# Bitkom Response

## to EBA Consultation on Draft Guidelines on the security measures for operational and security risks of payment services under PSD2, EBA/CP/2017/04 (the "Draft Guidelines")

2017 – 08 -01



Bitkom represents more than 2,500 companies in the digital sector, including 1,700 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 400 start-ups and nearly all global players, Bitkom' members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focussing the modernization of the education sector and a future-oriented network policy.

Federal Association
for Information Technology,
Telecommunications and
New Media

**Markus Humpert**
**Bereichsleiter Digitale Transformation**
P +49 30 27576-233
m.humpert@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

## 1. Responses to EBA's Questions

**Question 1: Do you agree with the level of detail set out in the Guidelines as proposed in this Consultation Paper or would you have expected more or less detailed requirements on a particular aspect of the Guidelines? If not, please provide your reasoning.**

Generally, EBA would like to emphasize the principles of technological neutrality, proportionality and of own responsibility of PSPs for their risk management. Also, EBA should allow PSPs sufficient time after 13 January 2018 to implement the Guidelines.

EBA must concede that certain levels of security can be achieved by different means. Generally, EBA should maintain technological neutrality when setting risk management guidelines. Guideline 3.8 is an example where we see a deviation from that principle.

The term "proportionate" is used in several occasions throughout the Draft Guidelines. The term "proportionate" asks for a subject matter to which it relates. Bitkom understands this term to relate to the kind, the extent, the complexity and the intrinsic risks of the PSP's payment services activities. Bitkom asks EBA to clarify this in the

Guidelines.

Risk management is a crucial factor in the management of a business. The risk policy setting the "risk appetite" of the business is a core feature of a business's strategy which can decide about the success or failure of a business. EBA should therefore emphasize that it is the prerogative of the management of the business of a PSP to set the risk policy and risk management measures derived from that policy – within the limits of reasonableness. This must be made clear throughout the Guidelines.

Art. 95(3) of PSD2 forsees that EBA issues guidelines (the "Guidelines") as of 13 July 2017. This would have meant a period of six months in which PSPs could have adapted their internal and external procedures to such new guidelines. The final guidelines should therefore allow for a period of at least six months from the publication of the final guidelines by EBA to the date of application of such guidelines.

Generally, Bitkom recommends substantiating certain definitions and terminology used in the Guidelines to achieve a higher level of certainty for compliance. See responses below for further details.

Also, any process set out in the Guidelines should be standardized to the extent possible in order to avoid different levels of compliance.

The Guidelines should further emphasize that mandatory European or national law, in particular the provisions regarding data protection, shall not be affected by the Guidelines.

The term "security risk" requires a precise definition in particular to identify any gaps, threats or risks for an adequate risk management.

**Question 2: Do you agree with the proposed Guideline 1 on Governance? If not, please provide your reasoning.**

In Guidelines 1.1 and 1.2 EBA should clarify the terms "risk management framework" and "security policy" and how they relate to each other.

In Guideline 1.4 it does not seem to be reasonable to change the risk management framework for major changes in infrastructure, processes or procedures or after major incidents. In most cases it will suffice to change the respective risk measures; this would leave the overarching risk management framework unchanged.

In Guideline 1.5, EBA should define what is meant by "three lines of defence". The Guidelines should further determine more specific processes and/or objectives regarding the "three lines of defence" or risk measures.

Guideline 1.6 asks for an audit of security measures by internal and external independent and qualified auditors. Bitkom sees difficulties in implementing this requirement: (i) What would be the necessary qualification of an auditor, in particular if the security measures relate to highly specialized technology? (ii) The (internal or external) costs for a specialized audit can be very high. (iii) Outsourcing service providers may be reluctant to let a PSP perform audits where the third party service providers risks that core business secrets may be disclosed.

Bitkom therefore proposes: (i) An audit is not necessary where the PSP or the third party service provider has obtained a certification by a renowned, independent and qualified institution (e.g. an ISAE certification, IDW certification or other standards) [and the report on the certification can be provided to the internal auditor of the PSP]. (ii) A PSP engaging a third party service provider may decide in its own discretion to solely rely on the reported results of an audit by an external independent and qualified auditor. In addition, Bitkom suggests implementing a mechanism to determine reliable certification entities, e.g. by way of a register of recognized certification providers. Such register could be maintained by the national financial supervisory authority (for instance in Germany: the Federal Financial Supervisory Authority – BaFin).

Bitkom would also like to ask EBA to make use of the authorization contained in Art 95(3) PSD2, which clearly asks for certification processes: "*EBA shall [...] issue guidelines [...] with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.*"

On Guidelines 1.7 and 1.8, Bitkom proposes the following: Bitkom requests EBA to define the term "outsourcing". The definition should limit (regulatory) outsourcing to commissioning a third party service provider with services which are typical for the PSP itself and which would otherwise be performed by the PSP. Also, certain short term services provision should be excluded from the requirements of Guidelines 1.7 and 1.8.

In Guideline 1.8 EBA should define the terms "appropriate" and "proportionate"; see also above answer to Question 1.

**Question 3: Do you agree with the proposed Guideline 2 on Risk assessment? If not, please provide your reasoning.**

In Guidelines 2.1 and 2.2 it should be made clear that the term "regularly update" does not mean that the same term of updating applies to each inventory, but it is the PSPs prerogative to determine reasonable updating intervals for each inventory separately.

In Guidelines 2.2 and 2.3 it should be made clear that it is the PSP's prerogative to reasonably determine which business functions, human resources, processes and information assets are critical for the respective PSP's business.

In Guideline 2.3 it seems that sentences 2 to 4 are misplaced in Guideline 2 which generally deals with risk assessment and not risk mitigation. Also, in the context of access logs the extent of obligations of PSPs can be limited by the rights of the works councils (*Betriebsraete*) in several European jurisdictions (in particular Germany); this should be mentioned in the guideline.

In Guideline 2.5 it should be made clear that it is always the PSP itself who determines in his reasonable assessment which changes will be necessary – depending on the individual risk policy set by the management of the PSP.

**Question 4: Do you agree with the proposed Guideline 3 on Protection? If not, please provide your reasoning.**

Guideline 3.2 refers to the 'defence-in-depth'-approach for "covering people, processes and technology related to the provision of payment services". 'Defence-in-depth' in practice is used for information assurance and is based at the first level of defence. Bitkom is concerned that a more general requirement referring to "multi-layered controls" could be misinterpreted as a "basic rule" for the first level of defence, which would not necessarily lead to better security but solely to an increasing complexity. From our point of view, general reference should be made to the more

adequate "three levels of defence"-principle in this context, a reference to the 'defence-in-depth'-approach could still be included "as far as appropriate".

Guideline 3.3 should be rephrased as follows: "PSPs should protect the confidentiality, integrity and availability of their critical logical and physical assets, resources related to the provision of payment services. PSPs should protect the sensitive payment data of their payment service users against abuse, attacks and inappropriate access and theft."

In Guideline 3.5, EBA should clarify that a PSP will not be held responsible for protecting any sensitive payment data (etc.) in transit, if the PSP has no influence on such data anymore. A PSP should only be held responsible for any breaches committed in its own sphere. Also, a PSP should not be obliged to check and verify the authenticity and integrity of software, firmware and information outside its sphere of influence. Thus, the risk spheres of the relevant participants should be further specified in the Guidelines.

The current wording of Guideline 3.6 is not up-to-date regarding market needs, as in practise PSPs often face the hurdle of hardly being able to convince national Competent Authorities that agile structures of technology/software development and deployment (esp. so-called agile and cross-functional development structures) can still meet security requirements within the limits of rather classical principles, such as "least privilege" or "segregation of duties". At first sight these structures are contradicting the regulatory needed principles of "segregation" and "least privilege". However, there are adequate measures that still assure adequate security. Especially, as automation is key to be compliant with "least privilege" and security can even be increased by that means. Bitkom proposes an EU-wide clarification as part of Guideline 3.6 that agile software development structures are still feasible from a risk management point of view as long as the targeted risks are consistently covered.

In Guideline 3.7, the reference to "data minimisation" is too broad and should be further specified and also referred to specific content. PSPs are already obliged by European and national data protection laws to safeguard customer's personal data.

In Guideline 3.8, the term "up to date" is rather imprecise and needs clarification. It should be clarified that also older software can be up to date if the software is maintained and serviced by the developer or by another service provider in reasonable intervals. Also, it must be clarified that the obligation to update can only apply to software within the sphere of influence of the PSP and cannot apply to the main frame software. EBA should provide a more specific definition of this term.

In Guideline 3.10 and 3.11, a PSP should not be obliged to implement measures that violate any national law; in particular local employment law. As a global remark: national employment law should take precedence over the Guidelines and this fact should be reflected in the Guidelines.

In Guideline 3.12, the term "strong authentication" should be further specified. EBA should in particular clarify that the term "strong authentication" shall not have the same meaning as in Art 97, 98 of PSD2 and the respective Regulatory Technical Standards developed by EBA.

Guideline 3.13 requires clarification. In particular the terms "products" and "tools" are unclear.

**Question 5: Do you agree with the proposed Guideline 4 on Detection? If not, please provide your reasoning.**

In Guideline 4.6 EBA could clarify that this includes establishing procedures with outsourcing service providers to inform the PSP about security incidents and security related customer complaints.

Moreover, with regard to Guidelines 4.4 - 4.6 it might be helpful to refer for further guidance (general definitions of security incidents) to the EBA's final Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2) - EBA/GL/2017/10.

**Question 6: Do you agree with the proposed Guideline 5 on Business continuity? If not, please provide your reasoning.**

Guideline 5.1 requires PSPs to ensure their ability to provide payment services even in case of a severe business disruption. However, in such case, the PSP may not be able to provide payment services to the extent to which the PSP would provide under normal circumstances. Therefore, guideline 5.1 should be clarified, that payment services must be provided to the extent possible in case of a severe business disruption.

**Question 7: Do you agree with the proposed Guideline 6 on Testing of security measures? If not, please provide your reasoning.**

Guideline 6 should be understood in the light of Guideline 2.2 and the respective comment above. It is the PSP's prerogative to reasonably determine which business functions, human resources, processes and information assets are critical for the respective PSP's business. Testing obligations should be graduated in accordance with the criticality based on the PSP's risk assessment and the PSP's risk policy.

**Question 8: Do you agree with the proposed Guideline 7 on Situational awareness and continuous learning? If not, please provide your reasoning.**

With regard to Guideline 7.1 (a) we would like to state that Instead of obliging all PSPs to do market assessments as well as information sharing with third parties/PSPs (not being sure to what extent they are allowed to share information on security incidents); the EBA should provide the alternative within the Guidelines to introduce "central contact points" at EBA or on national authority level. Doing so, PSPs - who in general have to report new incidents to authorities anyway - would be provided with a central contact point for sharing and obtaining information on new risks.

**Question 9: Do you agree with the proposed Guideline 8 on PSU relationship management? If not, please provide your reasoning.**

Art. 95(3) PSD2 states: EBA shall [...] issue guidelines [...] with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.

In Art. 95(3) PSD2 EBA is not asked to issue guidelines on the relationship of the PSP to the PSU. Bitkom therefore is of the opinion that Guideline 8 exceeds the authority conveyed to EBA under Art. 95(3) PSD2 and Guideline 8 should therefore be deleted in its entirety.

If the EBA does not agree with this view, we would at least expect the Authority to consider the following necessary adaptions. Guideline 8 generally speaks of the PSP and thereby includes all PSPs. However, most PSPs do not have any legal relationship, in particular not a contractual relationship, with the PSU. This is in most cases true also for the payment initiation service provider. It can therefore not be the obligation of "all" PSPs to provide information to the PSU, let alone such PSPs (e.g. an acquirer) violating obligations in their legal relationship with other PSPs (e.g. issuers of payment instruments) when addressing the other PSPs PSUs.

Guideline 8.8 should be deleted without replacement. A PSP has no influence on any updates outside his sphere.

Guideline 8.10 also covers cases in which the PSP may not notify the PSU pursuant to applicable anti money laundering law. Guideline 8.10 should be limited respectively.

**Question 10: Do you consider the extent of the requirements proposed in the Guidelines to be sufficient and clear? If not, please provide your reasoning.**