are no obligations to disclose such information to third parties or to make it available in any other way. This does not apply insofar as there are statutory disclosure requirements for law enforcement purposes, unless such disclosure obligations exist towards foreign intelligence or security authorities. In cases of doubt, the supply source must refer to the statutory disclosure obligation(s) before the declaration is submitted."* It refers to the disclosure obligations to foreign intelligence or security authorities. The wording potentially covers both data transfers to foreign authorities via mutual legal assistance and the proposed mechanisms of the planned EU E-Evidence Regulation. This ultimately means that no manufacturer can actually issue the guarantee under No. 4, because these mechanisms are ultimately mandatory legal obligations that cannot be waived. Especially the aspect of e-evidence is absolutely central in the

course of the notification to the Commission, because this is ultimately a direct conflict between national law and (future) EU law. Furthermore, it should be noted that nowhere is it specifically specified who is a "third party" or "foreign" in the sense of this norm.

Regarding 5.1 Security monitoring

The change made in the first sentence to specify mandatory monitoring infrastructures, away from "[...] *to continuously identify and prevent threats*" and towards " [...] *in order to continuously identify, limit or remedy faults or errors in telecommunications systems*", apparently comes along with additional and more extensive tasks. What exactly is intended by the changed wording remains to be specified. Overall, the required mandatory monitoring infrastructures in their current form are difficult to implement. We still consider an alignment with the protection goals to be more sensible.

Regarding 8. Diversity

In general, it is to be welcomed that the catalogue explicitly refers to the use of open standards. Specifically, chapter 8 reads: "*[components] should be independent of each other and not equally dependent on a third party. In particular, critical network functions and network elements should not depend on a single provider of critical components based on the network topology implemented.*" Considering that individually certified products could use the same critical components without disclosing which third party components they depend on, this new regulation is difficult to comply with and one of the products or components may have to be replaced by administrative act.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.