# figo's consultation input on the supervision of dedicated interfaces under PSD2

## Background information

Until August 13th, 2018 the European Banking Authority (EBA) consulted with market participants on some new draft guidelines regarding the supervision of dedicated interfaces to be offered by banks under the revised Payment Service Directive (PSD2).

These guidelines are supposed to clarify issues identified by market participants and authorities in relation to the four conditions to be met to benefit from an exemption from the fallback option envisaged under Article 33(6) of the Regulatory Technical Standards on SCA and Communication (RTS). Or to put it more simply, the guidelines - planned to apply from January 1, 2019 - aim at regulating how national authorities, such as the BaFin in Germany, are going to assess if a bank offers a PSD2 and RTS compliant dedicated interface. In a second step, such positive assessment means that the bank is exempted from the obligation to offer an alternative direct access for third party providers. So even if these guidelines are addressed to national authorities, they have quite an impact on our future open banking market in Europe.

As it might take a while for the EBA to publish all consultation input and as figo would like to offer some background information today, we herewith decided to publish our input. Please note that general consultation papers by the EBA contain specific questions that need to be answered using an online form. This time figo answered **ten questions** regarding the draft guidelines under consultation on August 10th, 2018. Please find our answers on the following pages. And in advance some PSD2ish to be prepared:

- Account Servicing Payment Service Provider (ASPSP) is referring to banks and other payment services providers, offering access to payment accounts under PSD2
- Third Party Providers (TPPs) is for our purposes referring to Account Information Service Providers (AISP) and Payment Initiation Service Providers (PISP)
- Payment Service User (PSU) is supposed to benefit from PSD2 the most, i.e. it's the consumer of open banking.

# EBA consultation input by figo

## Question 1: Do you agree with the EBA's assessments on KPIs and the calculation of uptime and downtime and the ASPSP submission of a plan to publishing statistics, the options that EBA considered and progressed or discarded, and the requirements proposed in Guideline 2 and 3? If not, please provide detail on other KPIs or calculation methods that you consider more suitable and your reasoning for doing so.

figo GmbH (figo) has always been fostering the idea of KPIs as clear Compliance requirements for dedicated interfaces. A list of specific KPIs such as provided by the EBA by means of the drafted Guideline 2 is a good start. With regard to the EBA's Guideline 3, figo sees a broad need for optimisation as it is striking that important factors for a smoothly functioning, well-supervised and therefore innovative EU open banking market have not yet been considered. We are well aware that parts of the RTS were already unfortunate in that regard and that in most cases the EBA can only provide clear incentives to foster the following optimisation measures for the benefit of all involved parties, including the EBA itself and CAs on national level. Consequently, we will also provide according incentive ideas. figo would like to outline the following recommendations (details to each point can be found below):

(1) Clarify that all interfaces by the ASPSPs to PSUs and TPPs are covered

(2) Clarify that different PSUs/TPPs can cause one downtime

(3) TPP access and clustering of data per TPP is needed for root cause determination

(4) Response times have to be reported in percentiles

(5) A joint and access restricted KPI web platform on EU level is needed

(6) Data must be published real-time, i.e. at least on a daily instead of a quarterly basis

(7) Offer incentives to ASPSPs in order to get support for such an approach – i.e. (1) to (6)

### (1) Clarify that all interfaces by the ASPSPs to PSUs and TPPs are covered

Initially it should be clarified as part of Guideline 2 or 3 or as part of provided rationales, that the EBA's intention behind the wording of Guideline 2.1: "interface(s)" was to be able to compare service

level, objectives and targets for all online interfaces an ASPSPs is providing to PSUs (e.g. incl. mobile) as well as to TPPs.

In this way one could avoid that ASPSPs choose an inappropriate interface for comparison or that any unnecessary administrative efforts are prevented, which would be needed to determine the most comparable interface by ASPSPs in a first and CAs in a 2nd level step.

**(2) Clarify that different PSUs/TPPs can cause one downtime**

Due to the original wording of Art. 33 (1) of the RTS and therefore the final definition of a "downtime", we only recommend that the EBA clarifies as part of Guideline 2.2 / 2.4b, that the referred to "five consecutive requests for access" must not need to be undertaken by a single PSU nor a single TPP, but could also be undertaken by different PSUs/TPPs.

**(3) TPP access and clustering of KPI data per TPP is needed for root cause determination**

TPP access to KPI data is beyond other reasons also needed to distinguish between the originators (ASPSP or TPP) of downtimes or delayed response times.

To avoid ASPSPs to be sanctioned for uncaused non-compliance, KPIs should be clustered by TPPs as part of the reporting. In this way all parties, including CAs would get an idea of statistical outliers on TPPs side. Also TPPs would be able to compare themselves to other TPPs and could work on potential root cause problems on their side.

So a clustering of availability and performance KPIs by TPPs is highly recommended.

**(4) Response times have to be reported in percentiles**

With regard to the draft of Guideline 2.3 figo would like to point out that no clarification is provided on how to calculate such performance indicators, i.e. response times. We highly recommend to clarify as part of Guideline 2 how to report "the time taken" (3 times used wording in Guideline 2.3) in a consolidated way. We think it would not help the purpose of KPI monitoring, if ASPSPs reported on the basis of simple average figures - or even worse - in any kind of abstract bad/ok/good categories.

In best case all indicators referred to in **2.3 a., b., c.** should be provided in EBA-specified percentiles, i.e. aggregated on certain user percentages:

- 90 % of users/TPPs had a response time of X seconds on average
- 95 % of users/TPPs had a response time of X seconds on average
- 98 % of users/TPPs had a response time of X seconds on average

- 99 % of users/TPPs had a response time of X seconds on average

Those metrics should moreover be clustered adequately in different URLs and methods, i.e. get/post/put/delete events.

**(5) A joint and access restricted KPI web platform on EU level**

Indicators in line with our aforementioned recommendations, publicly accessible on ASPSPs websites could actually lead to some cyber and information security as well as competition risks for ASPSPs.

The current draft of Guideline 3 therefore could lead to ASPSPs having good reasons for only providing restricted access to such information on their website. This is worrying on the other hand, because it means a lot of administrative effort - mainly for authorities and TPPs to connect to each bank's data for connectivity monitoring. And it's more than an obstacle to innovation to have each bank in Europe come up with their own front-ends for according publication needs resulting in fragmented and inconsistent data.

Therefore, we highly recommend to implement a central online information point to gather such data in standardised formats. And consequently, publishing according KPIs should be limited to a joint and access restricted KPI web platform on EU level, to which only the publishing ASPSPs, all competent authorities and TPPs are granted access.

Due to cross-border TPP cases and expanding open banking players in Europe, joint platforms on national level would be too short-sighted.

**(6) Data must be published real-time, i.e. at least on a daily instead of a quarterly basis**

Provided there is a safe, i.e. access restricted, KPI web platform, ASPSPs might as well publish their daily statistics - or even in real-time instead of gathering data for quarterly terms.

All involved parties can benefit from a real-time monitoring of availability and performance, e.g. for root cause determination, etc.

**(7) Offer incentives to ASPSPs in order to get support for such an approach – i.e. (1) to (6)**

In order to foster the aforementioned approach, clear incentives are needed for ASPSPs, such as:

- ASPSPs who provide real-time data to a joint and access restricted KPI web platform on EU level (which is content wise in line with the final Guideline 2) - are not obliged to provide any additional reports, e.g. to national authorities on a quarterly basis.

- Moreover and more important, the EBA and CAs commit to a mid- or at least long-term strategy on how to automate their own obligation of monitoring and stress-testing acc. to Art. 32 (2) of the RTS on the basis of this joint and access restricted KPI web platform on EU level. The EBA and CA's would be able to consolidate and nationally compare developments on interfaces, indicators and targets and therefore would also be able to easily track compliance with RTS by ASPSPs as well as by CAs (see also Question 3).

- By means of a central database, average availability/performance data across Europe could be easily obtained and used as a basis to actually define specific numeric availability and performance targets for each of the KPIs. Considering rationale 23 of the Draft Guidelines on hand and why those minimum targets have not been considered so far, an approach that includes the gathering of availability/performance data on average across Europe, would already help to detect statistical outliers in a short-term, be it at ASPSPs or even at country level. At a later stage, the EBA would even be enabled to define specific numeric availability and performance targets per country and cross-border (for the latter longer response times due to distance of servers could define different targets).

- Last but not least an incentive for ASPSPs could be that CAs are enabled by the EBA to check API availability/performance KPIs on the level of common technical service providers, as far as banks have outsourced the operation of dedicated interfaces. Administrative efforts for all parties would be minimised, if technical service providers took care of performance/availability reporting for a certain multitude of ASPSPs.

**Question 2: Do you agree with the EBA's assessments on stress testing and the options it considered and progressed or discarded, and the requirements proposed in Guideline 4? If not, please provide your reasoning.**

figo highly recommends to integrate - at least high level - stress testing results into the aforementioned joint and access restricted KPI web platform on EU level (please see Questions 1). Any benchmarks could then be challenged and aligned per country or per size of APSPSs by CAs and the EBA itself and by means of very manageable efforts.

Moreover, we strongly recommend to include some useful relation within Guideline 4.1 with regard to "an extremely high number of requests". For example to comprehensible and common peak traffic days/periods such as paydays, tax return season, etc.

**Question 3: Do you agree with the EBA's assessments on monitoring? If not, please provide your reasoning.**

Legislators and regulators are expecting and requiring ASPSPs and TPPs to implement all kinds of technology nowadays in order to comply with regulation. Herewith, figo once again strongly encourages the EBA - jointly with CAs - to evolve in due course of innovation and commit to a clear strategy of developing a technical monitoring system on EU Level for the supervision of dedicated interfaces under PSD2.

The Guidelines under consultation are addressed to CAs and should include a clear commitment by the EBA as well as CAs (the latter being required by RTS to consult with EBA regarding those processes) on defining future solutions on how to technically monitor dedicated interfaces in an automated, cost-efficient and future-proof way.

This commitment and the monitoring itself would be strongly fostered in a first but important step, if the EBA was to follow figo's approach on a joint and access restricted KPI web platform on EU level (see Questions 1 for details). As a joint database and with over 6.000 ASPSPs in Europe; the EBA and CAs would be enabled to consolidate and compare developments on interfaces, indicators and targets - each on national and EU level - and therefore would also be able to easily track compliance with RTS by ASPSPs as well as by CAs on their own requirements.

In a second and long-term step, a strategy on automated monitoring could even include a direct way for CAs to test dedicated interfaces in an automated way, e.g. by CA's own testing interfaces/APIs. An essential starting point for this could be the joint and access restricted KPI web platform on EU level.

**Question 4: Do you agree with the EBA's assessments on obstacles, the options it considered and progressed or discarded, and the requirements proposed in Guideline 5? if not, please provide your reasoning.**

With regard to Guideline 5 and potential obstacles for TPPs, figo is mainly concerned about two points. First with the softening of the "no imposed redirect"- standard and second with solely debating TPP access obstacles, which could lead to losing track of important other obstacles that also could cause material business model risks for TPPs, such as misused GDPR conflicts/grey zones.

**Softening of the "no imposed redirect"- standard by Art. 32 (3) of the RTS**

The debate on redirection is almost as old as PSD2 itself and one should finally put an end to it – neither the Commission with leaving room for interpretation by using the three letter word "may" nor the EBA by providing the Guidelines on hand have yet achieved this goal, as the current draft does not consider a balanced trade-off.

Let us just quote PSD2 with its Level One rationale No 69, that already contained: *"However, terms and conditions or other obligations imposed by payment service providers on payment service users in relation to keeping personalised security credentials safe should not be drafted in a way that prevents payment service users from taking advantage of services offered by other payment service providers, including payment initiation services and account information services. Furthermore, such terms and conditions should not contain any provisions that would make it more difficult, in any way, to use the payment services of other payment service providers authorised or registered pursuant to this Directive."* as this rationale pretty much described the intentions of PSD2 legislators that should be considered when regulating re-directs. According to the meaning and purpose of this rationale any contradicting practical/technical implementations by ASPSPs would contradict PSD2 as well.

The EBA's approach to simply conclude that „*The use of what is commonly referred to as 'redirection' is not in itself an obstacle.*" (see rationale 35 of the Guidelines under consultation) without making clear what a non-obstacle redirection could look like, does neither clarify the handling of redirection for competent authorities or market players, nor does it help the EBA to fulfil its statutory mandate of bringing about regulatory and supervisory convergence across the EU and to support the objectives of PSD2 to contributing to a single EU payments market.

On the contrary, CAs in countries with a still small or "scraping-only TPP"-market will tend to accept hindering redirect solutions, compared to CAs of countries with a better developed TPP-market and API experience, where the consequences of hindering redirection are recognised much better (and at the same time meaning more efforts for the CAs to assess if a redirection is an obstacle by checking this on a very deep technical level). Moreover the latter group does not resemble the majority of CAs in EU countries, which could raise its concerns in an audible manner. figo is very concerned that a pro-redirect lobby group is currently working against the objectives of PSD2 and for its own competitive advantages, be it on a political/national/CA or industry level.

A reasonable question by EBA would be now: why is no TPP initiative currently running a big counter campaign against the EBA approach? Well officially, because solutions are discussed as part of an API Evaluation group, which includes - again - "scraping only TPPs" and bank representatives. And unofficially, because those TPPs might have eventually lost trust in finding any trade-offs on a regulatory level, that would suit their needs and already have come up with their own practical, legally sound but likely non-innovative fall back solutions. In a worst case scenario this would result in the following: imposed but hindering redirects could lead to TPPs scraping redirect front-ends of dedicated interfaces. This sentence itself is a farce. Even if this approach meant higher TPP-internal efforts, it would secure not losing the high user experience standards, crucial to their business cases. These TPPs would do so, referring to material PSD2 principles and rights, such as:

- using credentials issued by the ASPSP and relying on their authentication procedures and
- actually being regulated as PISP or AISP due to the fact that credentials were wanted to be processed in line with regulatory standards; as a focus of PSD2 obligations is obviously put on the processing of credentials by TPPs.

A worst case result such as that would bring PSD2 ad absurdum and all work and years of debate by everyone involved would have been wasted.

When debating a final redirect wording, the EBA should also take a look to the UK. However, not to take it as a role model for a great redirect solution, but as a warning why after six months of dedicated interfaces being implemented and live, those interfaces do not seem to be in any commercial use (see for example here).

Considering these points, plus recognizing that for more than 6000 EU interfaces a non-obstacle redirect is hardly auditable, figo sees two possibilities for the EBA to react according to our justified concerns, at least if the EBA wants to hold on to its general interpretation of the RTS on redirection:

(1) The best case due to less efforts for ASPSPs and CA's: figo proposes that it should be clarified within the guidelines on hand what kind of features on high level are expected for a non-obstacle redirection, such as:

- a frictionless Oauth Flow serving the specifics of different use cases and front-ends (e.g. mobile vs. non-mobile) plus
- a TPP token management for the purpose of permanent and especially AIS use cases (compare Art. 36 (5b) of the RTS) so that users do not have to be redirected for SCA repeatedly, e.g. to update several accounts of third-party banks in a multi-banking solution.

These minimum features could be used by ASPSPs to prove compliance with the requirement of not providing a hindering redirect.

(2) Alternate 2nd best solution, because it involves unnecessary effort for ASPSPs: figo proposes alternatively a clear statement that a redirection option offered by the ASPSP must not be imposed by using it as the sole method of access for the dedicated interface. If ASPSPs' redirect solutions are frictionless and smart to a merchantable extent, a TPP will make use of it on a voluntary basis. So another way to foster non-obstacle redirection that suits market and security needs, would be to offer it besides an embedded/decoupled approach. The corresponding – solely ASPSP-friendly – wording of rationale 36 on more than one method of access would have to be adapted by the EBA accordingly.

**Important other obstacles not to lose track off**

Last but not least, current obstacle examples and debates as well as the draft on Guideline 5 on hand are solely focussed on methods of access, including authorisation. figo is concerned though that there is material potential for other obstacles. For example in the form of ASPSPs finding ways NOT to provide AISPs with the same information from designated payment accounts and associated payment transactions made available to the PSU as required by Art. 36 (1a) of the RTS.

First of all, the initial exemption included within Art. 36 No. 1a of the RTS ("provided that this information does not include sensitive payment data") already leaves room for interpretation as sensitive payment data is - if at all - only defined in detail (i.e. specific data sets) on national and or practice level.

And second, still open debates on conflicts and unsolved grey areas between conflicting goals of PSD2 and GDPR could foster intended non-compliance by ASPSPs for competitive reasons. ASPSPs for example could alter account information, based on the need to protect silent party data within transaction details, referring to GDPR-compliance purposes. From our point of view initial attempts to clarify such conflicts by the European Data Protection Board were rather useless and concentrated - again - on PIS only, while the risk for operating AIS, when AISPs are not being provided account information to the usual extent, is substantially higher.

figo is aware that the EBA cannot conclusively decide on data protection matters, however strongly advises the EBA to consider and regulate as part of Guideline 5 some practical processes for the EBA and CAs when it comes to necessary EU level agreements on any obstacles resulting from PSD2 vs. GDPR conflicts - especially during the initial implementation phase of dedicated interfaces.

**Question 5: Do you agree with the EBA's assessments for design and testing, the options it considered and progressed or discarded, and the requirements proposed Guideline 6? If not, please provide your reasoning.**

Also according to the process of the design and testing to the satisfaction of PSPs, figo strongly encourages the EBA - jointly with CAs - to evolve in due course of innovation and commit to a clear strategy of developing a technical testing system on EU Level for the supervision of dedicated interfaces under PSD2.

When reading Guideline 6, it's quite obvious that the whole process of test reportings and auditing results will lead to huge and for sure avoidable administrative efforts for CAs, i.e. huge efforts to assess the divers testing result input by various ASPSPs.

Therefore, we highly recommend a commitment by the EBA and CAs on striving for a strategy for an automated testing of dedicated interfaces, e.g. by CAs or EBA's own testing interfaces/APIs (working with all offered and RTS-necessary API endpoints themselves, to test compliance continuously). An essential starting point for this would already be the aforementioned KPI monitoring web platform on EU level.

Consequently, figo already addressed the idea of authority testing interfaces/APIs as part of the EBA hearing on these guidelines on July 25th, 2018. The EBA's reaction with regard to the specific question on what kind of hurdles the authority is facing, when considering such innovative step for the EBA as well as CAs in order to consider them for this consultation was disappointing though. The EBA's representative replied "the obvious". This cannot be a serious answer when, the EBA on the other hand is expecting and requiring ASPSPs and TPPs to implement all kinds of technology nowadays in order to comply with regulation and even in order to foster innovation as part of PSD2. The regulator has to evolve simultaneously to achieve PSD2's goals and a smoothly functioning, well-supervised and therefore innovative EU open banking market.

Guideline 6 under consultation is addressed to CAs and should include a clear commitment by the EBA as well as CAs (the latter being required by RTS to consult with EBA regarding those processes) on defining future solutions on how to technically test dedicated interfaces in an automated, cost-efficient and future-proof way for supervision purposes.

**Question 6: Do you agree with the EBA's assessment for 'widely used', the options it considered and discarded, and the requirements proposed Guideline 7? If not, please provide your reasoning.**

The aforementioned joint and access restricted KPI web platform on EU level could be extended by all information required under Guidenline 7. By gathering such information transparently with reading access for TPPs, ASPSPs would automatically be challenged regarding the traceability of the ASPSPs documentation on its interface usage which could result in way less audit efforts for CAs.

**Question 7: Do you agree with the EBAs assessment to use the service level targets and statistical data for the assessment of resolving problems without undue delay,**

**the options it discarded, and the requirements proposed Guideline 8? If not, please provide your reasoning.**

The aforementioned joint and access restricted KPI web platform on EU level could be extended by the information required under Guideline 8.

Average problem response and solving times could be additional KPIs, offered on a platform with access for all involved parties so they can be automatically challenged by TPPs and monitored by CAs.

**Question 8: Do you agree with the proposed Guideline 9 and the information submitted to the EBA in the Assessment Form in the Annex? If not, please provide your reasoning.**

It actually seems self-explanatory to figo, what an extension of the use of an aforementioned KPI platform could also mean for the provisions of Guideline 9 and Art. 33 (7) of the RTS.

Let us just state the most simple reasons, why also for this process the EBA cannot ignore the chances of using such joint platform: Assessment Forms could be handled via that platform plus CA's and the EBA could automatically monitor, when the point is reached that an ASPSP is non-compliant with Art. 33 (6) of the RTS for more than two consecutive calendar weeks.

**Question 9: Do you have any particular concerns regarding the envisaged timelines for ASPSPs to meet the requirements set out in these Guidelines prior to the September 2019 deadline, including providing the technical specifications and testing facilities in advance of the March 2019 deadline?**

As part of the hearing on July 25th, 2018 the EBA clarified verbally that it interpretes the three months testing to happen with live data. figo strongly recommends to make this clear as part of the guidelines on hand.

Regarding our overall consultation input and several referrals to an urgent need of innovation at the level of EBA and CAs, we would like to point out once again that an innovative open banking market in Europe cannot evolve as aimed for in PSD2, if authorities do not evolve in due course. That is why we highly recommend to at least find strong and clear commitments within these guidelines to implement initial basics to further foster a future-proof supervision of Open Banking interfaces in Europe. This could mean to use the remaining time of 2018 to check technical feasibilities of launching a minimum viable PSD2 interfaces KPI/monitoring/testing platform by March 2019 and

compare this solution to the current planning of the EBA with regard to efforts and costs for CAs and market participants.

And from our figo point of view and based on this reasoning the EBA in general cannot refer to the EU Commission for regulating an evolved Open Banking market since PSD2 was finalised (as also done by the EBA during the hearing on these guidelines on July 25th, 2018). Of course, the EBA cannot conclusively regulate account access beyond payment accounts. However, simple and practical approaches can be undertaken now when it comes to the supervision of PSD2 APIs, instead of initiating years (!) of new debates that do not help anyone, except for e.g. US market players catching up with our narrow EU lead in Open Banking innovation.

figo herewith offers further active support to the EBA as well as to CAs in drafting such concepts, e.g. by being a sparring partner and/or further consulting on the usability from a market perspective.

**Question 10: Do you agree with the level of detail set out in the draft Guidelines as proposed in this Consultation Paper or would you have expected either more or less detailed requirements on a particular aspect? Please provide your reasoning.**

For the current content the level of detail would be sufficient. If recommendations by figo are to be considered, one could consider further - but rather separate - guidance on the usage of a joint PSD2 interfaces KPI/monitoring/testing platform for example.