

Brussels, 5 July 2018  
EDPB-84-2018

Sophie in 't Veld,  
Member of the European Parliament  
60 rue Wiertz  
Brussels  
Belgium

Dear Ms in 't Veld,

On 16 February 2018 the Article 29 Working Party (WP29) received your letter regarding the revised Payment Services Directive (hereafter 'PSD2'). In this letter you request the European Commission (Commission), the European Data Protection Supervisor (EDPS) and the WP29 to provide further clarification regarding a number of issues related to PSD2 and the protection of personal data.

As you already mentioned in your letter, the General Data Protection Regulation (GDPR) has been applicable since 25 May 2018. As from this date, the WP29 has been replaced by the European Data Protection Board (EDPB), the EU body composed of representatives of the national data protection authorities and the European Data Protection Supervisor and whose tasks and powers are set forth by Article 70 of the GDPR. The WP29 at the time was not officially involved during the process of negotiating PSD2 and the Regulatory Technical Standards (hereafter 'RTS'). Nevertheless the European Supervisory authorities which now make up the EDPB are aware of current discussions within Member States regarding the (implementation of) PSD2, more specifically in relation to the protection of personal data. The legal framework regarding the protection of personal data in the context of PSD2 is complex and developments in this regard are therefore being monitored by the EDPB.

## **Legal framework**

The EDPB notes that PSD2 includes a number of specific rules concerning the processing of personal data, in particular in Article 94 which provides that the processing of personal data for the purposes of PSD2 must be compliant with EU data protection law.

Moreover, it is explicitly mentioned in Recital 89 of PSD2 (on the processing of personal data for the provision of payment services) that the precise purpose should be specified, the relevant legal basis referred to, the relevant security requirements laid down in Directive 95/46/EC complied with, and the principles of necessity, proportionality, purpose limitation and proportionate data retention period 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 this Directive.

The GDPR lays down a strong and coherent data protection framework, whose consistent and homogenous application should be ensured throughout the Union. Article 94 GDPR states that references to the repealed Directive 95/46 shall be construed as references to the GDPR. Hence, the interpretation and the implementation<sup>1</sup> of the articles in PSD2 have to be made in light of the GDPR. Member States had to transpose PSD2 into national law before 13 January 2018. As the GDPR has been applicable since 25 May 2018, we expect that the national implementation laws are also in full consistency with that data protection legal framework.

In your letter you raised some specific issues.

## **Silent party data**

Concerning “silent party data”, you raised the question whether the processing of personal data of “silent parties” is legitimate when explicit consent for the processing of personal data has (only) been given by another data subject. In relation to PSD2, this would for instance be the case when data subject A - being a payment service user under PSD2 - has given explicit consent to a Payment Initiation Service Provider (PISP) to process personal data for the performance of this service, based on Article 94 (2) of PSD2. When data subject A uses the services of a PISP to transfer money to data subject B without there being a contractual relation between data subject B and the PISP, the question is whether the PISP can also process the data of data subject B – being a silent party - in order to make the transfer possible.

In your letter you stated that additional clarification is required relating to the question whether the legal framework allows for this kind of processing of silent party data, for instance with reference to “legitimate interest” (Article 6 (1)(f) GDPR).

---

<sup>1</sup> See Recital 90 of PSD2.



The EDPB considers that personal data can only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes. Furthermore, the EDPB notes that the GDPR may indeed allow for the processing of personal data based on the legitimate interests pursued by a controller or by a third party *ex Article 6 (1)(f)*. It should, however, be noted that 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*”.<sup>2</sup> In addition the EDPB notes that any processing of personal data based on the GDPR must be both necessary as well as proportional and in line with the other principles of the GDPR, such as those of purpose limitation, data minimisation and transparency. A lawful basis for the processing of these silent party data by PISPs or Account Information Service Providers (AISPs) - in the context of payment and account services under PSD2 - could be the legitimate interest of a controller or a third party *ex Article 6 (1)(f)* to perform the contract with the service user. This means that the legitimate interest of the controller is *limited and determined* by the reasonable expectations of data subjects.<sup>3</sup>

In addition, with regard to further processing<sup>4</sup> 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, also given the restrictions on processing set out in Article 66 (3) (g) and Article 67 (2) (f) of PSD2 and that data subjects do not reasonably expect any further processing.

### **Explicit consent**

In addition to the processing of silent party data, you raised the question whether the legal framework is sufficiently clear regarding the process of issuing and withdrawing consent under PSD2.

In this regard, the EDPB notes that the legal framework regarding explicit consent is complex, since both PSD2 as the GDPR include the concept of “explicit consent”.<sup>5</sup> This leads to the question whether “explicit consent” as mentioned in Article 94 (2) of PSD2<sup>6</sup> should be interpreted in the same way as explicit consent under the GDPR.

---

<sup>2</sup> Article 6 (1) (f) GDPR: “*Processing shall be lawful only if and to the extent that 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.*”

<sup>3</sup> See Recital 47 of GDPR.

<sup>4</sup> Article 6 (4) (b) 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 which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller.*”

<sup>5</sup> PSD2 uses the notion of “consent” and “explicit consent” with a different meaning than that under GDPR see e.g. Article 4 (23), Article 52 (2) (c), Article 64, Article 65 (1) (b) and (2) (a) of PSD2.

<sup>6</sup> Article 94 (2) of PSD2: “*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.*”

The EDPB is of the view that the “explicit consent” referred to in Article 94 (2) of PSD2 is a contractual consent. Payment services are always provided on a contractual basis between the payment services user and the payment services provider. As stated in recital 87 of PSD2, *"This Directive should concern only contractual obligations and responsibilities between the payment service user and the payment service provider."* In terms of the GDPR, the legal basis for the processing of personal data 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. We consider that, in view of the foregoing, article 94(2) of PSD2 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. This implies that Article 94 (2) of PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes 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. The concept of explicit consent under Article 94(2) of PSD2 is therefore an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR.

Further processing of personal data for other purposes, not necessary for the performance of the contract, could be based on consent under Article 6(1) (a) GDPR, provided that the requirements and the conditions for consent laid out in Article 7 and Article 4 (11) GDPR<sup>7</sup> are fully respected. Consideration should also be given to the need to respect the specific conditions of Article 9 GDPR in case special categories of personal data are being processed. For the EDPB it is clear that consent under the GDPR is a reversible decision and that a data subject can exercise control over these processing activities.

### **Regulatory Technical Standards**

The RTS on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) are established by the European Banking Authority (EBA) with the aim to enhance consumer protection, promoting innovation and improving the security of payment services across the EU. The EDPB has not been officially consulted during their development, but -without prejudice to possible future considerations- it should however be noted that, in respect of security of payment services, PSD2 introduces standards, such as effective incident management procedures and stronger authentication procedures<sup>8</sup> and underlines the responsibility of payment service providers in ensuring security.

---

<sup>7</sup> Article 4 (11) GDPR: *"Consent of the data subject under the GDPR means 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."*

<sup>8</sup> Regarding the notion of authentication the EDPB considers that this term ('authentication') in practice might be ambiguous under the PSD2 Directive. Authentication is a technical measure to ensure that the person who has given his or her consent is the legitimate user of the service, and must not be confused with the consent itself.



## **Position of Banks**

In your letter you requested further clarification regarding the question whether “banks are sufficiently cooperative in establishing secure interfaces and avoiding alternative, less secure, methods of accessing account data”. This question touches upon the new obligations of banks from a competition perspective. The EDPB considers that – should this comment have been made from the perspective of competition law - it is neither the task nor the competence of Data Protection Authorities to assess whether banks are sufficiently cooperative in establishing such interfaces from the perspective of competition law.

Regarding the question whether the interfaces that are - or will be - established are sufficiently secure from a data protection perspective, the EDPB remarks that Data Protection Authorities are fully competent to assess whether banks provide a level of protection of personal data that is in line with the GDPR. In this respect, the EDPB highlights that Article 32 GDPR has strengthened the obligation for every organisation that processes personal data to take measures to ensure a level of security appropriate to the risks and that Article 25 GDPR provides for the obligation of data controllers to implement privacy by design and privacy by default measures to meet the data protection requirements and protect the rights of data subjects.

Data Protection Authorities may naturally decide to take appropriate action should there be any doubt regarding the safety of these new interfaces.

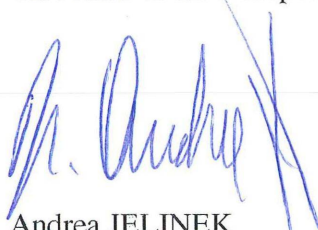
## **Further activities**

As mentioned at the beginning of this letter, the EDPB is aware of current discussions regarding PSD2 in relation to the protection of personal data and will continue monitoring the issue.

The EDPB notes that, as clearly shown by the interrelating points between PSD2 and GDPR, there may be relevant grounds for a fruitful interaction between EU competent bodies, in particular data protection and financial supervisory authorities. It therefore wishes that a dialogue among such authorities is started in order to set up a coordinated approach aiming at ensuring a strengthened and consistent protection for EU citizens.

Yours sincerely,

On behalf of the European Data Protection Board,



Andrea JELINEK

Chairperson

