1. Introduction

Open Banking Implementation Entity (OBIE) is a body which creates open API standards that enable firms throughout Europe to meet their relevant obligations under the second Payment Services Directive (Directive 2015/2366/EU) ("PSD2") for the provision of open banking services. We are therefore well-placed to understand the impact on both Account Servicing Payment Servicing Providers ("ASPSPs") and Third Party Providers ("TPPs")[1] of evolving regulatory requirements and guidance. Processing of personal data plays a fundamental part in the provision of open banking services and OBIE has ensured that its standards have been designed to assist entities adopting them to meet their relevant GDPR obligations.

OBIE is supportive of Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR ("Guidelines") issued by the European Data Protection Board ("EDPB") and has previously considered many of the issues that have been outlined. OBIE recognises the importance of providing a comprehensive assessment of the interplay between PSD2 and GDPR to ensure that both TPPs and ASPSPs can effectively comply with both legal frameworks.

Based on the expertise gathered in the Open Banking ecosystem, we would further like to raise the following key points:

2. Lawful Bases for Processing:

OBIE is broadly supportive of the proposed lawful bases for processing of personal data by both ASPSPs and TPPs. We note that PISPs and AISPs would likely rely on performance of a contract[2] as a basis for processing the personal data of the Payment Service User ("PSU"), in order to provide their payment service, however, they may also rely on legitimate interests[3] for certain aspects of their service offering.

Ultimately, our position is that controllers need to assess the most appropriate lawful basis for processing personal data in the context of their service offering.

Further, we agree that ASPSPs will likely rely on necessary for compliance with a legal obligation[4] basis for processing personal data in response to TPP requests.

3. Consent under PSD2 & GDPR

The distinction between consent and explicit consent under GDPR and PSD2 respectively is critical when considering the provision of open banking services. As it currently stands, there are four 'types' of consents that TPPs need to consider:

(i) Explicit consent which is needed for the provision of payment services in relation to CBPII[5], PISP[6] and AISP[7]

[1] TPPs include account information service providers ("**AISPs**") and payment initiation service providers ("PISPs")
[2] GDPR ,Article 6(1)(b)
[3] GDPR ,Article 6(1)(f)
[4] GDPR, Article 6(1)(c)
[5] PSD2, Article 65(2)(a)
[6] PSD2,Article 66(2) read in line with Article 64
[7] PSD2,Article 67(2)(a)

(ii) Explicit consent which is needed for accessing, processing and retaining personal data necessary for the provision of payment services[8]

(iii) Consent under the GDPR, where this is relied upon as a lawful basis for processing personal data[9] (where applicable)

(iv) Explicit Consent under the GDPR to process special category personal data, where required (e.g. where no other appropriate derogation exists)[10]

Due to the specific requirements relating to the use of consent as a lawful basis for processing personal data, we expect that many TPPs will choose to rely on a different lawful basis for processing personal data.

OBIE has created guidelines to assist TPPs in meeting their obligations in a way which keeps the customer informed, without causing unnecessary disruption to the customer journey. The Customer Experience Guidelines ("CEGs") predominantly focus on the principles of explicit consent for the provision of payment services under PSD2 and require TPPs to provide a complete set of information to the customer relating to their service. This is commonly referred to as the 'consent step'.

OBIE has further created the TPP Operation Guidelines, which expand upon GDPR principles including in relation to data privacy checklists, data breaches and rights of data subjects. We believe that this provides TPPs with important tools to help meet their compliance obligations with both PSD2 and GDPR in a holistic manner.

In developing the CEGs, OBIE also considered the complexities of using consent as a lawful basis for the processing of personal data by ASPSPs. OBIE concluded that the gathering of consent by ASPSPs within their customer journeys would not align with the provisions of the Regulatory Technical Standards on Strong Customer Authentication[11] ("SCA-RTS") relating to obstacles within customer journeys for ASPSP, which prevent ASPSPs from checking the consent granted by the PSU to the TPP[12]. The introduction of additional language to gather consent under GDPR within an ASPSP's authentication journey would inevitably result in a replay of consent under PSD2, resulting in an obstacle. We would be interested if this point were further explored in further guidance.

4. Silent Party Data and Special Category Personal Data

We broadly agree with the principles set out in relation to silent party data and that legitimate interests appears to be well placed as the appropriate lawful basis for processing silent party data. We note that silent party data will likely be more relevant in the context of account information services, where the data set requested will be richer. The majority of PISPs will not have access to silent party data in the provision of their service, although it is possible that a limited set of silent party data is processed within the payment instruction.

We are concerned by the suggestion in paragraph 57 relating to technical measures having to be put in place to prevent the processing of special categories of personal data, for instance by preventing the

[8] PSD2, Article 94(2)
9GDPR, Art. 6(1)(a)
[10] GDPR, Article 9(2)(a)
[11] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017
[12] SCA-RTS, Article 32(3).

processing of certain data points and the potential exclusion of processing special category personal data relating to silent parties. There are several issues with this approach:

(1) From a PSD2 perspective, ASPSPs are expected to treat data requests transmitted through the services of an AISP without any discrimination for other than objective reasons.[13] Failing to respond to an AISP's request on the basis that information contains special category personal data could, in our view, amount to discrimination thereby causing the ASPSP to contravene this obligation.
(2) The SCA-RTS requires ASPSPs to provide AISPs with the same information from designated payment accounts and associated payment transactions made available to the PSU when directly requesting access to the account information, provided that this information does not include sensitive payment data[14]. Failing to respond to an AISP's request on the basis that the information contains special category data would arguably result in the ASPSP contravening this obligation, noting that the scope of special category data differs from (and is wider than) sensitive payment data.
(3) The implementation of technical measures to prevent the processing of certain data points would significantly impact the quality of the payment service being offered to the PSU by the AISP, which may require a full data set to effectively provide its payment service and make an accurate assessment.
(4) There may be practical challenges in implementing a solution that prevents the processing of certain data points without, from time to time, catching other data points which do not constitute special category data in the context (and in doing so may cause an ASPSP to breach its obligations as outlined above).

We note that silent party data is processed on a regular basis in the context of payments and it would be good to have policy guidance of how this can be reconciled within the context of open banking and PSD2.

5. Data Minimisation, Security, Transparency, Accountability and Profiling

OBIE already supports data minimisation by the use of data clusters for the provision of AISP services. OBIE customer research found that grouping permissions together and adding another layer of description aided the PSU's understanding of the data they were being asked to consent to share. This approach also allows a consistency of language across AISPs and ASPSPs to provide additional comfort to PSUs that they are sharing the data they intended to. If consistent language is used, it will drive PSU familiarity and adoption. It also enables AISPs to consider how data clusters can be used to both support their data minimisation requirements under GDPR, and to avoid requesting more data than is needed for their service offering under PSD2. OBIE would be interested in a further clarification on the concept of 'digital filters' and the expectation on how this can be technically supported.

Further, we note that the Guidelines state that under PSD2, ASPSPs are should provide access to payment account information and there is no further requirement to provide access to personal data contained in other accounts, such as savings, mortgages or investment accounts. In the UK, we are currently exploring the concept of Open Finance, where one of the objectives considers access

[13] PSD2, Article 67(3)(b)
[14] SCA-RTS, Article 36(1)(a)

extending beyond payment accounts, enabling AISPs to potentially access comprehensive sets of financial data from both payment and non-payment accounts. The aim of this initiative is to enable AISPs to make available a broader range of products and services to their customers. We note that in these instances, both AISPs and ASPSPs will need to ensure an appropriate lawful basis for processing personal data under the GDPR to support their activities.

Finally, we were very interested to read the points raised in paragraph 77 relating to the privacy dashboard. Within the Open Banking ecosystem, there are two types of dashboards which are supported by our participants:

(i) Consent Dashboards: These are available in the TPP and enable the PSU to view, manage and revoke their consent for their payment service for different ASPSPs.
(ii) Access Dashboards: These are available at the ASPSP and enable the PSU to view, manage and revoke access to their payment account granted to different TPPs.

If a PSU no longer wishes to use a TPP service, they would be able to revoke their consent with the TPP subject to the agreed terms of the contract. The PSU, may also revoke access at their ASPSP's access dashboard, which would effectively prevent that AISP from accessing their account until access is reinstated. It is important to note that revocation of access at the ASPSP access dashboard does not result in revocation of consent. This is similar to direct debits, where cancellation of a direct debit at the ASPSP, will not invalidate the existing commercial arrangement with the payee. In our view, explicit consent is agreed solely between the PSU and the TPP and the ASPSPs cannot have control of that consent, including by seeking confirmation of the PSU's consent. The revocation of access simply invalidates the ability of the AISP to access the account until such time as the PSU has gone through a strong customer authentication process with their ASPSP to re-establish AISP access to the payment account.

Consequently, we have concerns with an approach which suggests that an ASPSP may offer the PSU the possibility to withdraw a specific explicit PSD2 consent at their dashboard and further, that this would result in a denial of access to their payment accounts to one or more TPPs. From a regulatory perspective, when an ASPSP denies access to a TPP it should only be based on unauthorised or fraudulent access to their payment account thereby triggering reporting requirements to the regulator and notification requirements to the PSU. Revocation of access at the ASPSP dashboard is very unlikely to trigger these requirements in most circumstances, as any access by the AISP would likely be based on a valid PSD2 consent obtained by the TPP from the PSU. The OBIE technical solution enables ASPSPs and TPPs to notify each other when either consent or access has been revoked enabling them to manage further engagement with the PSU. We would welcome a revision of paragraph 77 accordingly.

GDPR and PSD2 are key legislative frameworks that must co-exist holistically ensuring that personal data is protected, while at the same time enabling the provision of payment services and driving competition and customer benefits. OBIE is eager to engage and support at an industry level to ensure a thriving and collaborative ecosystem. Thank you for considering our response and please feel free to engage with us directly should you wish to discuss any of these points.