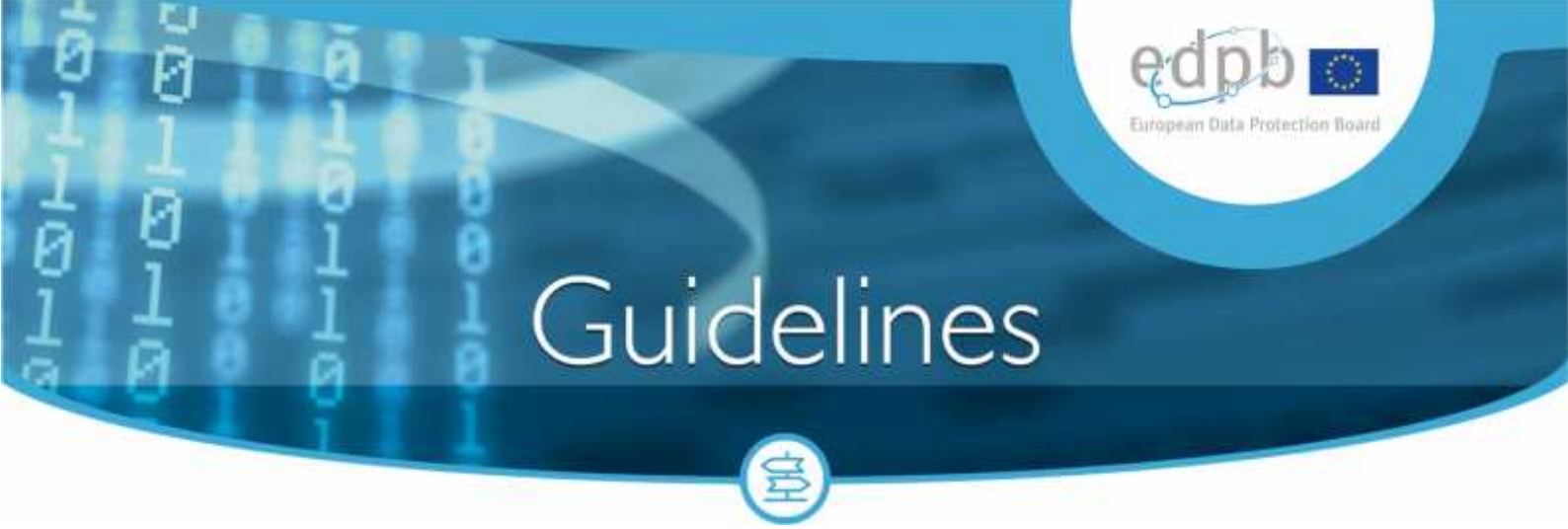

Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

Version 2.0

Adopted on 15 December 2020

Version history

Version 2.0	15.12.2020	Adoption of the Guidelines after public consultation
Version 1.0	17.07.2020	Adoption of the Guidelines for publication consultation

Table of contents

The European Data Protection Board

Having regard to Article 70 (1) (e) of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas:

(1) The General Data Protection Regulation provides for a consistent set of rules for the processing of personal data throughout the EU.

(2) The second Payment Services Directive (Directive 2015/2366/EU of the European Parliament and of the Council of 23 December 2015, hereinafter "PSD2") repeals Directive 2007/64/EC and provides new rules to ensure legal certainty for consumers, merchants and companies within the payment chain and modernizing the legal framework for the market for payment services[2]. Member States had to transpose the PSD2 into their national law before the 13 January 2018.

(3) An important feature of the PSD2 is the introduction of a legal framework for new payment initiation services and account information services. The PSD2 allows these new payment service providers to obtain access to payment accounts of data subjects for the purposes of providing the said services.

(4) With regard to data protection, in accordance with Article 94 (1) of the PSD2, any processing of personal data, including the provision of information about the processing, for the purposes of the PSD2, shall be carried out in accordance with the GDPR[3] and with Regulation (EU) No 2018/1725.

(5) Recital 89 of the PSD2 states that where personal data is processed for the purposes of the PSD2, the precise purpose of the processing should be specified, the applicable legal basis should be named, the relevant security requirements laid down in the GDPR must be implemented, and the principles of necessity, proportionality, purpose limitation and proportionate data retention periods respected. Also, data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of the PSD2[4].

(6) Recital 93 of the PSD2 states that the payment initiation service providers and the account information service providers on the one hand and the account servicing payment service provider on the other, should observe the necessary data protection and security requirements established by, or referred to in, this Directive or included in the regulatory technical standards.

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] Recital 6 PSD2
[3] As PSD2 predates the GDPR, it still refers to Directive 95/46. Article 94 GDPR states that references to the repealed Directive 95/46 shall be construed as references to the GDPR.
[4] Recital 89, PSD2

HAS ADOPTED THE FOLLOWING GUIDELINES

1. INTRODUCTION

1. The second Payment Services Directive (hereinafter "PSD2") has introduced a number of novelties in the payment services field. While it creates new opportunities for consumers and enhances transparency in such field, the application of the PSD2 raises certain questions and concerns in respect of the need that the data subjects remain in full control of their personal data. The General Data Protection Regulation (hereinafter "GDPR") applies to the processing of personal data including processing activities carried out in the context of payment services as defined by the PSD2[5]. Thus, controllers acting in the field covered by the PSD2 must always ensure compliance with the requirements of the GDPR, including the principles of data protection set out in Article 5 of the GDPR, as well as the relevant provisions of the ePrivacy Directive[6]. While the PSD2[7] and the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (hereinafter "RTS"[8]) contain certain provisions relating to data protection and security, uncertainty has arisen about the interpretation of these provisions as well as the interplay between the general data protection framework and the PSD2.

2. On July 5 2018, the EDPB issued a letter regarding the PSD2, in which the EDPB provided clarifications on questions concerning the protection of personal data in relation to the PSD2, in particular on the processing of personal data of non-contracting parties (so called 'silent party data') by account information service providers (hereinafter "AISPs") and payment initiation service providers (hereinafter "PISPs"), the procedures with regard to giving and withdrawing consent, the RTS and the cooperation between account servicing payment services providers (hereinafter "ASPSPs") in relation to security measures. Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges.

3. These guidelines aim to provide further guidance on data protection aspects in the context of the PSD2, in particular on the relationship between relevant provisions on the GDPR and the PSD2. The main focus of these guidelines is on the processing of personal data by AISPs and PISPs. As such, this document addresses conditions for granting access to payment account information by ASPSPs and for the processing of personal data by PISPs and AISPs, including the requirements and safeguards in relation to the processing of personal data by PISPs and AISPs for purposes other than the initial purposes for which the data have been collected, especially when they have been collected in the context of the provision of an account information service[9]. This document also

[5] Art. 1 (1) GDPR

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); OJ L 201, 31/07/2002 P. 0037 - 0047

[7] Art. 94 PSD etc.

[8] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance.); C/2017/7782; OJ L 69, 13.3.2018, p. 23–43; available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

[9] An account information service is an online service to provide consolidated information on one or more payment accounts held by the payment service user either with another payment service provider or with more than one payment service provider.

addresses different notions of explicit consent under the PSD2 and the GDPR, the processing of 'silent party data', the processing of special categories of personal data by PISPs and AISPs, the application of the main data protection principles set forth by the GDPR, including data minimisation, transparency, accountability and security measures. The PSD2 involves cross-functional responsibilities in the fields of, inter alia, consumer protection and competition law. Considerations regarding these fields of law are beyond the scope of these guidelines.

4. To facilitate the reading of the guidelines the main definitions used in this document are provided below.

1.1 Definitions

'Account Information Service Provider' ('AISP')' refers to the provider of an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;

'Account Servicing Payment Service Provider' ('ASPSP') refers to a payment service provider providing and maintaining a payment account for a payer*;*

'Data minimisation' is a principle of data protection, according to which personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

'Payer' refers to a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

'Payee' refers to a natural or legal person who is the intended recipient of funds, which have been the subject of a payment transaction*;*

'Payment account' means an account held in the name of one or more payment service users, which is used for the execution of payment transactions;

'Payment Initiation Service Provider' ('PISP') refers to the provider of a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;

'Payment service provider' refers to a means a body referred to in Article 1(1) of the PSD2[10] or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33 of the PSD2;

[10] Art. 1 (1) PSD2 states that the PSD2 establishes the rules in accordance with which Member States shall distinguish between the following categories of *payment service provider*:
(a) credit institutions as defined in point (1) of Art. 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council (1), including branches thereof within the meaning of point (17) Art. 4(1) of that Regulation where such branches are located in the Union, whether the head offices of those branches are located within the Union or, in accordance with Art. 47 of Directive 2013/36/EU and with national law, outside the Union;
(b) electronic money institutions within the meaning of point (1) of Art. 2 of Directive 2009/110/EC, including, in accordance with Art. 8 of that Directive and with national law, branches thereof, where such branches are located within the Union and their head offices are located outside the Union, in as far as the payment services provided by those branches are linked to the issuance of electronic money;
(c) post office giro institutions which are entitled under national law to provide payment services;
(d) payment institutions;

'Payment service user' means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Data protection by design' refers to technical and organizational measures embedded into a product or service, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects;

'Data protection by default' refers to appropriate technical and organisational measures implemented in a product or service which ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed;

'RTS' refers to the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication;

'Third Party Providers' *('TPP')* refers to both PISPs and AISPs.

1.2 Services under the PSD2

5. The PSD2 introduces two new kinds of payment service (providers): PISPs and AISPs. Annex 1 of the PSD2 contains the eight payment services that are covered by the PSD2.

6. PISPs provide services to initiate payment orders at the request of the payment service user with respect to a user's payment account held at another payment service provider[11]. A PISP can request an ASPSP (usually a bank) to initiate a transaction on behalf of the payment service user. The (payment service) user can be a natural person (data subject) or a legal person.

7. AISPs provide online services for consolidated information on one or more payment accounts held by the payment service user either with another payment service provider or with more than one payment service provider[12]. According to recital 28 PSD2, the payment service user is able to have an overall view of its financial situation immediately at any given moment.

8. When it comes to account information services, there could be several different types of services offered, with the emphasis on different features and purposes. For example, some providers may offer users services such as budget planning and monitoring spending. The processing of personal data in the context of these services is covered by the PSD2. Services that entail creditworthiness assessments of the payment service user or audit services performed on the basis of the collection of information via an account information service fall outside of the scope of the PSD2 and therefore fall under the GDPR. Furthermore, accounts other than payment accounts (e.g. savings,

(e) the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities;
(f) Member States or their regional or local authorities when not acting in their capacity as public authorities.

[11] Art. 4 (15) PSD2.

[12] Art. 4 (16) PSD2

investments) are not covered by the PSD2 either. In any case, the GDPR is the applicable legal framework for the processing of personal data.

Example 1:

HappyPayments is a company that offers an online service consisting of the provision of information on one or more payment accounts through a mobile app in order to provide financial oversight (an Account Information Service). With this service the payment service user can see at a glance the balances and recent transactions in two or more payment accounts at different banks. It also offers, when a payment service user chooses to do so, a categorisation of spending and income according to different typologies (salary, leisure, energy, mortgage, etc.), thus helping the payment service user with financial planning. Within this app, HappyPayments also offers a service to initiate payments directly from the users designated payment account(s) (a Payment Initiation Service).

9. In order to provide those services, the PSD2 regulates the legal conditions under which PISPs and AISPs can access payment accounts to provide a service to the payment service user.

10. Articles 66 (1) and 67 (1) PSD2 determine that the access and the use of payment and account information services are rights of the payment service user. This means that the payment service user should remain entirely free with regard to the exercise of such right and cannot be forced to make use of this right.

11. Access to payment accounts and the use of payment account information is partly regulated in Articles 66 and 67 PSD2, which contain safeguards regarding the protection of (personal) data. Article 66 (3) (f) PSD2 states that the PISP shall not request from the payment service user any data other than those necessary to provide the payment initiation service, and Article 66 (3) (g) PSD2 provides that PISPs shall not use, access or store any data for purposes other than for performing the payment initiation service explicitly requested by the payment service user. Furthermore, Article 67 (2) (d) PSD2 limits the access of AISPs to the information from designated payment accounts and associated payment transactions, whereas Article 67 (2) (f) PSD2 states that AISPs shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules. The latter emphasises that, within the context of the account information services, personal data can only be collected for specified, explicit and legitimate purposes. An AISP should therefore make explicit in the contract for what specific purposes personal account information data are going to be processed for, in the context of the account information service it provides. The contract should be lawful, fair and transparent under Article 5 of the GDPR and also comply with other consumer protection laws.

12. Depending on specific circumstances, payment service providers could be a controller or processor under the GDPR. In these guidelines, 'controllers' are those payment service providers who, alone or jointly with others, determine the purposes and means of the processing of personal data. More guidance on this can be found in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

2 LAWFUL GROUNDS AND FURTHER PROCESSING UNDER THE PSD2

2.1 Lawful grounds for processing

13. Under the GDPR, controllers must have a legal basis in order to process personal data. Article 6 (1) of the GDPR constitutes an exhaustive and restrictive list of six legal bases for processing of personal data under the GDPR[13]. It is up to the controller to define the appropriate legal basis and ensure that all conditions for this legal basis are met. Determining which basis is valid and most appropriate in a specific situation depends on the circumstances under which the processing takes place, including the purpose of the processing and relationship between the controller and the data subject.

2.2 Article 6(1)(b) of the GDPR (processing is necessary for the performance of a contract)

14. Payment services are provided on a contractual basis between the payment services user and the payment services provider. As stated in recital 87 of the PSD2, "*[t]his Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider.*" In terms of the GDPR, the main legal basis for the processing of personal data for the provision of payment services is Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

15. The payment services under the PSD2 are defined in annex 1 of the PSD2. The provision of these services as defined by the PSD2 is a requirement for the establishment of a contract in which parties have access to payment account data of the payment service user. These payment service providers also have to be licenced operators. In relation to payment initiation services and account information services under the PSD2, contracts may incorporate terms that also impose conditions about additional services that are not regulated by the PSD2. The *EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* make clear that controllers have to assess what processing of personal data is objectively necessary to perform the contract. These Guidelines point out that the justification of the necessity is dependent on the nature of the service, the mutual perspectives

[13] According to Article 6 processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

and expectations of the parties to the contract, the rationale of the contract and the essential elements of the contract.

16. The EDPB guidelines 2/2019 also make clear that, in light of Article 7(4) of the GDPR, a distinction is made between processing activities necessary for the performance of a contract and terms making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract. 'Necessary for performance' clearly requires something more than a contractual condition[14]. The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. Merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b) of the GDPR.

17. Article 5 (1) (b) of the GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. When assessing whether Article 6(1)(b) is an appropriate legal basis for an online (payment) service, regard should be given to the particular aim, purpose, or objective of the service[15]. The purposes of the processing must be clearly specified and communicated to the data subject, in line with the controller's purpose limitation and transparency obligations. Assessing what is 'necessary' involves a combined, fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal". Article 6(1)(b) does not cover processing which is useful but not objectively necessary for performing the contractual service or for taking relevant pre-contractual steps at the request of the data subject, even if it is necessary for the controller's other business purposes[16].

18. The EDPB Guidelines 2/2019 make clear that contracts cannot artificially expand the categories of personal data or types of processing operation that the controller needs to carry out for the performance of the contract within the meaning of Article 6(1)(b)[17]. These Guidelines also address cases in which 'take it or leave it' situations may be created for data subjects who may only be interested in one of the services. This could happen when a controller wishes to bundle several separate services or elements of a service with different fundamental purposes, features or rationale into one contract. Where the contract consists of several separate services or elements of a service that can in fact reasonably be performed independently of one another, the applicability of Article 6(1)(b) should be assessed in the context of each of those services separately, looking at what is objectively necessary to perform each of the individual services which the data subject has actively requested or signed up for[18].

19. In line with the abovementioned Guidelines, controllers have to assess what is objectively necessary for the performance of the contract. Where controllers cannot demonstrate that the processing of the personal payment account data is objectively necessary for the provision of each of these services separately, Article 6 (1) (b) of the GDPR is not a valid legal ground for processing. In these cases, the controller should consider another legal basis for processing.

[14] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, EDPB, page 8.
[15] Idem.
[16] Idem, page 7.
[17] Idem, page 10.
[18] Idem, page 11.

2.3 Fraud prevention

20. Article 94 (1) PSD2 states that Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of personal data strictly necessary for the purposes of preventing fraud could constitute a legitimate interest of the payment service provider concerned, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject[19]. Processing activities for the purpose of fraud prevention should be based on a careful case by case evaluation by the controller, in accordance with the accountability principle. In addition, to prevent fraud, controllers may also be subject to specific legal obligations that necessitate the processing of personal data.

2.4 Further processing (AISP and PISP)

21. Article 6 (4) of the GDPR determines the conditions for the processing of personal data for a purpose other than that for which the personal data have been collected. More specifically, such further processing may take place, where it is based on a Union or Member State law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), where the data subject has given their consent or where the processing for a purpose other than that for which the personal data were collected is compatible with the initial purpose.

22. Articles 66 (3) (g) and 67 (2) (f) of the PSD2 have to be taken into careful consideration. As mentioned above, Article 66 (3) (g) of the PSD2 states that the PISP shall not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer. Article 67 (2) (f) of the PSD2 states that the AISP shall not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

23. Consequently, Article 66(3)(g) and Article 67 (2) (f) of the PSD2 considerably restrict the possibilities for processing for other purposes, meaning that the processing for another purpose is not allowed, unless the data subject has given consent pursuant to Article 6(1)(a) of the GDPR or the processing is laid down by Union law or Member State law to which the controller is subject, pursuant to Article 6 (4) of the GDPR. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law, the restrictions laid down in Article 66(3)(g) and Article 67(2)(f) of the PSD2 make clear that any other purpose is not compatible with the purpose for which the personal data are initially collected. The compatibility test of Article 6(4) GDPR cannot result in a legal basis for processing.

24. Article 6 (4) of the GDPR allows for further processing based on Union or Member State law. For example, all PISPs and AISPs are obliged entities under Article 3 (2) (a) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing of the anti-money laundering directive. These obliged entities are therefore compelled to apply the customer due diligence measures as specified in the directive. The personal data processed in connection with a

[19] Recital 47 GDPR.

PSD2 service are, therefore, further processed based on at least one legal obligation resting on the service provider[20].

25. As mentioned in paragraph 20, Article 6 (4) of the GDPR indicates that the processing for a purpose other than that for which the personal data have been collected could be based on the data subject's consent, if all the conditions for consent under the GDPR are met. As set out above, the controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42 of the GDPR).

2.5 Lawful ground for granting access to the Account (ASPSPs)

26. As mentioned in paragraph 10, payment service users can exercise their right to make use of payment initiation and account information services. The obligations imposed on the Member States in Articles 66(1) and 67(1) of the PSD2 should be implemented in national law in order to guarantee the effective application of the right of the payment service user to benefit from the aforementioned payment 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.

27. The processing of personal data by the ASPSP consisting of granting access to the personal data requested by the PISP and AISP in order to perform their payment service to the payment service user is based on a legal obligation. In order to achieve the objectives of the PSD2, ASPSPs must provide the personal data for the PISPs´ and AISPs´ services, which is a necessary condition for PISPs and AISPs to provide their services and thus ensure the rights provided for in Articles 66(1) and 67(1) of the PSD2. Therefore, the applicable legal ground in this case is Article 6 (1) (c) of the GDPR.

28. As the GDPR has 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), the obligation for ASPSPs to grant access should stem from the national law transposing the PSD2.

[20] Note that a thorough examination of the question whether the anti-money laundering directive meets the standard of Art. 6 (4) GDPR falls outside of the scope of this document.

3 EXPLICIT CONSENT

3.1 Consent under the GDPR

29. Under the GDPR, consent serves as one of the six legal grounds for the lawfulness of processing of personal data. Article 4 (11) of the GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". These four conditions, freely given, specific, informed, and unambiguous, are essential for the validity of consent. According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, consent can only be an appropriate lawful basis if a data subject is offered control and a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid legal basis for processing, rendering the processing activity unlawful[21].

30. The GDPR also contains further safeguards in Article 7, which sets out that the data controller must be in a position to demonstrate that there had been valid consent at the time of processing. Also, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Furthermore, the data subject must be informed of the right to withdraw consent at any time, in just as simple a way as it was to grant consent.

31. According to Article 9 GDPR, consent is one of the exceptions from the general prohibition for processing special categories of personal data. However, in such case the data subject's consent must be 'explicit'[22].

32. According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, explicit consent under the GDPR refers to the way consent is expressed by the data subject. It means that the data subject should give an express statement of consent for specific processing purpose(s). An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.

33. Under no circumstances can consent be inferred from potentially ambiguous statements or actions. A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service.

3.2 Consent under the PSD2

34. The EDPB notes that the legal framework regarding explicit consent is complex, since both the PSD2 and the GDPR include the concept of 'explicit consent'. This leads to the question whether "explicit consent" as mentioned in Article 94 (2) PSD2 should be interpreted in the same way as explicit consent under the GDPR.

[21] Guidelines 05/2020 on consent under Regulation 2016/679, EDPB, para. 3.

[22] See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.

3.2.1 Explicit consent under Article 94 (2) PSD2

35. The PSD2 includes a number of specific rules concerning the processing of personal data, in particular in Article 94 (1) of the PSD2, which determines that the processing of personal data for the purposes of the PSD2 must comply with EU data protection law. Furthermore, Article 94 (2) of the PSD2 sets out that payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user. Pursuant to Article 33 (2) of the PSD2, this requirement of the explicit consent of the payment service user does not apply to AISPs. However, Article 67 (2)(a) of the PSD2 still provides for explicit consent for AISPs for the provision of the service.

36. As mentioned above, the list of lawful bases for processing under the GDPR is exhaustive. As mentioned in paragraph 14, the legal basis for the processing of personal data for the provision of payment services is, in principle, Article 6(1)(b) of the GDPR, meaning that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. From that, it follows that Article 94 (2) of the PSD2 cannot be regarded as an additional legal basis for processing of personal data. The EDPB considers that, in view of the foregoing, this paragraph should be interpreted, on the one hand, in coherence with the applicable data protection legal framework and, on the other hand, in a way that preserves its useful effect. Explicit consent under Article 94(2) PSD2 should therefore be regarded as an additional requirement of a contractual nature[23] in relation to the access to and subsequently processing and storage of personal data for the purpose of providing payment services and is therefore not the same as (explicit) consent under the GDPR.

37. "Explicit consent" referred to in Article 94 (2) PSD2 is a contractual consent. This implies that Article 94 (2) PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under the PSD2, data subjects must be made fully aware of the specific categories of personal data that will be processed. Further, they have to be made aware of the specific (payment service) purpose for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject.

38. Central to the notion of "explicit consent" under Article 94 (2) of the PSD2 is the gaining of access to personal data to subsequently process and store these data for the purpose of providing payment services. This implies that the payment service[24] provider is not yet processing the personal data, but needs access to personal data that have been processed under the responsibility of any other controller. If a payment service user enters into a contract with, for example, a payment initiation service provider, this provider needs to obtain access to personal data of the payment service user that is being processed under the responsibility of the account servicing payment service provider. The object of the explicit consent under Article 94 (2) PSD2 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service. If explicit consent is given by the data subject, the account servicing payment service provider is obliged to give access to the indicated personal data.

39. Although the consent of Article 94 (2) of the PSD2 is not a legal ground for the processing of personal data, this consent is specifically related to personal data and data protection, and ensures

[23] Letter of the EDPB regarding the PSD2 directive, 5 July 2018, page 4.
[24] This applies to services 1 to 7 of Annex 1 of the PSD2.

transparency and a degree of control for the payment service user[25]. While the PSD2 does not specify the substantive conditions for consent under Article 94 (2) PSD2, it should, as stated above, be understood in coherence with the applicable data protection legal framework and in a way that preserves its useful effect.

40. With regard to the information to be provided by controllers and the requirement of transparency, Article 29 Working Party Guidelines on Transparency specifies that a "*A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used*"[26].

41. Furthermore, as required by the principle of purpose limitation, personal data must be collected for specified, explicit and legitimate purposes (Article 5 (1) (b) of the GDPR). Where personal data are collected for more than one purpose, "*controllers should avoid identifying only one broad purpose in order to justify various further processing activities which are in fact only remotely related to the actual initial purpose*"[27]. The EDPB has highlighted, most recently in the context of contracts for online services, the risk of inclusion of general processing terms in contracts and has stated that the purpose of the collection should be clearly and specifically identified: it should be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied[28].

42. When considered in the context of the additional requirement of explicit consent pursuant to Article 94(2) of the PSD2, this entails that controllers must provide data subjects with specific and explicit information about the specific purposes identified by the controller for which their personal data are accessed, processed and retained. In line with Article 94(2) of the PSD2, the data subjects must explicitly accept these specific purposes.

43. Furthermore, as set out above in paragraph 10, the EDPB highlights that the payment service user must be able to choose whether or not to use the service and cannot be forced to do so. Therefore, the consent under Article 94 (2) of the PSD2 also has to be a freely given consent.

3.3 Conclusion

44. Explicit consent under the PSD2 is different from (explicit) consent under the GDPR. Explicit consent under Article 94 (2) of the PSD2 is an additional requirement of a contractual nature. When a payment service provider needs access to personal data for the provision of a payment service, explicit consent in line with Article 94 (2) of the PSD2 of the payment service user is needed.

[25] Art. 94 (2) PSD2 falls under Chapter 4 'Data protection'.
[26] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, paragraph 10 (adopted on 11 April 2018) - endorsed by the EDPB.
[27] Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 16.
[28] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, paragraph 16 (public consultation version) and Article 29 Working Party Opinion 03/2013 on purpose limitation (WP203), page 15–16.

4 THE PROCESSING OF SILENT PARTY DATA

4.1 Silent party data

45. A data protection issue that needs careful consideration, is the processing of so called 'silent party data'. In the context of this document, silent party data are personal data concerning a data subject who is not the user of a specific payment service provider, but whose personal data are processed by that specific payment service provider for the performance of a contract between the provider and the payment service user. This is for example the case where a payment service user, data subject A, makes use of the services of an AISP, and data subject B has made a series of payment transactions to the payment account of data subject A. In this case, data subject B is regarded as the 'silent party' and the personal data (such as the account number of data subject B and the amount of money that was involved in these transactions) relating to data subject B, is regarded as 'silent party data'.

4.2 The legitimate interest of the controller

46. Article 5 (1) (b) GDPR requires that personal data are only collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. In addition, the GDPR requires that that any processing of personal data must be both necessary as well as proportionate and in line with the data protection principles, such as those of purpose limitation and data minimisation.

47. The GDPR may allow for the processing of silent party data when this processing is necessary for purposes of the legitimate interests pursued by a controller or by a third party (Article 6 (1)(f) GDPR). However, such processing can only take place when the legitimate interest of the controller is not "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".

48. 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. The necessity to process personal data of the silent party is limited and determined by the reasonable expectations of these data subjects. In the context of providing payment services that are covered by the PSD2, effective and appropriate measures have to be established to safeguard that the interests or fundamental rights and freedoms of the silent parties are not overridden, and to ensure that the reasonable expectations of these data subjects regarding the processing of their personal data are respected. In this respect, the controller (AISP or PISP) 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. If feasible, also encryption or other techniques should be applied to achieve an appropriate level of security and data minimisation.

4.3 Further processing of personal data of the silent party

49. As stated under paragraph 29, personal data processed in connection with a payment service regulated by the PSD2, could be further processed based on legal obligations resting on the service provider. These legal obligations could concern personal data of the silent party.

50. 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 the personal data have been collected, other on the basis of EU or Member State law. Consent of the

silent party is legally not feasible, because in order to obtain consent, personal data of the silent party would have to be collected or processed, for which no legal ground can be found under Article 6 GDPR. The compatibility test of Article 6.4 of the GDPR cannot offer a ground for the processing for other purposes (e.g. direct marketing activities) either. 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[29]; the absence of any connection between any other purpose and the purpose for which the personal data were initially collected (i.e. the fact that PSPs only need the silent party data in order to perform a contract with the other contracting party); the nature of the personal data involved[30], the circumstance that data subjects are not in a position to reasonably expect any further processing or to even be aware which controller may be processing their personal data and given the legal restrictions on processing set out in Article 66 (3) (g) and Article 67 (2) (f) of PSD2.

[29] Recital 87 of PSD2 states that PSD2 only concerns 'contractual obligations and responsibilities between the payment service user and the payment service provider'. Silent Party Data therefore do not fall under the scope of PSD2.

[30] Particular care should be taken when processing financial personal data, as the processing can be considered as increasing the possible risk to the rights and freedoms of individuals, according to the Guidelines on Data Protection Impact Assessment (DPIA).

5 THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA UNDER THE PSD2

5.1 Special categories of personal data

51. Article 9 (1) GDPR prohibits the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

52. It should be emphasised that in some Member States, electronic payments are already ubiquitous, and are favoured by many people over cash in their day to day transactions. At the same time, financial transactions can reveal sensitive information about an individual data subject, including those related to special categories of personal data. For example, depending on the transaction details, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. Trade union membership may be revealed by the deduction of an annual membership fee from a person's bank account. Personal data concerning health may be gathered from analysing medical bills paid by a data subject to a medical professional (for instance a psychiatrist). Finally, information on certain purchases may reveal information concerning a person's sex life or sexual orientation. As shown by these examples, even single transactions can contain special categories of personal data. Moreover, account information services might rely on profiling as defined by article 4 (4) of the GDPR. As previously stated in the Working Party 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as endorsed by the EDPB , "profiling can create special category of data by inference from data which is not special category of data in its own right, but becomes so when combined with other data."[31] This means that, through the sum of financial transactions, different kinds of behavioural patterns can be revealed, which may include special categories of personal data. Therefore, the chances are considerable that a service provider processing information on financial transactions of data subjects also processes special categories of personal data.

53. With regard to the term 'sensitive payment data', the EDPB notes the following. The definition of sensitive payment data in the PSD2 differs considerably from the way the term 'sensitive personal data' is commonly used within the context of the GDPR and data protection (law). Where the PSD2 defines 'sensitive payment data' as 'data, including personalized security credentials which can be used to carry out fraud', the GDPR emphasises the need for specific protection of special categories of personal data which under Article 9 of the GDPR are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, such as special categories of personal data[32]. In this regard it is recommended to at least map out and categorize precisely what kind of personal data will be processed. Most probably a Data Protection Impact Assessment (DPIA) will be required in accordance with article 35 GDPR, which will help in this mapping exercise. More guidance on DPIAs can be found in the Working Party 29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation

[31] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 15.
[32] For example, in recital 10 of the GDPR, special categories of personal data are being referred to as 'sensitive data'.

2016/679, as endorsed by the EDPB.

5.2 Possible derogations

54. The prohibition of Article 9 GDPR is not absolute. In particular, whereas derogations of paragraphs (b)-(f) and (h)-(j) of Article 9 (2) GDPR are manifestly not applicable to the processing of personal data in the PSD2 context, the following two derogations in Article 9 (2) GDPR could be considered:

a) The prohibition does not apply if the data subject has given explicit consent to the processing of those personal data for one or more specified purposes (Article 9 (2) (a) GDPR).

b) The prohibition does not apply if the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9 (2) (g) GDPR).

55. It should be pointed out that the list of derogations in Article 9 (2) GDPR is exhaustive. The possibility that special categories of personal data are included in the personal data processed for the provision of any of the services falling under the PSD2 must be recognised by the service provider. As the prohibition of Article 9 (1) GDPR is applicable to these service providers, they must ensure that one of the exceptions in Article 9 (2) GDPR is applicable to them. It should be emphasised that where the service provider cannot show that one of the derogations is met, the prohibition of article 9 (1) is applicable.

5.3 Substantial public interest

56. Payments services may process special categories personal data for reasons of substantial public interest, but only when all the conditions of Article 9 (2) (g) of the GDPR are met. This means that the processing of the special categories of personal data has to be addressed in a specific derogation to article 9 (1) GDPR in Union or Member State law. This provision will have to address the proportionality in relation to the pursued aim of the processing and contain suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Furthermore, this provision under Union or Member State law will have to respect the essence of the right to data protection. Finally, the processing of the special categories of data must also be demonstrated to be necessary for the reason of the substantial public interest, including interests of systemic importance. Only when all of these conditions are fully met, this derogation could be made applicable to designated types of payment services.

5.4 Explicit consent

57. In cases where the derogation of article 9 (2) (g) GDPR does not apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR, seems to remain the only possible lawful derogation to process special categories of personal data by TPPs. The EDPB Guidelines 05/2020 on consent under Regulation 2016/679 states[33] that: “Article 9(2) does not recognize “necessary for the performance of a contract” as an exception to the general prohibition to process special categories of data. Therefore, controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). When service providers rely on Article 9 (2) (a) GDPR, they must ensure that they have been granted explicit

[33] Guidelines 05/2020 on consent under Regulation 2016/679, EDPB, para. 99

consent before commencing the processing." Explicit consent as set out in Article 9 (2) (a) GDPR must meet all the requirements of the GDPR.

5.5 No suitable derogation

58. 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 could 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.

6 DATA MINIMISATION, SECURITY, TRANSPARANCY, ACCOUNTABILITY AND PROFILING

6.1 Data minimisation and data protection by design and default

59. The principle of data minimisation is enshrined in Article 5 (1) (c) GDPR: "Personal data shall be […] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Essentially, under the principle of data minimisation, controllers should process no more personal data than what is necessary in order to achieve the specific purpose in question. As pointed out in Chapter 2, the amount and the kind of personal data necessary to provide the payment service is determined by the objective and mutually understood contractual purpose[34]. Data minimisation is applicable to every processing (e.g. every collection of or access to and request of personal data). The EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (DPbDD), state that 'processors and technology providers are also recognised as key enablers for DPbDD, they should also be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection[35].'

60. Article 25 of the GDPR contains the obligations to apply data protection by design and by default. These obligations are of particular importance to the principle of data minimisation. This Article determines that controllers shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. These measures may include encryption, pseudonymisation and other technical measures.

61. When the obligation of article 25 of the GDPR is applied, the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing are the elements that have to be taken into account. Further clarifications about this obligation are given in the abovementioned EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

6.2 Data minimisation measures

62. 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. As has been shown in Chapter 2, the PSD2 requires ASPSPs to share payment service user information on request of the payment service user, when the payment service user wishes to use a payment initiation service or an account information service.

[34] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, EDPB, para 32
[35] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, page 29.

63. When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories should 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 and the transaction characteristics. Also, unless required by Member State or EU law, the IBAN of the silent party's bank account may not need to be displayed.

64. In this respect, the possible application of technical measures that enable or support TPPs in their obligation to access and retrieve only the personal data necessary for the provision of their services could be considered, as part of the implementation of appropriate data protection policies, in line with article 24 (2) GDPR. In this respect, the EDPB recommends the usage of digital tools in order to support AISPs in their obligation to only collect personal data that are necessary for the purposes for which they are processed. For instance, when a service provider does not need the transaction characteristics (in the description field of the transaction records) for the provision of their service, a digital selection tool could function as a means for TPPs to exclude this field from the overall processing operations by the TPP.

Example 2:

HappyPayments, our Account Information Service provider from example 1, wants to ensure that it only processes the personal payment account data which its users are interested in. To seek access to more payment account data would not be necessary for the provision of the service. Therefore, it allows the users to select the specific types of information they are interested in.

User A wants an overview of its spending for the last two months. Thus, it asks for its two banking accounts, held with two different ASPSPs, the information on all transactions of the last two months, the transaction amount, the date of execution and the recipient's name, and ticks the corresponding boxes in HappyPayments' user interface.

HappyPayments then commences to request from the respective ASPSPs only the information corresponding to the fields set by User A and only for the period of the last two months. Information such as the "communication" of the transfer or even the IBAN are not requested, as User A did not ask for this information.

To allow HappyPayments to comply with its data minimisation obligations, the ASPSPs allow HappyPayments to request specific fields for a range of dates.

65. 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.

66. Besides collecting as little data as possible, the service provider also has to implement limited retention periods. Personal data should not be stored by the service provider for a period longer than is necessary in relation to the purposes requested by the payment service user.

67. If the contract between the data subject and the AISP requires the transmission of personal data to third parties, then only those personal data that are necessary for the execution of the contract can be transmitted. Data subjects should also be specifically informed about the transmission and the personal data that are going to be transmitted to this third party.

6.3 Security

68. The EDPB already highlighted that the violation of financial personal data *"clearly involves serious impacts in the data subject's daily life*" and quotes the risks of payment fraud as an example[36].

69. Where a data breach involves financial data, the data subject may be exposed to considerable risks. Depending on the information that is leaked, data subjects may be exposed to a risk of identity theft, of theft of the funds in their accounts and other assets. Furthermore, there is the possibility that the exposure of transaction data is related to considerable privacy risks, as transaction data may contain references to all aspects of a data subject's private life. At the same time, financial data are obviously valuable to criminals and therefore an attractive target.

70. As controllers, payment service providers are obligated to take adequate measures to protect the personal data of data subjects (Article 24 (1) GDPR). The higher the risks associated with the processing activity carried out by the controller, the higher the security standards that need to be applied. As the processing of financial data is connected to a variety of severe risks, the security measures should be accordingly high.

71. Service providers should be held to high standards, including strong customer authentication mechanisms and high security standards for the technical equipment[37]. Other procedures, such as vetting processors for security standards and implementing procedures against unauthorised access, are also important.

6.4 Transparency and accountability

72. Transparency and accountability are two fundamental principles of the GDPR.

73. With regard to transparency (Article 5 (1)(a) of the GDPR), Article 12 of the GDPR specifies that controllers shall take appropriate measures to provide any information referred to in Articles 13 and 14 GDPR. Furthermore, it requires that the information or communication about the processing of personal data must be concise, transparent, intelligible and easily accessible. The information must be in clear and plain language and in writing "or by other means, including where appropriate, by electronic means". The Article 29 Working Party 'Guidelines on transparency under Regulation 2016/679', as endorsed by the EDPB, offers specific guidance for compliance with the principle of transparency in digital environments.

74. According to the abovementioned Guidelines on transparency under Regulation 2016/679, Article 11 GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights should be made possible with the help of additional information provided by the data subject. There may be situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

75. For the services under the PSD2, Article 13 GDPR is applicable for the personal data collected from the data subject and Article 14 is applicable where personal data have not been obtained from the data subject.

[36] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 - endorsed by the EDPB.
[37] See the RTS.

76. In particular, the data subject has to be informed about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period, and where applicable, the legitimate interests pursued by the controller or by a possible third party. Where processing is based on consent as referred to in Article 6(1) (a) GDPR or explicit consent as referred to in Article 9(2) (a) GDPR, the data subject has to be informed of the existence of the right to withdraw consent at any time.

77. The controller shall provide the information to the data subject, having regard to the specific circumstances in which the personal data are processed. If the personal data are to be used for communication with the data subject[38], which will probably will be the case for AISPs, the information has to be provided at the latest at the time of the first communication to that data subject. If personal data are to be disclosed to another recipient, the information has to be provided at the latest when the personal data are first disclosed.

78. With regard to online payment services, the abovementioned Guidelines clarify that a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. It is in particularly recommended that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on a screen, in order to avoid information fatigue, and at the same time ensuring the effectiveness of the information.

79. The abovementioned Guidelines also clarify that controllers may choose to use additional tools to provide information to the individual data subject, such as privacy dashboards. A privacy dashboard is a single point from which data subjects can view 'privacy information' and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the controller in question[39]. A privacy dashboard could provide an overview of the TPPs that have obtained the data subjects explicit consent, and could also offer relevant information on the nature and amount of personal data that has been accessed by TPPs. In principle, an ASPSP may offer the user the possibility to withdraw a specific explicit PSD2 consent[40] through the overview, which would result in a denial of access to their payment accounts to one or more TPPs. The user could also request an ASPSP to deny access to their payment account(s) to one or more particular TPPs[41], as it is the right of the user to (not) make use of an account information service. If privacy dashboards are used in order to give or withdraw an explicit consent, they should be designed and applied lawfully and in particular prevent creating obstacles to the TPPs right to provide services in accordance with the PSD2. In this respect and in accordance with the applicable provisions under the PSD2, a TPP has the possibility to obtain explicit consent from the user again after this consent has been withdrawn.

80. The accountability principles requires the controller to lay down appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in

[38] Art. 14 (3) (b) of the GDPR.

[39] According to the Article 29 Working Party Guidelines on transparency under Regulation 2016/679 - endorsed by the EDPB, privacy dashboards are particularly useful when the same service is used by data subjects on a variety of different devices as they give them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject.

[40] See for example the 'explicit consent' mentioned in Article 67 (2) (a) of the PSD2.

[41] See also EBA/OP/2020/10, paragraph 45

accordance with the GDPR, in particular with the main data protection principles provided for by Article 5 (1). Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons, and must be reviewed and updated when necessary[42].

6.5 Profiling

81. The processing of personal data by payment service providers may entail 'profiling' as referred to in Article 4 (4) of the GDPR. For example, AISPs could rely on automated processing of personal data in order to evaluate certain personal aspects relating to a natural person. A data subject's personal financial situation could be evaluated, depending on the specifics of the service. Account information services, to be provided as requested by users, may involve an extensive evaluation of personal payment account data.

82. The controller also has to be transparent to the data subject on the existence of automated decision-making, including profiling. In those cases, the controller has to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Article 13(2) (f) and Article 14 (2) (g) and recital 60)[43]. Likewise, under Article 15 of the GDPR the data subject has the right to request and obtain information from the controller about the existence of automated decision-making, including profiling, the logic involved and the consequences for the data subject, and, in certain circumstances, a right to object to profiling, regardless of whether solely automated individual decision-making based on profiling takes place[44].

83. Furthermore, what is also relevant in this context is the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affecting him or her, provided for by Article 22 of GDPR. This norm also includes, in certain circumstances, the need for data controllers to implement suitable measures to safeguard the data subject's rights such as specific information to the data subject, the right to obtain human intervention in the decision making and to express his or her point of view and contest the decision. As also stated in recital 71 of GDPR this means, inter alia, that data subjects have the right not to be subject to a decision, such as automatic refusal of an online credit application without any human intervention[45].

84. Automated decision-making, including profiling that involves special categories of personal data is only allowed under the cumulative conditions of Article 22(4) GDPR:

- there is an applicable Article 22(2) exemption;
- and paragraph (a) or (g) of Article 9(2) GDPR applies. In both cases, the controller shall put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests[46].

85. The requirements for further processing, as stated in these guidelines, should also be observed. The clarifications and instructions on automated individual decision-making and profiling given by

[42] Art. 5(2) and Art. 24 GDPR.
[43] Guidelines on transparency under Regulation 2016/679, WP 260 rev.01 - endorsed by the EDPB
[44] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01
[45] Recital 71 GDPR.
[46] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 24.

the Working Party 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as endorsed by the EDPB, are fully relevant in the context of payment services and should therefore be duly considered.

For the European Data Protection Board

The Chair

(Andrea Jelinek)