IK
Interessengemeinschaft
Kreditkarten

IK Interessengemeinschaft Kreditkarten · Im Uhrig 7 · 60433 Frankfurt

European Banking Authority (EBA)

One Canada Square (Floor 46)
Canary Wharf
London E14 5AA|
United Kingdom

Munich, 24 September 2018

Dr. Markus Escher markus.escher@gsk.de
Dr. Hugo Godschalk hgodschalk@paysys.de

Consultation Paper: EBA/CP/2018/11 on the Draft Guidelines on Outsourcing arrangements

Dear Sir or Madam,

We refer to you on behalf of the German *IK Interessengemeinschaft Kreditkarten* (IK Interest Group Credit Cards, hereinafter referred to as "**IK"**).

The IK is a competition neutral platform without legal capacity for entities, which act in the credit and debit card business in Germany (Issuer, Acquirer, Network Service Providers, Processing Entities, Licensors), registered in the EU-Transparency Register under aforementioned Ident-no. The IK also contributed to several other EBA discussion papers and consultation papers.

We hereinafter comment on EBA's Consultation Paper (EBA/CP/2018/11) on the Draft Guidelines on Outsourcing arrangements (hereinafter referred to as "**EBA's Draft"** or **"Consultation Paper**" or with respect to the Draft Guidelines "**Guidelines**" or "**GL**"). All references made to enumerations without additional reference to a specific directive or regulation refer to EBA's Draft / Consultation Paper.

I. Comments on EBA's question no. 1

[Question 1: Are the guidelines regarding the subject matter, scope, including the application of the guidelines to electronic money institutions and payment institutions, definitions and implementation appropriate and sufficiently clear?]

1. Applicability to payment and e-money institutions

a. Directive (EU) 2015/2366 ("**PSD2**") as well as a number of technical standards and guidelines based on PSD2 provisions already provide a comprehensive regulatory framework which pays particular attention to the specific risk of payment service providers' business models including risks related to outsourcing. It does not become clear why – in addition to that – payment and e-money institutions need to be subject (in full) to the GL. In contrast, the fact that the legislator deliberately conveyed in the PSD2 mandates to EBA with regard to several matters, but that there is none on outsourcing guidelines, makes it clear that the legislator did not see a respective necessicity given the already extensive PSD2 provisions at Level 1, 2 and 3. The EBA should therefore not use its general rights and legal possibilities to further impose regulatory provisions on payment and e-money institutions.

In parts, the GL seem to address particularly big banks and investment firms, including systemically important institutions. Some of those may expose the European Union (EU) to financial stability risks while those payment and e-money institutions currently active in the EU – given their business models and the volume of their businesses – do not.

The IK is of the opinion that – instead of imposing a comprehensive set of new, additional regulatory requirements – consistent monitoring of already applicable regulation would better serve the goal of ensuring a reliable functioning of the payment services market.

Therefore the GL should not apply to payment and e-money institutions.

b. Certain regulatory provisions which the GL refer to are not applicable to payment and e-money institutions. Therefore explicit exemptions for payment and e-money institutions should be made where the GL are based on or refer to

- the EBA's Guidelines on Internal Governance, including their Section 18 (new products and significant changes, (EBA/GL/2017/11); footnotes 19, 20, 21 should therefore be deleted and on page 20/no. 16 it should be made clear that payment institutions are not exclusively bound by the EBA's Guidelines on Internal Governance, but may also use other reasonable criteria when applying the principle of proportionality;
- the EBA's guidelines on SREP (EBA/GL/2018/03) und the EBA's guidelines on ICT risk (EBA/GL/2017/05); no. 103 of Title V – Guidelines on outsourcing addressed to

competent authorities (page 47) should therefore not apply to payment and e-money institutions.

This is in line with the Lamfalussy regulatory approach according to which at level 3 (guidelines), supervisors are responsible **exclusively** for advising the Commission in the adoption of **already applicable** level 1 and 2 acts and for issuing guidelines on the implementation of the **already applicable** rules. Therefore the scope of regulatory provisions that are not applicable to payment and e-money institutions should not be extended by the EBA's draft.

2. Differentiation between outsourcing and other external procurement of goods and services

a. The IK welcomes that the EBA's draft clearly states (at page 23/no. 23) that the acquisition of services, goods and utilities that are not normally performed by the (payment) institutions are not considered outsourcing. No. 23, however, should be amended to include in line with

- BaFin's Minimum Requirements for Banks' Risk Management (AT 9);
- Recital (82) of the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 supplementing Directive 2011/61/EU of the European Parliament and of the Council, and
- EBA's analysis and feedback on page 30 of Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2 (EBA/GL/2017/17).

the following text:

"*This also includes services that are usually provided by a supervised enterprise and which, owing to actual circumstances or legal provisions, the institution itself is normally unable to provide either at the time of external procurement or in the future (e.g. the use of central banking functions within a network of affiliated financial institutions or the use of clearing houses in the context of payment transactions).*

Supporting tasks like administrative or technical functions assisting the management tasks such as logistical support in the form of cleaning, catering and procurement of basic services or products, should not be deemed to constitute outsourcing as well; other examples of technical or administrative functions are buying standard software 'off-the-shelf' and relying on software providers for ad hoc operational assistance in relation to off-the-shelf systems or providing human resources support such as sourcing of temporary employees or processing of payroll.

Payment devices, terminals and software used for the provision of payment services, the authentication of the payment services user or the generation/receipt of authentication codes manufactured by other companies should also be considered as

'standard products' which are purchased. It is the responsibility and task of the relevant institution and payment institution to test all security measures before implementation and during operations. How this should be done is up to the relevant institution and payment institution."

b. The IK does not agree with the EBA's approach on page 22/no. 22 of the EBA's draft that for the differentiation between outsourcing and other external procurement of goods and services it should not be relevant whether or not the institution or the payment institution has performed that function in the past or it would be able to perform it by itself. The IK believes that this contradicts the definition of "outsourcing" proposed by the EBA itself on page 18 ("*that would otherwise be undertaken by the institution … itself*").

The last sentence of no. 22 should therefore be deleted.

3. Differentiation between outsourcing of important and critical functions and outsourcing of other functions; principle of proportionality

The GL should clearly differentiate between (i) outsourcing of important and critical functions and (ii) outsourcing of other functions.

a. The IK would welcome if, formally, different sections with respective headlines were used for provisions applicable to (i) outsourcing of important and critical functions and (ii) outsourcing of other functions.

b. In order to act in compliance with the principle of proportionality, as set out in the Executive Summary of EBA's Draft and as explicitly pointed out recently by the Financial Stability Institute (FSI), jointly created by the Bank for International Settlements (BIS) and the Basel Committee on Banking Supervision (BCBS) to assist supervisors around the world in improving and strengthening their financial systems, (FSI Insights on policy implementation No 1, Proportionality in banking regulation: a cross-country comparison, August 2017), the IK suggests to emphasize the principle of proportionality in the context of this distinction.

c. Costs arising from compliance with new regulatory instruments for the parties whom they affect should be well balanced with the real value add those instruments provide in terms of reducing relevant risks to the market and customers. The IK is of the opinion that proper application of the principle of proportionality by (payment) institutions also includes the demand that institutions, in individual cases, shall make more extensive provisions over and above particular requirements that are explicitly formulated in the GL this is necessary to ensure that their risk management with regard to outsourced activities is appropriate and effective. Therefore, institutions whose business activities are particularly complex, internationalised or exposed to risk shall make more extensive risk management arrangements than smaller institutions with less complexly structured business activities that do not incur any extraordinary risk exposure.

The GL, however, do not mirror this approach, but require any institution or payment institution subject to the GL to apply the full set of requirement.

Therefore it is all the more important to differentiate well between risky outsourcing structures where more onerous regulatory burdens may be justified compared to low-risk, basic outsourced services.

The GL, however, set out a comprehensive framework that includes extensive organizational requirements which – with a view to the principle of proportionality – seem only appropriate for outsourcing **of important and critical functions**, but not for **any** kind of outsourcing.

Mere "*Outsourcing of other functions*" should certainly remain subject to individual risk management requirements of (payment) institutions.

However, e.g. excessive documentation requirements (including specific requirements as regards the content of respective outsourcing arrangements) as well as access, information and audit rights should be waived in general for "*outsourcing of other functions*".

From a practical perspective it would not suffice to allow that e.g. the – required – full rights of access and audit are exercised in a risk-based manner (e.g. by relying on third-party audit reports or certifications), if these rights must be contractually assured in any case. Negotiating respective contractual provisions as such, for example, will already be extremely time-consuming and will lead to increased overall costs for institutions and payment institutions if that requirement also applies to any kind of basic, low-risk outsourced service.

4. Sub-outsourcing

a. Again in consideration of the principle of proportionality, requirements regarding sub-contracting should generally only apply to those sub-contracted functions which themselves constitute a (sub-)outsourcing **of important and critical functions.** Minor sub-outsourced activities are not as critical and do not pose significant risks to (payment) institutions. Applying comprehensive internal organization requirements even for non-material sub-outsourced activities would be disproportionate in consideration of the principle of proportionality. It will be sufficient, instead, to include non-material sub-outsourced activities in standard risk management arrangements applicable on financial/payment services and IT-related risk.

b. The following references to "*sub-outsourcing*" should therefore be amended in such way that they only refer to "*sub-outsourcing **of important and critical functions***" and references to "*sub-service provider*" or "*sub-contractors*" should be amended in such way that they only refer to "*sub-service providers **to which important and critical functions are sub-outsourced***":

- Section 4 Outsourcing Policy (page 27), no. 34 c. ii.;
- Section 8 Documentation requirements (page 31), no. 47 b. iv., v.;
- Section 9.2 Due diligence (page 35), no. 56;
- Section 9.3 Risk assessment (page 36), no. 60 a., b.;
- Section 10.4 Termination rights (page 42), no. 81 c.;
- Section 11 Oversight of outsourced functions, no. 83;

In Section 10.1 (Sub-outsourcing of critical or important functions) it should be made clear that the requirements set out in no. 65 a. – h., no. 66 and no. 67 only apply to "sub-outsourcing **of important and critical functions**" as the current wording might be misleading in that regard.

What is more, the obligation to maintain an updated register relating to all outsourced activities is defined too broadly and does not entail regulatory benefits. It would generally be sufficient to maintain an updated register for outsourcing of important and critical functions.

5. Cloud services/cloud outsourcing

a. Definition of outsourcing

A few sections of the GL specify requirements applicable solely for "cloud outsourcing".

However, the specifics and the broad variety of cloud computing services products should be considered by expressly acknowledging that not all cloud computing products are covered by outsourcing regulation, and acknowledging the concept of purchasing of specific cloud services which is not regulated outsourcing by amending no. 23 on page 23 as follows at the end:

"*Some cloud computing products as well might not qualify as (cloud) outsourcing, but as purchasing / acquisition of services.*"

The example of purchasing of server capacities and the cloud-typical achievement of a high scalability and flexibility with cloud computing products – contrasting to own infrastructure and server capacities within institutions – confirms that (payment) institutions do not regularly "delegate" activities to cloud service providers, but instead purchase cloud computing products. The purchasing of these cloud products by the financial community is more comparable to purchasing "commodity", rather than "delegating functions or activities".

Cloud computing has historically – due to its expansion on a series of servers and IT-platforms – never been an in-house function of an institution as such services are provided by highly developed external IT service providers. In respect thereof, specialist know-how is required for setting up and maintaining cloud computing services and dedicated cloud infrastructure through a series of server and IT networks. Cloud service providers are pooling expertise and server capacities as main asset of

their business. Especially large IT service providers such as Microsoft, SAP or Oracle are quasi monopolists in their business areas. Hence, for most institutions it is technically not possible to run cloud infrastructures in-house by themselves. Because of the radical development of the IT industry in the last years, the business of cloud computing has been developed externally as own type of business from the very beginning and therefore never has been an internal function of institutions. As a consequence thereof, cloud computing services are often not "delegated" from institutions but purchased from external third-parties according to the above mentioned nature of the service from a historical point of view.

b. Date of application

Outsourcing to cloud service providers should be documented, according to the GL, by 01 July 2018 in line with the Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

The IK, however, is of the opinion that **a common date of application of the GL** to any kind of outsourcing arrangements would better serve the goal of a consistent implementation of the new requirements.

6. Multi-tenant service providers

a. With regard to the procurement of the outsourcing of certain services and processes, particularly in the area of cloud computing, institutions are mostly retaining quasi monopolists like Microsoft, Oracle or SAP, who service a broad range of customers with standardized cloud products.

In consideration of the aforementioned, the IK further is of the opinion that it is justified from a regulatory perspective that the specific circumstances of large and centralized "outsourcing" providers that service a significant number of clients (hereinafter "multi-tenant service providers") is duly taken into account.

The German National Competent Authority BaFin, in its Minimum requirements for risk management ("MaRisk"), recognizes the practical background of those "multi-tenant service providers" who simply cannot offer standardized IT-services, such as cloud computing, to customers, while applying completely different compliance or other IT risk management arrangements for the same IT-service but for maybe some dozens of different customers with different internal security landscapes. EU legislation and EBA Recommendations should still be feasible to be implemented, particularly for retaining multi-tenant providers, but should not impose impossible duties for stakeholders.

Hence, the IK suggests to explicitly consider the concept of multi-tenant service providers **not only with respect to access and audit rights, but particularly with regard to required minimum content of contractual arrangements in a proportionate manner**.

In this context it is proportionate as EBA suggested to either apply pooled customer audits or that institutions be provided by multi-tenant service providers with external audit reports.

In addition to that it should be clearly stated that in the case of multi-tenant service providers direct access and audit rights of (payment) institutions could be limited to exceptional cases when external audit reports do not comply with applicable audit report standards or when shortcomings or other findings are detected.

For the avoidance of any doubt, a definition of "multi-tenant service provider" should be included in the Definitions as follows:

"multi-tenant service provider means a service provider that service a significant number of clients with standardized cloud computing functions."

b. Due to the aforementioned circumstances, the IK also likes to propose a new alternative supervisory approach with regard to EBA's Draft.

The IK suggests considering certain dedicated certification requirements for cloud computing and other multi-tenant service providers specifically providing services to (payment) institutions rather than to continue the assumption that respective functions are "outsourced activities". Most of those services have never been (and never can be) performed in-house in (payment) institutions. Here, alternative concepts could be considered like recently applied for electronic identification schemes under the EU-eIDAS regulation 910/2014 with mutual recognition of schemes in the EU internal market on the one hand and the enabling of financial service providers to make use of electronic identifications – if compliant with aforementioned regulation – in the ambit of performing AML-know your customer duties, without qualifying this usage of electronic identifications as outsourcing, but as a "certified commodity".

The IK is of the opinion that "old" and maybe outdated outsourcing regulatory concepts including outsourcing agreements, access and audit rights, as are usual for outsourced business processes (BPO), may no further be appropriate particularly in more complex and sophisticated IT-cloud networks as the specific needs of individual institutions will have a reduced importance compared to a standardized supply of "IT-commodity cloud products". Here, new regulatory concepts including certifications of standardized cloud providers/multi-tenant providers and products may be a good way forward in order to ensure IT-risk mitigation for financial institutions but still follow innovative developments in the IT market.

II. Comments on EBA's question no. 2

[Question 2: Are the guidelines regarding Title I appropriate and sufficiently clear?]

Principle of proportionality

It should be made clear that payment institutions are not exclusively bound by the EBA's Guidelines on Internal Governance, but may also use other reasonable criteria when applying the principle of proportionality. The text on page 20/no. 16 at the end should therefore be amended as follows:

*"Those criteria **may** be used …. also by payment institutions … , **but payment institutions may also use other reasonable criteria when applying the principle of proportionality**."*

III. Comments on EBA's question no. 3

[Question 3: Are the guidelines in Title II and, in particular, the safeguards ensuring that competent authorities are able to effectively supervise activities and services of institutions and payment institutions that require authorisation or registration (i.e. the activities listed in Annex I of Directive 2013/36/EU and the payment services listed in Annex I of Directive (EU) 2366/2015) appropriate and sufficiently clear or should additional safeguards be introduced?]

1. The IK does not agree with the EBA's approach on page 22/no. 22 of the EBA's draft that for the differentiation between outsourcing and other external procurement of goods and services it should not be relevant whether or not the institution or the payment institution has performed that function in the past or it would be able to perform it by itself. The IK believes that this contradicts the definition of "outsourcing" proposed by the EBA itself on page 18 ("*that would otherwise be undertaken by the institution … itself*").

The last sentence of no. 22 should therefore be deleted.

2. The concept behind the provision in no. 26 (page 23) does not become fully clear, particularly with regard to payment institutions. Particularly, it is not clear how the outsourcing of regulated payment services to service providers in third countries relates to the PSD2 agent concept and the stipulations that are applicable under the PSD2 in that regard. It would therefore be helpful if the EBA clarified (in general and by providing respective examples) with a view to payment and e-money services:

- which activities exactly could be outsourced to service providers in third countries,
- how the provisions in no. 26 generally relate to (and do not conflict with) the basic principle that regulated activities can only be performed by entities with a respective licence under applicable EU/national law (e.g. PSD2 and the German Act on the Supervision of Payment Services), and
- whether PSD2 stipulations regarding the agent concept are in line with the provisions in no. 26 and whether or not or under which circumstances they need to be fulfilled in parallel (i.e. whether and if, how in-scope outsourced activities can be distinguished from agent activities).

IV. Comments on EBA's question no. 4

[*Question 4: Are the guidelines in Section 4 regarding the outsourcing policy appropriate and sufficiently clear?*]

1. The general requirements regarding the outsourcing relation between a payment service provider (PSP) and its service providers, including the relevant liability aspects, are covered in Articles 19 and 20 of PSD2. The requirements in *EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)*, particularly GL 2.7 and 2.8, take due consideration of the specificities of an outsourcing relation and its potential impact on the risk management function of PSPs and their level of detail was designed to provide an appropriate framework enabling flexible application by different PSPs. Section 4 should therefore be amended as follows:

"*Instead of the requirements in this Section 4 regarding the outsourcing policy, for payment and e-money institutions exclusively the EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) apply."*

2. The IK is of the opinion that consistent monitoring of proper application by PSPs of the EBA *Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)* instead of imposing additional regulatory requirements would better serve the goal of ensuring a reliable functioning of the payment services market.

V. Comments on EBA's question no. 5

[Question 5: Are the guidelines in Sections 5-7 of Title III appropriate and sufficiently clear?]

1. For payment service providers, the regulator has so far not seen a specific need for specific requirements on conflicts of interests in the PSD2 Level 1, Level 2 and Level 3 provisions. Payment service providers should therefore not become subject to such requirements by way of the GL.

Where with regard to intragroup outsourcing, conflicts of interests that may be caused by outsourcing arrangements between different entities within the scope of consolidation need to be taken into account, respective provisions should only refer to parent undertakings and subsidiaries subject to Directive 2013/36/EU on a consolidated or sub-consolidated basis, unless waivers have been granted under Article 21 of Directive 2013/36/EU.

Sections 5 of Title III should therefore be amended and a wording as follows should be inserted at its beginning:

"*This section on Conflicts of interest does not apply to payment and e-money institutions on a solo-basis. It only applies to (i) institutions and (ii) parent undertakings and subsidiaries subject to Directive 2013/36/EU on a consolidated or sub-consolidated basis, unless waivers have been granted under Directive 2013/36/EU.*"

All other references to payment institution in this section should be deleted.

2. The *EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)* already cover business continuity management for payment service providers (next to the monitoring, detection and reporting of operational or security incidents; scenario-based continuity plans including their testing and crisis communication; the testing of security measures and situational awareness and continuous learning). Section 6 should therefore be amended as follows:

"*Instead of the requirements in this Section 6 regarding Business continuity plans, for payment and e-money institutions exclusively the EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) apply.***"**

Again, the IK is of the opinion that consistent monitoring of proper application by PSPs of the EBA Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) instead of imposing additional regulatory requirements would better serve the goal of ensuring a reliable functioning of the payment services market.

3. Section 7 no. 42 footnote 22 should be deleted.

4. In no. 44 the words "*ascertain that*" should be replaced by "*shall examine and assess in a risk-oriented and process-independent manner*".

5. <u>No. 45 should be deleted completely.</u>

The way audit recommendations and findings are treated is already part of the generally applicable organizational requirements and therefore no additional or deviating provisions should be implemented by the GL.

VI. Comments on EBA's question no. 6

[*Question 6: Are the guidelines in Sections 8 regarding the documentation requirements appropriate and sufficiently clear?*]

1. Section 8 regarding the documentation requirements does not seem appropriate inasmuch as it applies to <u>all</u> outsourcing arrangements.

2. The comprehensive documentation requirements in Section 8 should be restricted to outsourcing/sub-outsourcing of critical and important functions only. That would not only better serve the principle of proportionality, but also allow for consistent application and monitoring of a risk-based approach.

3. In the IK's Opinion the template in Annex X is far to detailed. Besides it contains information that is not necessarily relevant from an operational outsourcing-related risk perspective like the estimated budget cost. What is more, the IK strongly disagrees with the EBA's approach. The table "List of Activities" should be deleted completely as it comprises some activities such as "legal advice" which are – according to the well-established supervisory practice of national competent authorities – not regarded as outsourcing.

VII. Comments on EBA's question no. 7

[Question 7: Are the guidelines in Sections 9.1 regarding the assessment of criticality or importance of functions appropriate and sufficiently clear?]

1. The IK disagrees with the EBA's approach to provide for a comprehensive set of criteria that need to be assessed in any case. Instead, the IK suggests replacing the texts of Section 9 and 9.1 (in line with the BaFin's MaRisk, AT 9 no. 2) by the following wording:

"*Based on a risk analysis, the institution or payment institution shall determine independently which outsourced activities and processes it regards as critical and important in terms of risk. The relevant organizational units shall be involved in conducting the risk analysis. The internal audit function shall also be involved within the scope of its duties. The risk analysis shall be adjusted to any material changes in the risk situation. The risk analysis shall take into account all aspects of the outsourced activities and processes that are relevant to the institution (eg outsourcing risks, suitability of the service provider); the intensity of the analysis shall depend on the nature, scale, complexity and riskiness of the outsourced activities and processes.*"

2. Besides, the IK is of the opinion that the term "***relate to*** *core business lines and critical functions*" in no. 50 is too vague and should by replaced by "***processes or services that form an integral part of*** *core business lines and critical functions*".

3. The fact that an outsourcing arrangement is not substitutable in an appropriate time frame should only be relevant for the outsourcing of critical and important functions. The wording in no. 52 should therefore be amended accordingly.

VIII. Comments on EBA's question no. 8

[Question 8: Are the guidelines in Section 9.2 regarding the due diligence process appropriate and sufficiently clear?]

1. Due diligence requirements set out in Section 9.2 should refer to outsourcing of critical and important functions only.

2. The provision in no. 56 does not seem necessary from a financial supervisory risk-based perspective. It should therefore be deleted.

IX. Comments on EBA's question no. 9

[Question 9: Are the guidelines in Section 9.3 regarding the risk assessment appropriate and sufficiently clear?]

The IK deems inappropriate that requirements set out in Section 9.3 shall apply regardless of whether or not an arrangement is regarded as outsourcing. The wording in no. 57 should therefore be replaced by the following:

"*Outsourced activities and processes that are not regarded as critical and important shall be subject to the general requirements relating to a proper business organization and risk management. For the outsourcing of critical and important functions the following applies:*"

X. Comments on EBA's question no. 10

[Question 10: Are the guidelines in Section 10 regarding the contractual phase appropriate and sufficiently clear; do the proposals relating to the exercise of access and audit rights give rise to any potential significant legal or practical challenges for institutions and payment institutions?]

1. Requirements set out in Section 10 no. 63 should – with due regard to the principle of proportionality and a consistent risk-based approach – not refer to all, but to outsourcing of critical and important functions only.

Otherwise the fulfillment of these requirements would be too onerous and time-consuming and increase costs for institutions and payment institutions significantly.

2. More particularly, no. 63 g. and h. shall be deleted completely.

From a practical perspective it would not suffice to allow that e.g. the – required – full rights of information, access and audit are exercised in a risk-based manner (e.g. by relying on third-party audit reports or certifications), if these rights must be contractually assured in any case. Negotiating respective contractual provisions as such, for example, will already be extremely time-consuming and will lead to increased overall costs for institutions and payment institutions if that requirement also applies to any kind of basic, low-risk outsourced service.

3. In Section 10.1 (Sub-outsourcing of critical or important functions) it should be made clear that the requirements set out in no. 65 a. – h., no. 66 and no. 67 only apply to "sub-outsourcing of important and critical functions".

4. Section 10.3 (Access, information and audit rights) should – with due regard to the principle of proportionality and a consistent risk-based approach – only apply to outsourcing of critical and important functions and should therefore be amended and at the beginning the following wording shall be inserted:

"*For the outsourcing of critical and important functions the following applies:"*

5. Section 10.4 (Termination rights) shall, in its no. 81 c. be amended in that:

"… (such as sub-contractings for critical and important functions or changes in sub-contractors for critical and important functions …"

XI. Comments on EBA's question no. 11

[Question 11: Are the guidelines in Section 11 regarding the oversight on outsourcing arrangements appropriate and sufficiently clear?]

Requirements set out in Section 11 should – with due regard to the principle of proportionality and a consistent risk-based approach – not refer to all, but to outsourcing of critical and important functions only.

XII. Comments on EBA's question no. 12

[Question 12: Are the guidelines in sections 12 regarding exit strategies appropriate and sufficiently clear?]

Requirements set out in Section 12 should – with due regard to the principle of proportionality and a consistent risk-based approach – not refer to all, but to outsourcing of critical and important functions only.

XIII. Comments on EBA's question no. 13

[Question 13: Are the guidelines in Section 13 appropriate and sufficiently clear, in particular, are there any ways of limiting the information in the register which institutions and payment institutions are required to provide to competent authorities to make it more proportionate and, relevant? With a view to bring sufficient proportionality, the EBA will consider the supervisory relevance and value of a register covering all outsourcing arrangements within each SREP cycle or at least every 3 years in regard of the operational and administrative burden.]

The obligation to maintain an updated register relating to **all** outsourced activities is defined too broadly and does not entail regulatory benefits. The IK is of the opinion that – with due regard to the principle of proportionality and a consistent risk-based approach – it should only be mandatory to maintain an updated register for outsourcing of important and critical functions.

XIV. Comments on EBA's question no. 14

[Question 14: Are the guidelines for competent authorities in Title V appropriate and sufficiently clear?]

1. Certain regulatory provisions which the GL refer to are not applicable to payment and e-money institutions. Therefore explicit exemptions for payment and e-money institutions should be made where the GL are based on or refer to the EBA's guidelines on SREP (EBA/GL/2018/03).

No. 103 of Title V – Guidelines on outsourcing addressed to competent authorities (page 47) should therefore not apply to payment and e-money institutions.

2. No. 98 (audit and excess rights) should only refer to "*outsourcing arrangements for important and critical functions".*

3. In line with our comments on Section 5 (conflicts of interest), no. 101 d. should not apply to payment institutions on a solo-basis.

XV. Comments on EBA's question no. 15

[Question 15: Is the template in Annex I appropriate and sufficiently clear?]

In the IK's Opinion the template in the Annex is far to detailed. Besides it contains information that is not necessarily relevant from an operational outsourcing-related risk perspective like the estimated budget cost. What is more, the IK strongly disagrees with the EBA's approach. The table "List of Activities" should be deleted completely as it comprises some activities such as "legal advice" which are – according to the well-established supervisory practice of national competent authorities – not regarded as outsourcing.

XVI. Comments on EBA's question no. 16

[Question 16: Are the findings and conclusions of the impact assessments appropriate and correct; where you would see additional burden, in particular financial costs, please provide a description of the burden and to the extent possible an estimate of the cost to implement the guidelines, differentiating one-off and ongoing costs and the cost drivers (e.g. human resources, IT, administrative costs, etc.)?]

Please see our answers above, particularly to Question 1.

Yours sincerely,

On behalf of the IK (Interessengemeinschaft Kreditkarten):

Dr. Markus Escher / Daniela Eschenlohr