API EG 032-18
Version 1.0
12 July 2018

[**X**] Public – [ ] Internal Use – [ ] Confidential – [ ] Strictest Confidence
Distribution: General Public

Summary of the 8th Meeting of the API Evaluation Group

14 May 2018, 10h30-18h00 CET
EPC, Cours Saint-Michel 30A, 1040 Brussels

(Approved by the API EG Members)

1. Welcome

The co-chairs, J. Whittle (NPSO Ltd) and O. Berglund (Trustly Group AB) welcomed the participants to the eight meeting of the API Evaluation Group (EG). Please see Annex I for the list of attendees.

J. Whittle informed that the API EG will be invited to review and approve the minutes of the previous meeting (23 April 2018) via email.

2. Approval of the agenda (API EG 031-18)

The agenda was approved unchanged.

The European Commission (EC) representative informed that a colleague from DG FISMA would join later to provide a presentation on the interaction between PSD2 and the General Data Protection Regulation (GDPR) (see section 4 for more details).

3. Regulatory updates

The API EG was informed that the publication of the EBA “Q&A” tool in relation to PSD2 had been delayed until end May/June 2018. Moreover, the EBA anticipates to be in a position to publish a clarification on the Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communication (“RTS”) by the end of June 2018.

4. Review list of ‘hot topics’ (API EG 020-18; input documents)

The hot topics that were discussed[1] by the API EG include:

AIS data

The main discussion is related to what is in, versus what is beyond, the scope of PSD2. As mentioned in the previous meeting, account-servicing payment service providers (ASPSPs) are of the view that the scope should be limited as per the API EG terms of reference to “all services and data which are to be made accessible for online payment accounts as per PSD2”. The account information service providers (AISPs) on the other hand have repeatedly expressed the need to extend the scope to other types of account

[1] Topic ‘Access to payment account information by AISPs (four times a day; 90-day period SCA)’ which was listed on the agenda was not discussed.

in order to ensure that the API will be widely used and to avoid the need for separate sessions based on direct access (“screen scraping”) to have access to the non-payment accounts data.

The EC commented that that it would be a pity if an API would not be used even though it fulfils all the legal requirements and that it would also be in the interest of ASPSPs as many of them offer AIS services.

While agreeing with potential benefits, the EBA also stressed that in the context of API evaluation, the NCAs can only assess against PSD2.

J. Whittle noted that as a first step the API EG needs to be very clear that what it recommends the API initiatives should provide as from “day 1” is based on PSD2 scope. As a second step (“day 2”) the API EG would also need to explain to the initiatives that there will be market pressure to bring more data via the API. The main question should hence be whether the API is scalable and to this end the API EG would need to better understand how API initiatives can facilitate this wider approach.

From the ASPSP side it was commented that the API EG should for the time being only focus on “day 1” and not yet start talking about “day 2”.

The API EG reached an agreement on the direction of travel in relation to the topic of AIS data, but further wordsmithing would be required. The team working on this hot topic was hence invited to finalise the document in order to be able to publish it in due course on the EPC website.

Consent in scope of PSD2 in the context of the GDPR

A presentation was provided by the EC (P. Silva) on the interaction between PSD2 and the General Data Protection Regulation (GDPR) with a focus on the legal ground for the processing of personal data by payment initiation service providers (PISPs) and AISPs (see Annex IV).

The following clarifications were provided:

- There is no obligation for passing on the payment service user’s (PSU) consent by the TPP to the ASPSP and the ASPSP does not have any responsibility to check the consent of the TPP customer.
- It falls under the realm of civil law of each Member State to decide whether you have concluded a valid contract with a third-party provider (TPP). When you conclude a contract, you automatically consent to all that is included in the contract.
- Explicit consent in GDPR in relation to the processing of sensitive data (which is different to sensitive payment data under PSD2) is an additional condition and not a legal ground.
- If a TPP wishes to process personal data for other purposes than providing payment services they will need another legal ground do to this (e.g. consent) or alternatively this could already be specified in the initial contract.

The EBA had a question on onward sharing of data and how granular the information needs to be for the PSU. It was commented that this should be as granular as possible given that the consumer needs to know with which third parties its data is shared with.

Following the presentation and clarification provided it was agreed that the topic “consent in the context of PSD2 and GDPR” should no longer be listed as a “hot topic”.

Topic 5: Who applies strong customer authentication (SCA)?

The TPP representatives invited the EBA/EC to clarify whether according to the PSD2/RTS both the ASPSPs and PISPs can apply an SCA exemption or whether only ASPSPs can do this? It was noted that the ASPSP representatives are of the view that there is no SCA obligation on TPPs as they do not authorise the transaction.

The EC representative commented that in his view SCA should be required systematically but that further clarification would be needed from the EBA. The EC representative also stated that in his view only the ASPSP (not another PSP in the chain) can exempt SCA being applied to payment transactions from SCA, and subject to the ASPSP being below relevant fraud thresholds.

J. Whittle noted that further clarification from the regulator would be welcomed as the text references to PSPs and suggested that the team working on this topic would further update the template document.

Note in editing: The EBA representatives were not present when this topic was discussed.

Security

An input document prepared by the team in charge of security had been provided prior to the meeting to the API EG.

From the TPP side it was commented that there is still an open question in relation to the term “session” and that there is a difference between a communication session and a transaction session. They are moreover of the view that it not should be required to have a separate communication session for every transaction.

The API EG agreed to include an additional question in the list of questions (see section 5) i.e. “Does the API initiative manage the use of eIDAS certificates for mutually authenticating the parties and securing the communication session?”

The EBA clarified that there is no obligation to use an eIDAS certificate for mutual authentication. A TPP member commented that if ASPSPs would use self-issued certificates there would be no assurance that the certificate is non-fraudulent and that it should be noted that eIDAS is also a legal framework. The API EG agreed that eIDAS is an important topic that needs to be further worked on.

The team is currently only focusing on the TPP/ASPSP API connection which is indeed a good starting point. They were invited to continue their work as further refinement would be required. Moreover, it was suggested that they should also have a look at liability and audibility of the trail.

P. Spittler volunteered to join the team working on security.

5. Review of the API functionalities (API EG 023-18; input documents)

As an introduction to this topic, J. Whittle highlighted that the API EG should focus on the following two categories of deliverables and that the aim should be to get as much guidance documents out by the end of June 2018:

- Clarification documents in relation to the 'hot topics', which should be published as soon as possible on the EPC website[2].
- List of 'recommended API functionalities' focusing on providing advice to the API initiatives as part of the engagement process.

In order to learn to what extent, the API initiatives align to these recommended functionalities, the API EG should initiate as soon as possible further engagement based on a list of questions. Time is of the essence as the API EG is expected to provide guidance to the API initiatives by the end of June 2018.

The EBA also shared their view that the industry, and a forum like the API EG, can play a very positive role by providing views/advice/recommendations on what good looks like, while regulators consider requirements, and when supervising regulated firms, they ensure that these firms comply with the requirements. The role of the EBA is to contribute to supervisory convergence among NCAs. The role of the industry is to clarify what good looks like.

In view of the above the API EG also needs to be careful in the terminology it uses. The API EG agreed that the term 'requirements' was not correct as it could be easily confused with legal and regulatory requirements which are the responsibility of regulators. The group hence agreed to rename 'requirements' to 'recommended functionalities' and also to refer to API initiatives (instead of API standards).

The ECB stressed the need for a common European approach or at least for the Euro zone (and to avoid as much as possible regional flavours). This was echoed by the merchants who stated that they need common message implementation guidelines. J. Whittle commented that the API EG should indeed strive towards consistency although it should be noted that even when the same API is chosen there could still be differences in how that API is implemented.

The EC representative remarked that over time the EC would like to see a more streamlined process and that the API EG should have a role in trying to reach API convergence. A concern however is related to the merchants as depending on the ASPSP, their customers could have a different user experience.

The API EG was reminded that at the previous meeting the members that had provided comments to the list of API 'requirements'[3] had been invited to reconcile these comments. The group consisting of ECSAs, TPP and EPIF representatives had organised a couple of conference calls which resulted into the conversion of requirements into simple (yes/no) questions. This document did not yet include the comments from BEUC as they were related to a previous version of the document and the aim would be to check during this meeting if these additional comments would lead to additional questions (see below). This document had been shared with the API EG prior to the meeting.

[2] A clarification document on authentication is already published on the EPC website.

[3] Term "requirements" was used in the previous version.

The API EG focused its discussion on the list of questions derived from these 'recommended functionalities' with the objective to agree on the 'recommended functionalities' at one of the next meetings. In particular, the API EG had a closer look at the following questions which required further clarification:

Question 1 "Does the API initiative allow for the measurement and monitoring of the API availability, performance and data provided in a way that it can be compared to the interface made available to the payment service user (PSU) for directly accessing its payment account online?"

TPP representatives expressed the view that TPPs should be able to measure the ASPSP's performance. The ASPSP representatives noted that the obligation for measurement and KPIs fell with the ASPSPs rather than the TPPs. They added that the measurement points could only be done at the ASPSP level and that nothing could be done at the API level, given the focus was on the comparison with the customer interface that is unique to each ASPSP. The EBA noted that the question is formulated differently to the corresponding requirement stated in the RTS, which is what the NCAs can assess ASPSPs against. The EBA added it was important to make it clear to API initiatives. The EC remarked that although it is not a legal requirement it would be helpful to include this question. Some members were also of the view that it could be an important tool in order to avoid disputes.

There are different speeds depending on the channel (e.g. mobile versus web-based) used. The key point is that there should be no discrimination per channel. It was clarified that ASPSPs would use one API that will be able to serve different channels.

The API EG concurred to keep the question in the list and also to note the discussion for future reference.

Question 9: Does the API Standard impose any restrictions on how the PSU can give/withdraw consent to the TPP or any restrictions on the content and/or granularity of the consent given by the PSU to the TPP?

The API EG agreed to split up this question in two separate questions.

Question 14 related to access to information

The API EG concurred to add a separate question in relation to card-based payment instrument issuer (PIIS) in line with other questions that refer to the possible roles.

Question 18 related to a technical OK/NOK status in a real-time versus non-real-time booking environment

ASPSPs reminded that they cannot give a guarantee without a contract. For TPPs it was however important to know if in case an ASPSP would be willing to provide a guarantee whether the API would be able to accommodate this. The difference between basic and premium versions of an API was also noted in this context.

The EBA explained that Article 36(1)(c) applies to PISPs so the legal requirement is to provide a confirmation (rather than guarantee although guarantee could be a 'recommended functionality'). The API EG agreed that the word "guarantee" should be replaced by "confirmation".

In addition, the EBA also suggested to include a question on whether the API initiatives foresee traceability as per RTS Article 29 and error messages as per RTS Article 36 (2). J. Whittle commented that Article 29 could be looked at by the team that is currently working on security (hot topic).

The BEUC representative reported on following suggested functionalities in relation to consent. The API EG assessed whether additional questions should be added in relation to these functionalities:

- “The API standard should enable the TPP to provide to the ASPSP the terms of the consent of the user”.

  J. Whittle suggested to add this item on the list of functionalities to discuss at a later stage. It was however commented that there was no such obligation and that it was out of scope as related to non-payment data.

- “The API standard should integrate that the consumer has instructed his ASPSP to refuse any kind of access, being another ASPSP, an AIS or a TPP. Or: The API standard should integrate the possibility for the consumer to instruct his ASPSP to refuse any kind of access, being another ASPSP, an AIS or a TPP”.

  The API EG concurred that this was not an API related issue

- “By clicking this box, I agree that the company “XXX” will have access to all my financial data managed by the ASPSPs” “YYY””.

  The API EG concurred that this was not an API related issue

- “The ASPSP (or the API?) should maintain a list of AIS or other AIPSPs for which the consumer has given access to his bank account. The consumer should be able to cancel at any time any specific agreement given to a third party”.

  The API EG concurred that this was not an API related issue

- The API standard should provide that when an agreement is cancelled by the consumer to the ASPSP or the TPP, the receiver of the cancellation informs the other party.

  The API EG concurred that this was not an API related issue

An updated version of the list of questions in relation to the functionalities that the API EG is considering recommending an API initiative to support will be created. Each question should be answered with a simple yes or no and an extra column will be added to allow the initiatives to include a rationale. This updated document will be sent shortly for validation to the API EG. The aim would be to provide the finalised questionnaire to the API initiatives at the latest by 21 May 2018 with the invitation to provide their responses by 31 May 2018. Moreover, it was agreed that the API initiatives should be invited to the next face-to-face meeting of the API EG in June in order to discuss the responses to the questionnaire.

6. Status update on the technical expert evaluation subgroups

The technical expert subgroups have not been very active lately as they are waiting for input from the API EG.

In order to keep the technical subgroups updated about the latest developments they will also be invited to a conference call to clarify the way forward in relation to the engagement with the API initiatives.

7. AOB

T. Sabri had prepared a document on Anti-Money Laundering (AML) related API functionality. Its main objective is to establish whether AML/Counter-Financing of Terrorism (CFT) related data needs to be exchanged by ASPSPs and TPPs through the APIs.

J. Whittle agreed that it would be a unique opportunity and that it would be helpful to have a clear position from the EC.

The EC informed that the AML Directive would need to be updated in order to exclude AISPs from its scope. However, the Directive was only recently adopted and hence this update will not take place before the end of 2019. The EC would need to think about whether it could potentially publish an open letter on this matter.

The EC further stated that the AML checks for PISPs relate to merchants, not payers.

The AML document will be circulated to the API EG.

8. Next meeting date (API EG 004-18)

A conference call was scheduled on 24 May 2018 (11-12 CEST) to which the API initiatives and technical subgroups will be invited to clarify the way forward in relation to the engagement and to give an opportunity to the API initiatives to request further clarification about the questionnaire on recommended API functionalities.

The next face-to-face meeting will take place in Brussels on 8 June 2018 (10-17 CEST). The focus will be on the engagement with the API initiatives and hence the API initiatives will also be invited.

9. Closure of the meeting

The co-chairs closed the meeting around 18h00 CEST and thanked the participants for the constructive meeting.

Annex I: List of attendees

Category	Name	Institution	Attendance
Co-Chairs	James Whittle	NPSO Ltd	Yes
	Oscar Berglund	Trustly Group AB	Yes
TPP Members	Joan Burkovic	Bankin’	Apologies
	Aoife Houlihan	Klarna	Yes
	Ralf Ohlhausen	PPRO	Yes
ASPSP Members	Marieke van Berkel	EACB	Yes
	Gijs Boudewijn	Dutch Payments Association (representing EBF)	Yes
	Emil Johansson	Swedbank (representing ESBG)	Yes
PSU Members	Farid Aliyev[4]	BEUC	Yes
	Tarik Zerkti[5]	Ecommerce Europe	Yes
	Pascal Spittler	IKEA (representing EuroCommerce)	Yes
Other Members	Thaer Sabri	EMA	Yes
	Krzysztof Korus	Polish Payment Institution Association (representing EPIF)	Yes
Observers	Ralf Jacob	European Commission	Apologies
	Philippe Pellé	European Commission	Yes
	Krzysztof Zurek	European Commission	Yes
	Nilixa Devlukia	EBA	Yes
	Helene Oger-Zaher	EBA	Yes
	Ann Börestam	ECB	Yes
Linking pin with technical experts	Arturo G. Mac Dowell	Eurobits	Yes
Guest	Lorenzo Gaston	Gemalto (Convenor ISO TC 68 / SC2 / SG1 TPP)	Yes
Secretariat	Etienne Goosse	EPC	Apologies
	Christophe Godefroi	EPC	Yes

[4] Alternate to Jean Allix

[5] Alternate to Just Hasselaar

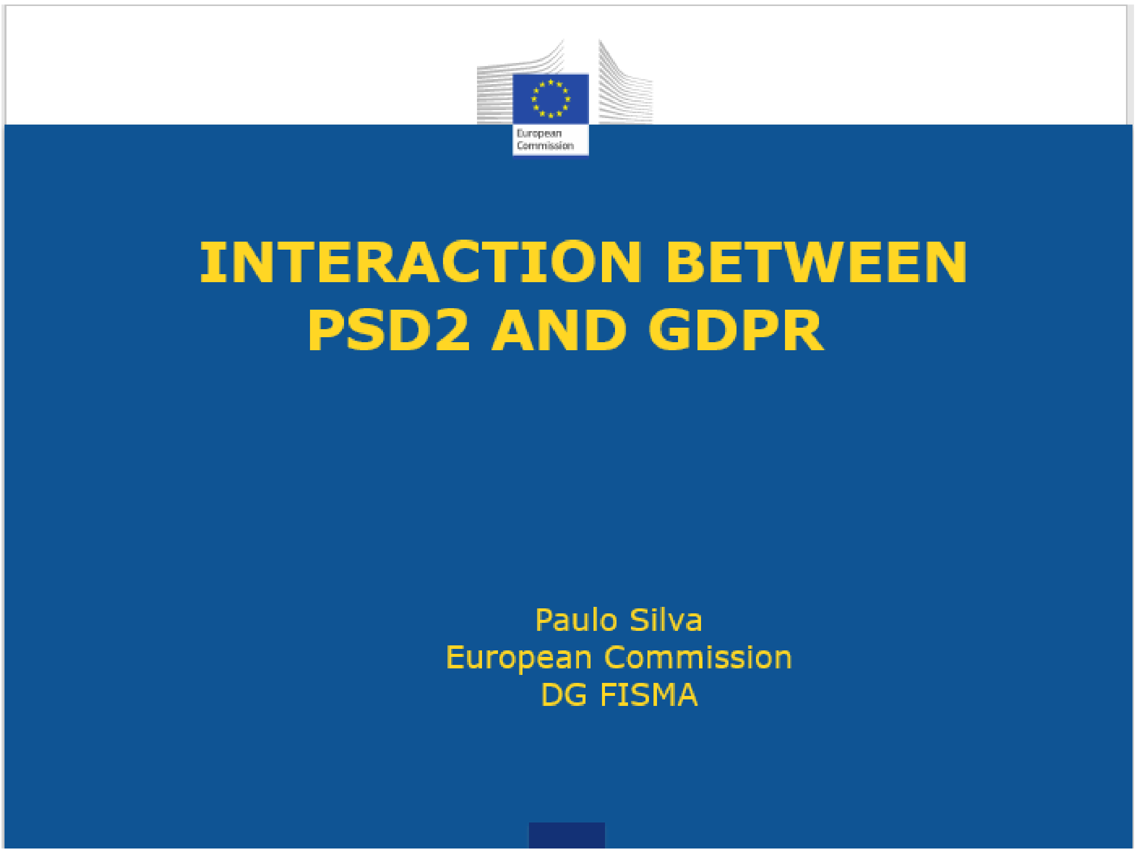
Annex II: Action points of the 8th meeting of the API EG

Item	Action	Owner	Status / Deadline
8-01	Create an updated version of the list of questions in relation to recommended API functionalities and distribute to the API EG	API EG co-chairs / EPC secretariat	15 May 2018
8-02	Review updated version of the list of questions in relation to recommended API functionalities	API EG	18 May 2018
8-03	Invite the API initiatives to provide their responses on the list of questions in relation to recommended API functionalities	API EG co-chairs / EPC secretariat	21 May 2018
8-04	Schedule an API EG conference call on 24 May 2018 + invite the API initiatives and technical expert subgroups	EPC secretariat	16 May 2018
8-05	Finalise the hot topic template on AIS data in order to be able to publish on the EPC website	A. Mac Dowell J. Burkovic M. van Berkel	In due course
8-06	Continue work on hot topic “who applies SCA”	A. Mac Dowell G. Boudewijn J. Burkovic K. Korus R. Ohlhausen	In due course
8-07	Refine hot topic document on security	A. Mac Dowell E. Johansson L. Gaston P. Spittler	In due course

Annex III Meeting Calendar

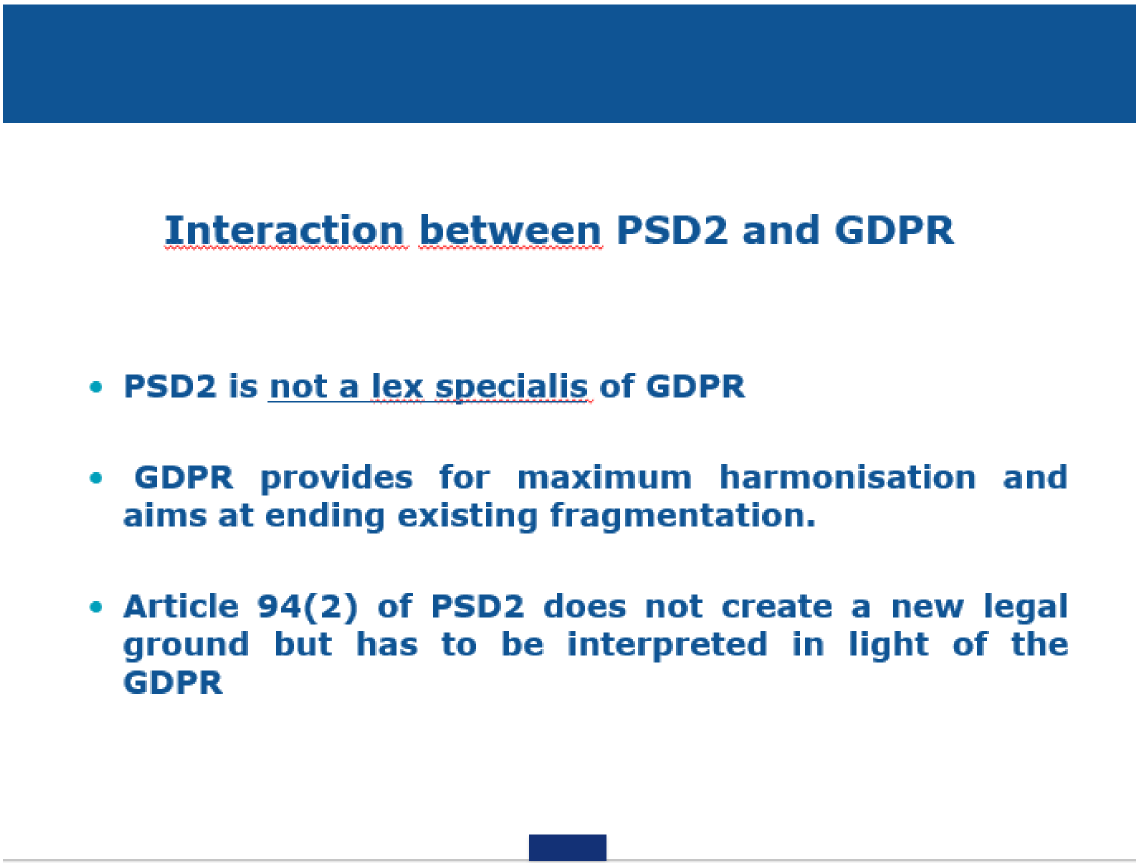
2018	API EG Meetings
January	**29 January 2018 (11:00-16:00 CET)** EPC, Brussels
February	**22 February 2018 (10:00-12:00 CET)** Conference call
	27 February 2018 (13:30–18:00 CET) – preceded by lunch as from 12:45 CET EPC, Brussels
	28 February 2018 (9:00-10.30 CET) **28 February 2018 (11:00-16:00 CET) API Evaluation Workshop with 5 API initiatives** EBF, Brussels
March	**27 March 2018 (09:00-17:00 CEST)** Brussels – EPC
April	**12 April 2018 (10.00-11.00 CEST) - Conference call** **23 April 2018 (10.30-17.00 CEST) - EPC, Brussels**
May	**14 May 2018 (10.30-18.00 CEST) - EPC, Brussels** **24 May 2018 (11.00-12.00 CEST) – Conference call with API initiatives**
June	**8 June 2018 (10.30-17.00 CEST) - Brussels** **25 June 2018 (10:30-17:00 CEST) - TBC**

Annex IV DG DISMA presentation on interaction between PSD2 and GDPR



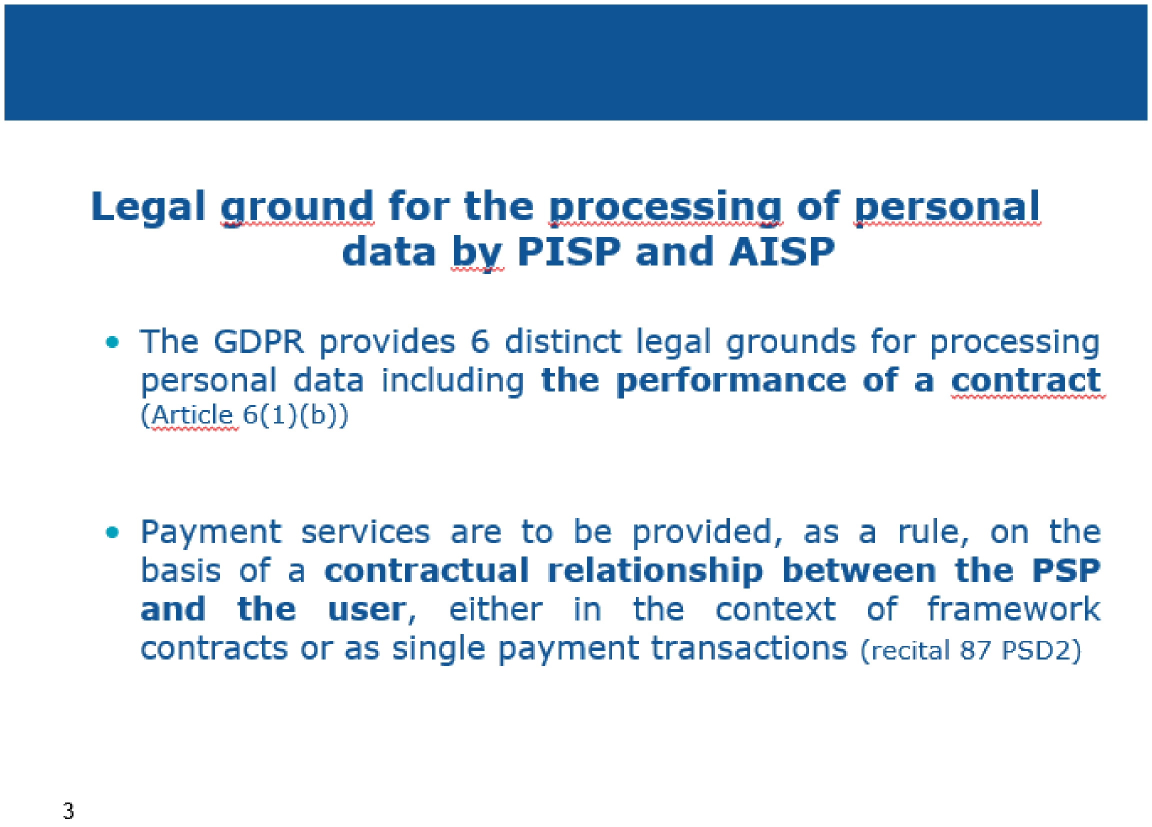
INTERACTION BETWEEN PSD2 AND GDPR

Paulo Silva
European Commission
DG FISMA



Interaction between PSD2 and GDPR

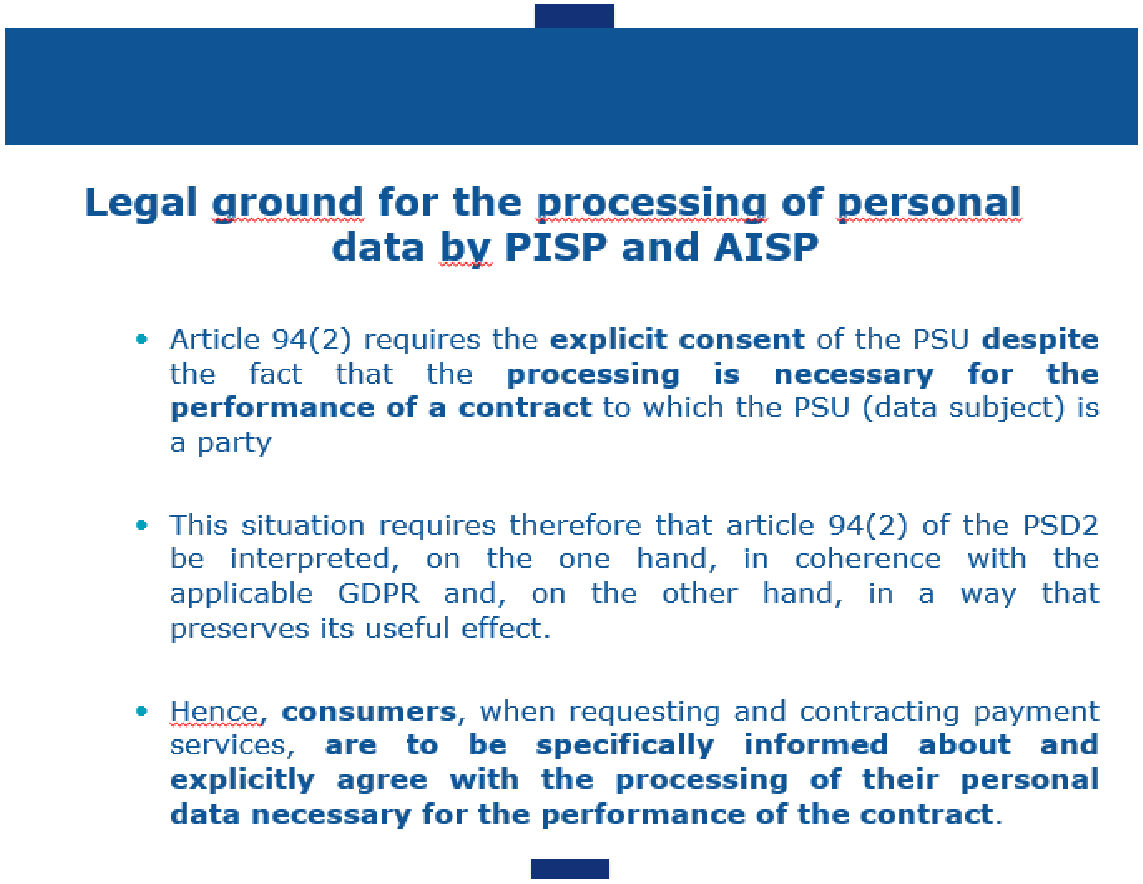
- PSD2 is not a lex specialis of GDPR
- GDPR provides for maximum harmonisation and aims at ending existing fragmentation.
- Article 94(2) of PSD2 does not create a new legal ground but has to be interpreted in light of the GDPR



Legal ground for the processing of personal data by PISP and AISP

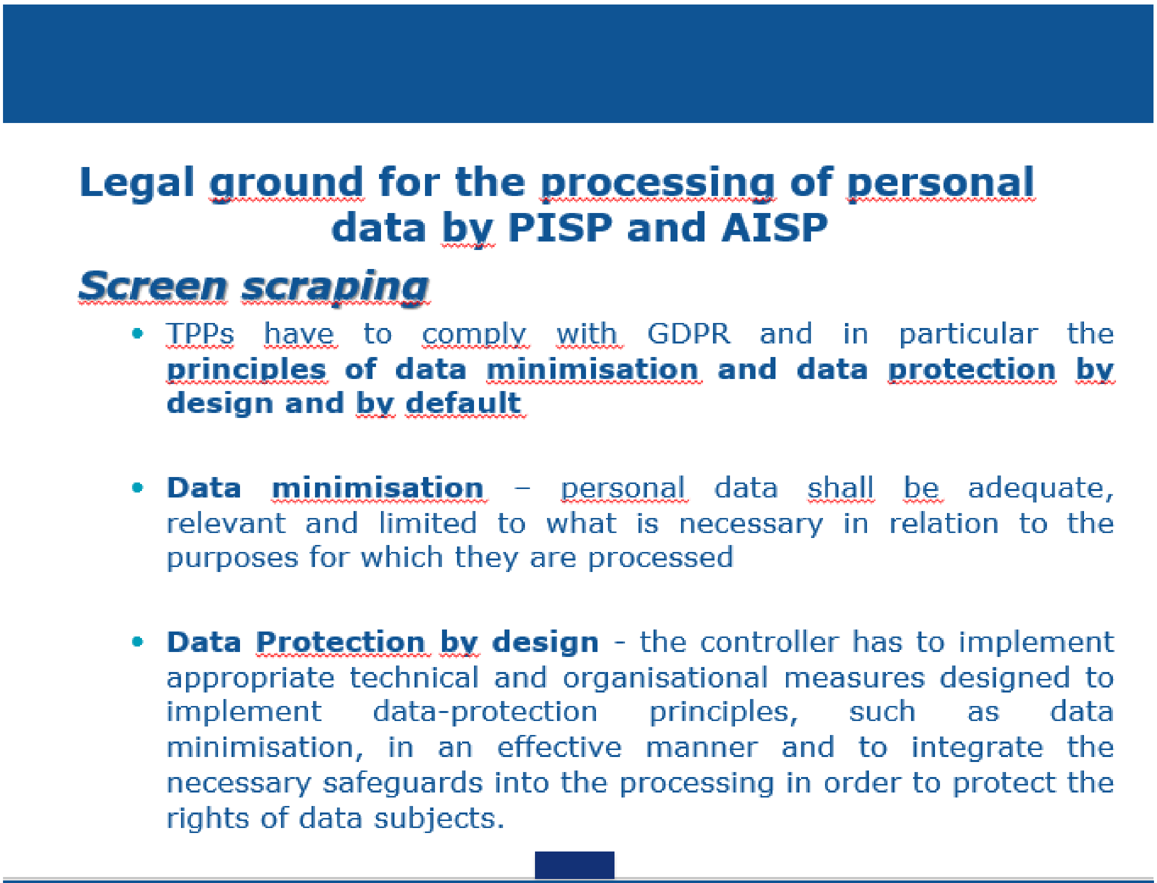
- The GDPR provides 6 distinct legal grounds for processing personal data including **the performance of a contract** (Article 6(1)(b))
- Payment services are to be provided, as a rule, on the basis of a **contractual relationship between the PSP and the user**, either in the context of framework contracts or as single payment transactions (recital 87 PSD2)

3



Legal ground for the processing of personal data by PISP and AISP

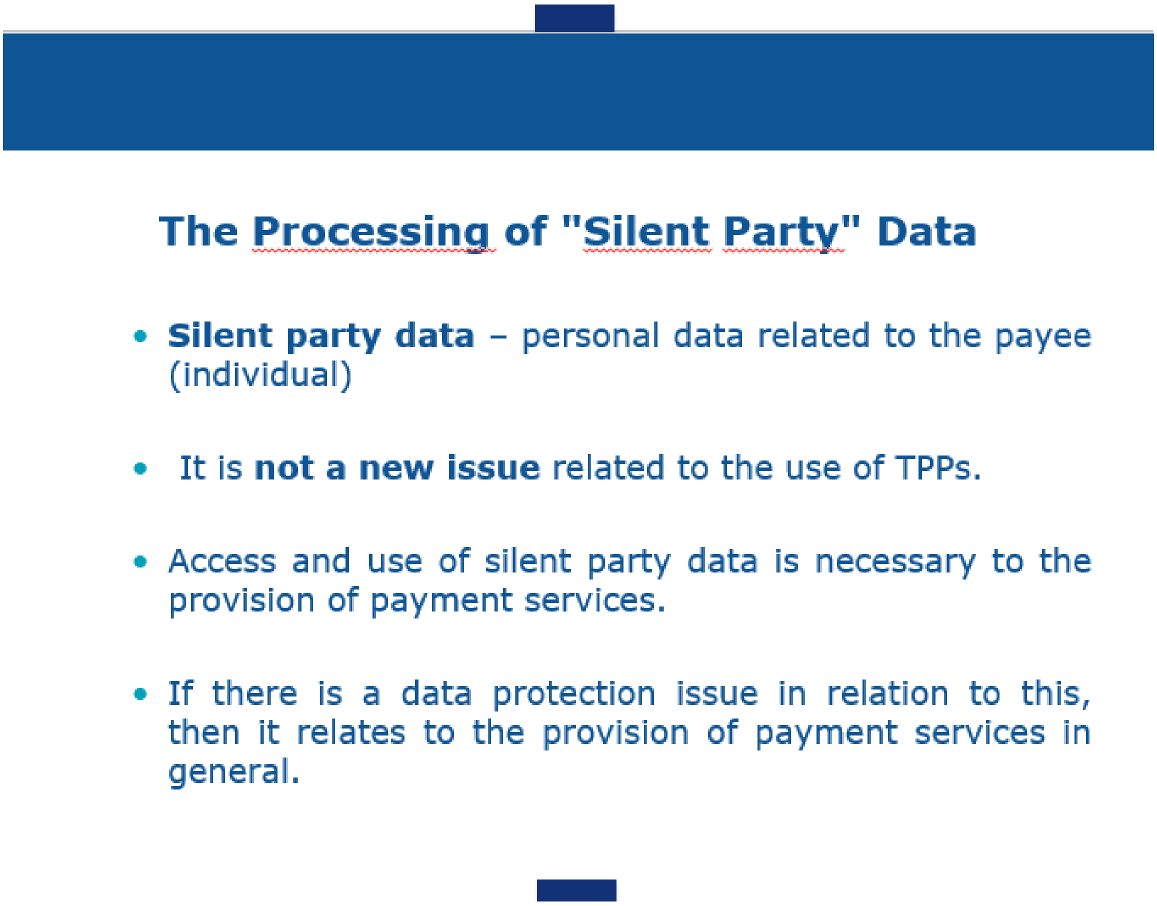
- Article 94(2) requires the **explicit consent** of the PSU **despite the fact that the processing is necessary for the performance of a contract** to which the PSU (data subject) is a party
- This situation requires therefore that article 94(2) of the PSD2 be interpreted, on the one hand, in coherence with the applicable GDPR and, on the other hand, in a way that preserves its useful effect.
- Hence, **consumers**, when requesting and contracting payment services, **are to be specifically informed about and explicitly agree with the processing of their personal data necessary for the performance of the contract**.



Legal ground for the processing of personal data by PISP and AISP

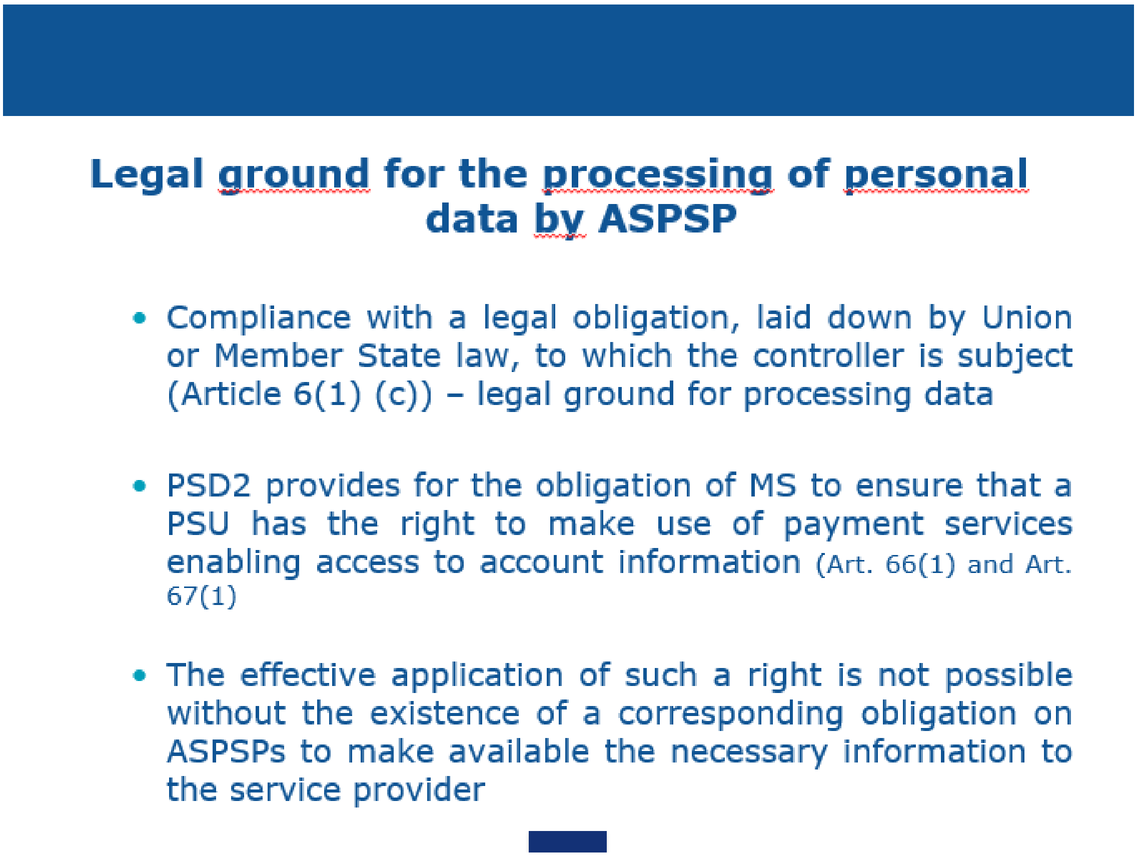
Screen scraping

- TPPs have to comply with GDPR and in particular the **principles of data minimisation and data protection by design and by default**
- **Data minimisation** – personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Data Protection by design** - the controller has to implement appropriate technical and organisational measures designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to protect the rights of data subjects.



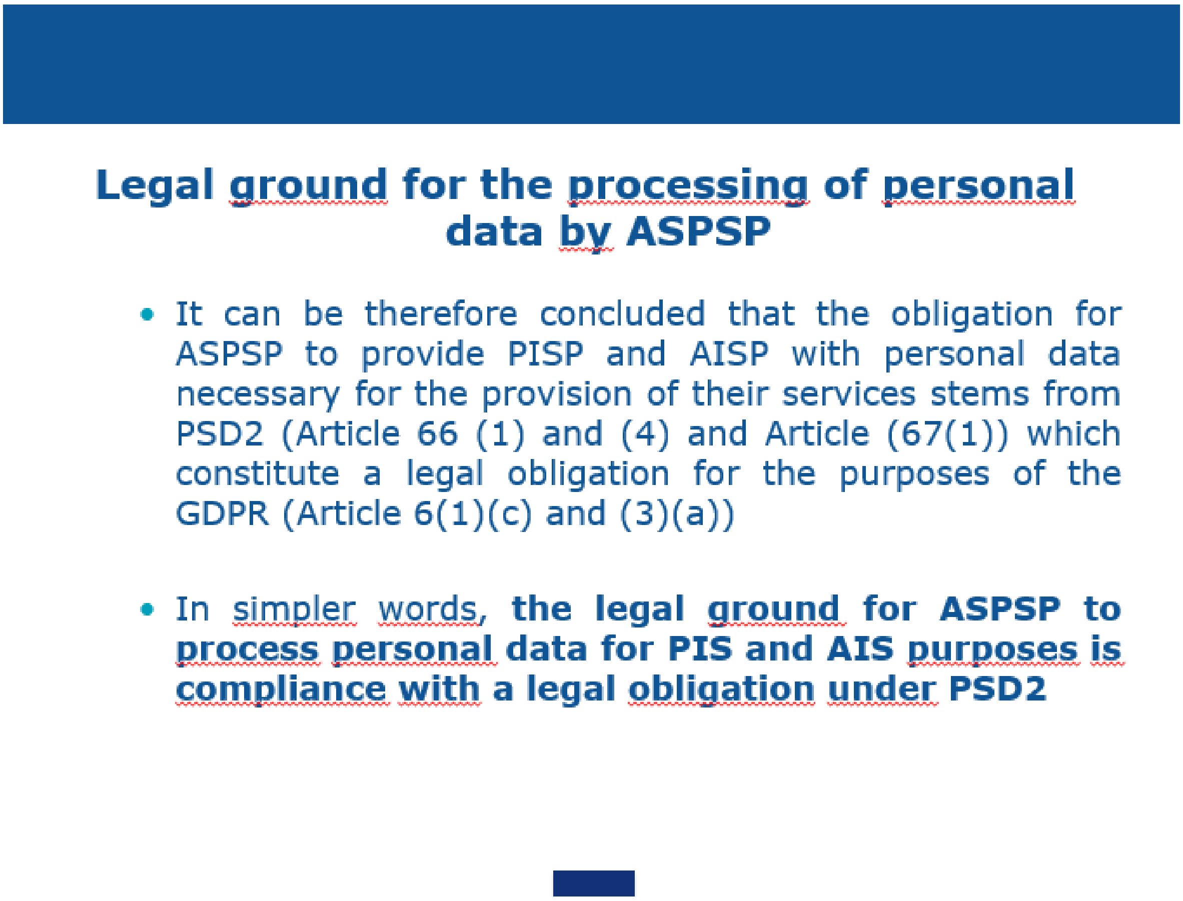
The Processing of "Silent Party" Data

- **Silent party data** – personal data related to the payee (individual)
- It is **not a new issue** related to the use of TPPs.
- Access and use of silent party data is necessary to the provision of payment services.
- If there is a data protection issue in relation to this, then it relates to the provision of payment services in general.



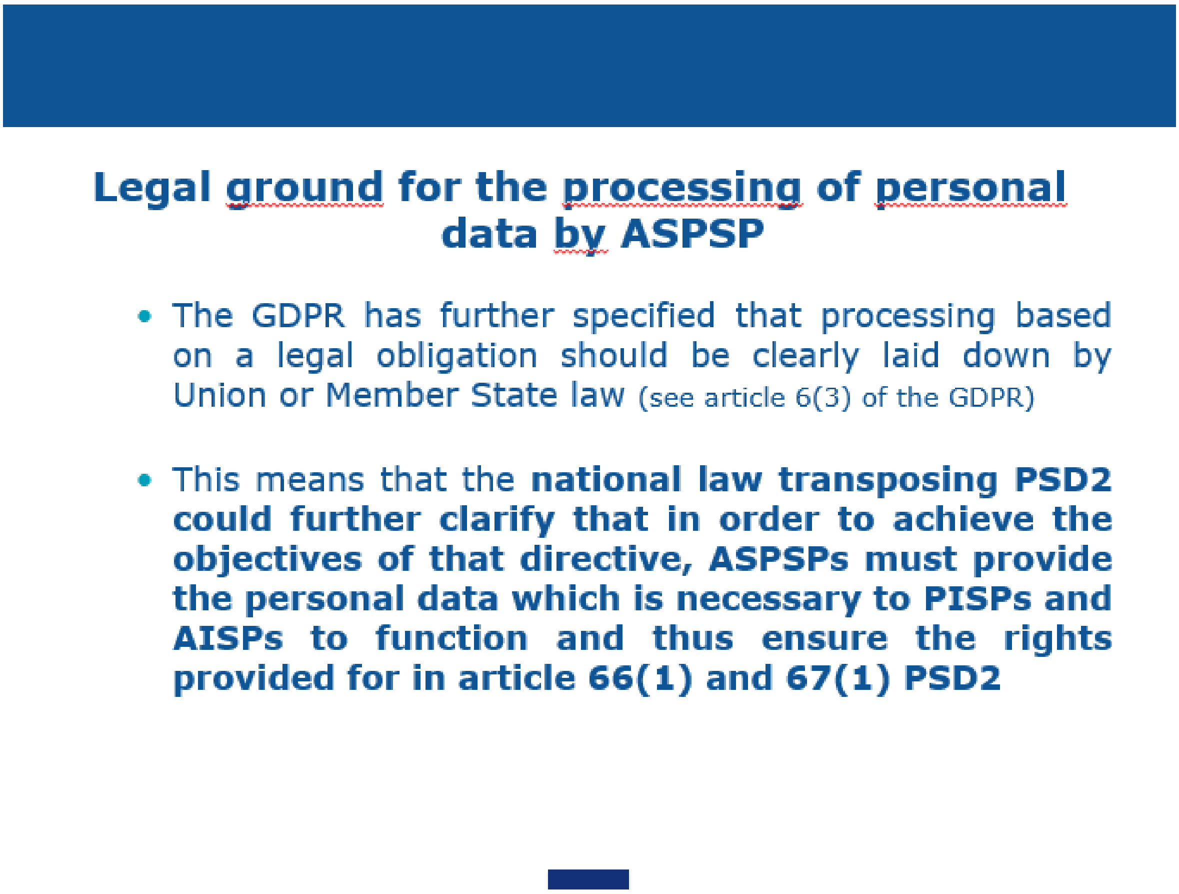
Legal ground for the processing of personal data by ASPSP

- Compliance with a legal obligation, laid down by Union or Member State law, to which the controller is subject (Article 6(1) (c)) – legal ground for processing data
- PSD2 provides for the obligation of MS to ensure that a PSU has the right to make use of payment services enabling access to account information (Art. 66(1) and Art. 67(1)
- The effective application of such a right is not possible without the existence of a corresponding obligation on ASPSPs to make available the necessary information to the service provider



Legal ground for the processing of personal data by ASPSP

- It can be therefore concluded that the obligation for ASPSP to provide PISP and AISP with personal data necessary for the provision of their services stems from PSD2 (Article 66 (1) and (4) and Article (67(1)) which constitute a legal obligation for the purposes of the GDPR (Article 6(1)(c) and (3)(a))
- In simpler words, **the legal ground for ASPSP to process personal data for PIS and AIS purposes is compliance with a legal obligation under PSD2**



Legal ground for the processing of personal data by ASPSP

- The GDPR has further specified that processing based on a legal obligation should be clearly laid down by Union or Member State law (see article 6(3) of the GDPR)

- This means that the **national law transposing PSD2 could further clarify that in order to achieve the objectives of that directive, ASPSPs must provide the personal data which is necessary to PISPs and AISPs to function and thus ensure the rights provided for in article 66(1) and 67(1) PSD2**