Contribution to EDPB Guidelines 06/2020

We welcome the fact that the European Data Protection Board (EDPB) with its Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR provides further guidance on data protection aspects in the context of Payment Initiation Services ("**PIS**") and Account Information Services ("**AIS**") in terms of PSD2. The access and the use of payment and account information services are, as EDPB also highlights in its guidelines, the rights of the payment service user ("**PSU**") and, as such, correlate with the aim of the General Data Protection Regulation ("**GDPR**") to empower individuals and give them control over their personal data.

The guidelines in its current version, however, raise concerns that some of its considerations might be misinterpreted in way to create obstacles both to the above mentioned rights of the PSUs and to the Third Party Providers' ("**TPP**") right to provide services in accordance with the PSD2, in particular with respect to the implementation of technical measures at the time of data collection (usage of digital filters), the processing of special categories of personal data and silent party data by TPPs and the access to accounts other than payment accounts. We are happy to elaborate on this further and would appreciate a clarification on these aspects in order to avoid inconsistencies between PSD2 and GDPR.

1. Granting access to payment account data by ASPSPs to TPPs - a legal obligation under PSD2

We welcome EDPB's clarification that the processing of personal data by the Account Servicing Payment Service Provider ("**ASPSP**") consisting of granting access to the personal data requested by the PISP/AISP in order to perform their payment service to the PSU is based on a legal obligation and accordingly, *"the applicable legal ground is Art. 6(1)(c) of the GDPR".*[1] This applies to personal data of the PSU and notably also to silent party data (see point 3.2, below).

EDPB explains that

> *25. As mentioned in paragraph 10, payment service users can exercise their right to make use of payment initiation and account information services. [...] The effective application of such rights would not be possible without the existence of a corresponding obligation on the ASPSP, typically a bank, to grant the payment service provider access to the account under the condition that it has fulfilled all requirements to get access to the account of the payment service user. Furthermore, Articles 66(5) and 67(4) of the PSD2 state clearly that the provision of payment initiation services and of account information services shall not be dependent on the existence of a contractual relationship between the PISP/AISP and the ASPSP.*

[1] EDPB: Guidelines 06/2020 on the interplace of the Second Payment Services Directive and the GDPR, Version 1.0, Adopted on 17 July 2020, p. 10, para. 26

The European Banking Authority ("**EBA**") and the European Commission have clarified that in the context of PSD2 and its implementation via the delegated Regulation EU 389/2018 of 27 November 2017 ("**RTS**"), banks shall not check whether the account-holder has given his consent, which is the legal responsibility of the regulated TPPs. Demanding additional checks would amount to an illegal obstruction of access to account in violation of Art. 68 (5) PSD2 and Art. 32 (3) RTS, see EBA opinion of June 4 2020 (EBA/OP/2020/10), para 43:

„*Article 32(3) RTS explicitly mentions additional checks of the consent given by PSUs to AISPs/PISPs as a potential obstacle. The EBA clarified in paragraph 13 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)14 and the final report on the EBA Guidelines on the exemption from the contingency mechanism under Article 33(6) RTS (EBA/GL/2018/07)15 that it is the obligation of the PISP/AISP to ensure that it has obtained the PSU's explicit consent in accordance with Article 66(2) of PSD2 and, respectively, Article 67(2)(a) of PSD2, and that the ASPSP should not check the consent given by the PSU to the PISP/AISP. This was also confirmed by the European Commission in its response to Q&A #4309*[2]*".*

As the European Commission set out in these Q&A #4309, an ASPSP *"is only entitled to deny an AISP or PISP access to a payment account on its own initiative for justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that specific PISP or AISP (Article 68(5) PSD2). When blocking the access the ASPSP shall immediately report the incident to the relevant competent authority. PSD2 thus provides adequate safeguards to ensure that PISPs and AISPs do not have unauthorised access to payment accounts."*

In this context, we would welcome a clarification that it is not the ASPSPs' responsibility to assess whether the requirements to get access to the account of the payment service user have been fulfilled by the TPP (PISP or AISP), but that it is the TPP's obligation to access and process data in accordance with PSD2 and GDPR. In other words, the ASPSP has no role or duty under the GDPR to withhold data from TPPs that are licenced and regulated under PSD2, as he is legally obliged to share the data and to enable the use of TPPs by account-holders.

Accordingly, we propose to add the following clarification:

It is the TPP's (PISP's / AISP's) obligation to access and process data in accordance with PSD2 and GDPR. The ASPSP should not (double)check the consent given by the PSU to the PISP/AISP. Demanding additional checks would amount to an illegal obstruction of access to account in violation of Art. 68 (5) PSD2 and Art. 32 (3) RTS, see EBA opinion of June 4 2020 (EBA/OP/2020/10 para 43).

[2] See: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4309. The Commission states therein: [An ASPSP] is only entitled to deny an AISP or PISP access to a payment account on its own initiative for justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that specific PISP or AISP (Article 68(5) PSD2). When blocking the access the ASPSP shall immediately report the incident to the relevant competent authority. PSD2 thus provides adequate safeguards to ensure that PISPs and AISPs do not have unauthorised access to payment accounts.

This corresponds with the principle of "data parity" in terms of Art. 67 (3)(b) PSD2, Art. 36 (1) (a) RTS according to which, in relation to payment accounts, the account servicing payment service provider *"shall treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons*" (Art. 67(3)(b) PSD2) and needs to provide "*account information service providers* ***with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information****, provided that this information does not include sensitive payment data*" (Art. 36 (1) (a) RTS).

In its opinion dated 13 June 2018, the European Banking Authority (EBA) further clarified that AISPs need to be granted access to the maximum amount of data available to the PSUs (EBA-Op-2018-04, 13 June 2018, recital 20): "*The EBA clarifies that the AISPs can access the maximum amount of data available to PSUs with regard to their payment account(s) held with a specific ASPSP regardless of the electronic channel (e.g. mobile application or web) used to access it*."

Accordingly, it is the ASPSPs' legal obligation to grant access to the personal data requested by the PISP and AISP without limitation. And it is the TPPs' responsibility to assess in the individual case what processing of personal data is objectively necessary to perform the contract (as indicated by the EDPB in chapter 2.2 para. 15 of the guidelines) or otherwise, whether the access to and processing of payment account data is permissible on another legal basis, such as the PSU's consent in terms of Art. 6 (1)(a) GDPR or Art. 6 (1)(f) GDPR for silent party data (see more under 3.2, below).

The reason for us to ask for a clarification in this respect lies in the history of PSD2 and its very purpose: TPPs had been illegally denied access to account by some ASPSPs based on various pretexts, including but not limited to data protection and security. The German Federal High Court (BGH, Germany' highest civil Court) only very recently confirmed the finding of the German Federal Cartel Office (FCO) that banks thereby intentionally violated antitrust law (BGH, KVR 13/19 of 7 April 2020), using pretexts to foreclose competition.[3]

PSD2 has included TPPs in order to remove these obstacles and ensure a regulated open access to payment accounts, clarifying that banks' terms and conditions "*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."*

We would like to make sure that the EDPB's comments are not used for yet another attempt in restricting access to account (X2A). We therefore believe it should be clarified that GDPR governs TPP's handling of the data, but does not grant ASPSPs a right to restrict X2A.

[3] See press release of the FCO: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/AktuelleMeldungen/2020/08_05_2020_BGH-Entscheidung_Deutsche_Kreditwirtschaft.html;jsessionid=138396E394E0B2BF719F80D9270D50C1.2_cid371

2. Access to other accounts types

As EDPB correctly states, PSD2 is restricted to access to payment accounts. The current wording of the guidelines, however, may leave room for the misinterpretation that as a consequence, access to other account types is not permitted.

> *64. It should also be noted in this regard that under the PSD2, ASPSPs are only allowed to provide access to payment account information. There is no legal basis under the PSD2 to provide access with regard to personal data contained in other accounts, such as savings, mortgages or investment accounts. Accordingly, under the PSD2, technical measures have to be implemented to ensure that access is limited to the necessary payment account information.*

Considering the above mentioned right of the payment service user to access and use of payment and account information services we would welcome a clarification that this is not the right conclusion to take. The fact that other account types are not covered by PSD2 does not mean that access to such accounts is generally excluded, but - for lack of regulation in the PSD2 - rather subject to general data protection law, in particular the GDPR. There is no objective reason why the data subjects' (PSUs') right to have control over their data should be limited to payment accounts.

To the contrary: The PSU has the right to grant his consent under Article 6 (1) lit a GDPR, and ASPSPs indeed are under an obligation to enable sharing the account data under Article 20 GDPR (Right to data portability).

The above-mentioned decision of the German Federal High Court (BGH KVR 13/19) of 7 April 2020 and the German FCO concerned the legal situation before PSD2 came into force in Germany as of 13 January 2018. It correctly reflects the legal rights and obligations of TPPs and banks outside of PSD2. Hence the fact that banks are neither legally free nor obliged to restrict access to account applies to non-payments accounts outside of PSD2 - as established and documented in that precedent. In that case, data protection had been discussed and dismissed as a legal basis for banks' blockade of X2A.

Accordingly, we propose to add the following clarification:

The fact that other account types are not covered by PSD2 does not mean that access to such accounts is generally excluded, but - for lack of regulation in the PSD2 - rather subject to general data protection law, in particular the GDPR.The PSU has the right to grant his consent under Article 6 (1) lit a GDPR, and ASPSPs indeed are under an obligation to enable sharing the account data under Article 20 GDPR (Right to data portability).

3. (Further) Processing of personal data by the TPPs

We would welcome a further elaboration on the processing of personal data by the TPPs, in particular with respect to the processing of special categories of personal data and of silent party data for other purposes than contract performance, such as anti-money laundering and fraud prevention. The legal basis for (further) processing of personal data by the TPPs very much depends on the individual case and requires a case-by-case assessment by the TPP.

3.1 Processing of payment service user data

EDPB states that

> *51. [...] At the same time, financial transactions can reveal sensitive information about individual data subject, including those related to special categories of personal data. For example, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes.[...] Therefore, the chances are considerable that a service provider processing information on financial transactions of data subjects also processes special categories of data.*
>
> *61. The TPP accessing payment account data in order to provide the requested services must also take the principle of data minimisation into account and must only collect personal data necessary to provide the specific payment services requested by the payment service user. As a principle, the access to the personal data should be limited to what is necessary for the provision of payment services. [...]*

We agree with the EDPB that financial transactions might reveal sensitive information about the individual data subject, including those related to special categories of personal data and as such, require a high level of protection. In case of special categories of personal data, the processing cannot be based on Art. 6(1)(b) or Art. 6(1)(f) of the GDPR, but is subject to the derogations in Art. 9(2) GDPR.

The guidelines suggest, however, that the processing of transaction characteristics - which for the most part do not contain special categories of data - are not necessary for the provision of PIS and AIS and therefore, should be excluded from processing.

> *57. As noted above, where the service provider cannot show that one of the derogations is met, the prohibition of Article 9 (1) is applicable. In this case, technical measures have to be put in place to prevent the processing of special categories of personal data, for instance by preventing the processing of certain data points. In this respect, payment service providers may explore the technical possibilities to exclude special categories of personal data and allow a selected access, which would prevent the processing of special categories of personal data related to silent parties by TPPs.*
>
> *62. When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories must be made by the AISP before the data are collected. For instance, data categories that may not be necessary may include [...] the transaction characteristics. [...]*

We would like to highlight that transaction characteristics form an essential part of PIS and AIS, for the purposes of providing the services including anti-money laundering and fraud prevention.

The guidelines lack clarity on the processing of special categories of personal data for anti-money laundering and fraud prevention purposes which to our understanding falls under the derogation of Art. 9(2)(g) GDPR. In particular, note 20 to para. 23[4] and para. 55 of the

guidelines create legal uncertainty for TPPs with respect to anti-money laundering obligations. Even though the processing of special categories of personal data related to the PSU can be based on the PSU's consent, it seems unreasonable to make the processing of special categories of personal data for anti-money-laundering and fraud prevention purposes dependent on a (revocable) consent of the data subject.

With respect to a pre-selection of relevant data categories by the AISP before the data are collected, as suggested by the EDPB in para. 62 of its guidelines, we would like to point out that this is often impossible, as it is not apparent before data collection whether or which transaction characteristics contain special categories of personal data. In order to be able to provide the service(s) requested by the PSU and/or comply with legal obligations, it is then necessary for TPPs to first collect the data and then select the relevant data points to be deleted or anonymized dependent on the nature, scope, context and purposes of processing in accordance with Art. 6 GDPR or Union law / Member State law.

It also needs to be considered that AISPs may take the role of a "processor" in the sense of Article 28 GDPR on behalf of the account-holder, in the same role as the ASPSP.

Where the account-holder is a private person not subject to GDPR, as a rule personal data in the sense of Article 9 GDPR relate to *his* personal life, so he may grant consent according to Article 9 (1) lit a GDPR. Only in rare cases might "silent" third parties conceivably make payments to a private person revealing categories in the sense of Art. 9. But this does not justify generally forgoing transaction characteristics. To the contrary, TPPs will only be able to discern and deselect such data in line with the GDPR once they see the transaction characteristics.

Based on the above, we suggest the following:

For the avoidance of doubt, para. 62 should be deleted. It should be highlighted that the ASPSP, on the one hand, has no role or duty under the GDPR to withhold (filter) data from TPPs that are licenced and regulated under PSD2. The processing of data by TPPs, on the other hand, is dependent on and limited to the purposes necessary to provide TPP services.

3.2 Processing of silent party data

We welcome the clarification of the EDPB that the processing of silent party data by the AISP or PISP can be the legitimate interest of the PISP/AISP to perform the contract with the PSU (account-holder) in terms of Art. 6 (1)(f) GDPR.

> *47. A lawful basis for the processing of silent party data by PISPs and AISPs - in the context of the provision of payment services under the PSD2 - could thus be the legitimate interest of a controller or a third party to perform the contract with the payment service user. [...]*

[4] EDPB: Guidelines 06/2020 on the interplace of the Second Payment Services Directive and the GDPR, Version 1.0, Adopted on 17 July 2020, p. 10: "*Note that a thorough examination of the question whether the anti-money laundering directive meets the standards of Art. 6(4) GDPR falls outside of the scope of this document*".

We also agree with EDPB that the processing of silent party data is necessary to perform the contract with the PSU.

The guidelines may suggest, however, that TPPs only need silent party data for the purpose of contract performance and that the further processing of silent party data is generally not permissible on the basis of Art. 6 (1)(f) GDPR.

> *47. [...] The necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects. [...] In this respect, the controller has to establish the necessary safeguards for the processing in order to protect the rights of data subjects. This includes technical measures to ensure that silent party data are not processed for a purpose other than the purpose for which the personal data were originally collected by PISPs and AISPs.*
>
> *49. With regard to further processing of silent party data on the basis of legitimate interest, the EDPB is of the opinion that these data cannot be used for a purpose other than that for which personal data have been collected, other on the basis of EU or Member State law. [...] The rights and freedoms of these silent party data subjects will not be respected if the new data controller uses the personal data for other purposes, taking into account the context in which the personal data have been collected, especially the absence of any relationship with the data subjects that are silent parties; [...]*
>
> *62. When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories must be made by the AISP before the data are collected. For instance, data categories that may not be necessary may include the identity of the silent party [...]. Also, unless required by Member State or EU law, the IBAN of the silent party's bank account may not need to be displayed.*

However, such interpretation would not take into account that the processing of silent party data may be necessary (indispensable) for other purposes such as anti-money laundering and fraud prevention or the performance of credit checks.

- First of all, the processing of silent party data for anti-money laundering purposes to our understanding falls below Art. 6(1)(c) GDPR in connection with Union and/or Member State law.

- The processing of personal data for fraud prevention purposes, on the other hand, is typically based on Art. 6(1)(f) GDPR. Such processing does not seem contradictory to the reasonable expectations of the silent parties, knowing that fraud prevention forms an essential and legitimate interest of the parties in connection with payment services. Also considering the limited scope of data (name and IBAN of the silent party) it is not apparent why the rights and freedoms of the silent party should generally prevail over the legitimate interests pursued by the TPP or by a third party, in particular when considering fraud prevention purposes.

  Indeed, Recital 47 to the GDPR itself explicitly states that the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.[5] There is no objective reason why

this should not apply to silent party data, under the condition that the rights and freedoms of these silent party data subjects are adequately considered by the TPPs in the context of a balancing exercise in terms of Art. 6(1)(f) GDPR and that appropriate technical and organizational measures are taken by the TPPs for the protection of silent party data (such as limited storage periods).

The question of which data may be necessary in the individual case depends on the individual service and scope of data processing; this requires a balancing exercise by the controller. For the purposes of clarification, we would like to name a few examples:

1) The PSU uses an AISP in context of a mobile app to provide financial oversight which includes a categorisation of spending and income according to different typologies (salary, leisure, energy, mortgage etc.): The processing of silent party data is necessary (indispensable) in order to perform the contract with the PSU.

2) The PSU uses an AISP for the purposes of informing his/her contractual partners on a change of bank accounts: The processing of silent party data is necessary (indispensable) in order to perform the contract with the PSU.

3) In order to fraudulently obtain a loan with a bank, the PSU pretends to have a regular income by means of “fake” transfers (a friend of the PSU transfers money with the payment purpose “salary” to the PSU who subsequently withdraws the money from an ATM and pays it back to his/her friend): Such fraud patterns can only be identified by analyzing the financial transactions, including silent party data. Without this information, the lending bank runs the risk of granting a loan to a PSU who is not credit-worthy. The analysis is indispensable to protect against fraud.

4) The PSU transfers money to a savings account which is also held by the PSU. This transaction can only be identified as “saving” by analysing the recipient. Pre-selecting the identity of the silent party before data collection in this case may result in the denial of a loan requested by the PSU although the money is not spent, but saved by the PSU for further expenses. Moreover, in this case the recipient data do not relate to any “silent” party but to the PSU himself. Furthermore, the analysis of the PSU’s spendings and savings helps the PSU to get an overview over his/her payment obligations and whether and to which extent he/she can afford the requested loan (e.g. whether the PSU can afford the leasing rate for a small car or for a middle class car).

Again, it will often be impossible to pre-select data points before collection, as it is not apparent before reviewing the data which financial transactions (including silent party data) are relevant for anti-money laundering or fraud prevention purposes or necessary to perform contractually agreed credit checks. TPPs will hence often need to perform a deselection of data once collected. EDPB seems to recognize this when saying in para 47 that PISP and AISP need to consider what parts of the data *“originally collected by PISPs and AISPs”* may

[5] Recital 47 GDPR: „[…] The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. […]”

be processed for a purpose other than the initial purpose (e.g. downloading the data on behalf of the account-holder for account information purposes).

Furthermore, we would like to highlight that silent party data often do not concern natural persons, but companies (phone providers, supplier of electric energy, insurances, banks, supermarkets, gas stations etc.) or public authorities and therefore, the processing of silent party data does not concern “personal data” and falls outside the scope of the GDPR.

Based on the above, we would welcome a more differentiated approach to the processing of silent party data in accordance with the GDPR and Union / Member State law, considering and balancing both the legitimate interests of TPPs and/or third parties and the rights and freedoms of the silent party in the individual case.

Therefore, we suggest the following:

For the avoidance of doubt, para. 62 should be deleted. It should be highlighted that the ASPSP, on the one hand, has no role or duty under the GDPR to withhold (filter) data from TPPs that are licenced and regulated under PSD2. The processing of data by TPPs, on the other hand, is dependent on and limited to the purposes necessary to provide TPP services.

About FinTecSystems GmbH

FinTecSystems GmbH is a B2B Fintech founded in 2014. On 01 March 2019, FinTecSystems received authorization from the German Federal Financial Supervisory Authority (BaFin) to act as a Payment Initiation and Account Information Service. With over 10 years of experience in the area of payment and FinTech (amongst others, at Sofort Überweisung), FinTecSystems GmbH’s management team has profound knowledge in the payment and banking sector. Our products accelerate loan commitments, minimise the risk of non-payment and categorise account data for our customers in real time. With access to over 6000 banks, FinTecSystems GmbH is market leader in the DACH region in the field of Open Banking. More than 150 companies put their trust in us, amongst them online merchants, price comparison websites, and banks.