YOUR TRAVEL PAYMENT COMPANY.

AirPlus INTERNATIONAL

Comments on the EDPB's consultation on Guidelines 06/2020 on the interplay of GDPR and PSD2

16th September 2020

A. Introduction

Since the entry into force of the PSD2 and its implementation in the respective national laws, the question arises as to how Article 94 para. 2 PSD2 is to be interpreted. A German payment service provider, such as Lufthansa AirPlus Servicekarten GmbH (hereinafter referred to as "AirPlus"), also had to deal with the question of how it should interpret the implementation law of Articles 94 PSD2 in Section 59 ZAG (Payment Services Regulation Act), since the European version was not incorporated literally into German law. German payment service providers therefore have to face a significant challenge, since, if German legislation is based on a European provision, they are obliged to give preference to the interpretation in which European law is best and most effectively enforced. A further challenge, analogous to the problem of implementing the requirements for strong customer authentication, is that the legislator appears to have focused primarily on payment services in B2C traffic, as is apparent from the recitals of the PSD2. Already during the discussion on strong customer authentication it has become clear that the B2B sector, especially in the Business Travel Management (BTM) sector, have an operating model that is different to others, i.e. in particular does not necessarily issue a plastic credit card based on a contract with the end-user.

AirPlus therefore very much welcomes the fact that the consultation procedure provides the opportunity to openly address challenges faced by payment service providers with the provision of Articles 94 para. 2 PSD2, allowing for an acceptable consensus in a broad discussion to be reached.

B. Summary

AirPlus considers that Article 94 PSD2 should not apply to the use of payment means in the B2B sector. Furthermore, Article 94 PSD2 should be interpreted restrictively against the background of the meaning and purpose of the provision when it concerns the processing of personal data for the fulfilment of legal requirements and the pursuit of legitimate interests. It should also be made clear that the EU-GDPR is lex specialis and lex posterior to the PSD2 concerning the processing of personal data in connection with the provision of payment services, in particular concerning long-established means of payment and payment processes.

This is justified as follows:

1. The use of a means of payment in the B2B sector is characterised in particular by the fact that the contract for the provision of the means of payment is not concluded with the data subject, but with the respective legal entity. The data subject in this context is a natural person who is authorised by the legal entity to use the payment means. Particularly, in the field of BTM, this typically includes all travellers of the payment service provider's contractual partner. Even though these data subjects' personal data is necessarily processed during the provision of the means of payment, no data covered by the actual protection objective of Articles 66, 67 PSD2 is processed. In particular, no data on the financial situation and/or creditworthiness of the data subject will be collected. A restriction of the available legal bases under Article 6 EU-GDPR based on the interpretation of Articles 66, 67 and 94 of the PSD2 is therefore disproportionate.

2. The specific wording (*with the explicit consent of the payment service user)* in Art. 94 para.2 PSD2 is in itself inconclusive. Consent can, by its very nature, only be given by the natural person (the data subject). In the B2B sector, the data subject is not the contractual partner of the payment service provider. Against the background of the meaning and purpose of Article 94 PSD2, over-regulation without added value is to be feared because, in particular, the objective of transparency with regard to data processing cannot be achieved in this way. The provision must therefore be interpreted restrictively in the B2B sector.

3. Furthermore, AirPlus considers the EU-GDPR as lex posterior and lex specialis concerning the processing of personal data in connection with the provision of payment services. AirPlus also takes the view that limiting the legal basis for the processing of personal data according to Art. 6 para. 1 EU-GDPR through Article 94 para. 2 PSD2 is not compatible with the EU-GDPR.

The European Data Protection Board - if possible in close consultation with the European Commission, the European Council and the European Parliament - **is therefore requested:**

> to clarify that Article 94 para. 2 PSD2 should **only apply** in the area of Account Information Service Provider (**AISP**) and Payment Initiation Service Provider (**PISP**) **in relation to consumers** covered by Articles 66 and 67 PSD2, but not in the B2B sector. Furthermore, it should be noted that **Article 94 para. 2 PSD2 is to be interpreted restrictively** against the background of the meaning and purpose of the provision, when it concerns the legal basis for processing of personal data. Furthermore, it is requested to confirm that the **EU-GDPR is lex specialis and lex posterior to PSD2 with regard to the applicable legal basis for data processing**, at least in the area of the provision of payment services in the B2B sector.

C. Reasoning

The above summary is the result of the legal interpretation of Article 94 para. 2 PSD2 by AirPlus.

I. Interpretation

1. Necessary personal data

Especially in the B2B sector, with a special focus on BTM, the associated (framework) contracts are concluded with a legal entity. Generally, this is the employer of the traveller, who in each case authorises the traveller internally to use the means of payment issued to the employer to pay for the goods or services used in connection with the business trip.

In the BTM context, personal data of the traveller is necessarily processed during the provision of the means of payment. Such data is primarily used within the employer's travel expense management processes. This represents a legitimate interest in accordance with Article 6 para. 1 lit. f EU-GDPR.

Travel expense management is becoming increasingly complex in many large organisations. In order to comply with the applicable accounting standards, AirPluss client organisations must properly allocate and document all costs and settlements related to a business trip. Each employee is assigned personnel numbers and/or cost centres, which can then also be found on the respective statement. The information is used to facilitate the client organisation's internal cost allocation and expense reporting. In addition, every large company usually has labour law regulations in place (such as travel policies or works agreements), which employees are required to comply with when travelling on business. It goes without saying that the employer is also entitled to monitor compliance with these regulations.

The lodge card (a centralised payment method that companies can use to facilitate company travel purchases) was created precisely for the purpose of covering the exact needs of these corporate customers.

The legal basis for the processing of this data is derived to a sufficient extent from Article 6 para. 1 lit. f EU-GDPR. Against this background, the requirement of consent pursuant to Article 94 para. 2 PSD2 is inconsistent with the EU-GDPR framework, particularly in view of the legal bases in Article 6 para. 1 EU-GDPR (see II. below).

2. With the *explicit consent of the payment service user*

Irrespective of the problem in the context of the German implementation law and the use of the different terms "Einwilligung" and "Zustimmung", however, it can be assumed that originally "consent" means consent that meets the requirements of data protection law, since the English versions of the PSD2 as well as the Directive applicable at the time and the currently applicable EU-GDPR do not differ with regard to the term "consent".

If, on the other hand, one looks at the requirements of Article 6 para.1 lit. a EU-GDPR and the concept of the payment service user, initial doubts arise as to whether the grammatical interpretation of the wording can fully exhaust the scope for interpretation. For the reasons set out below, it is considered that a so-called teleological interpretation, or alternatively a "restrictive interpretation", must lead to the conclusion that there must be other alternatives to explicit consent in order to act lawfully when processing personal data in this context.

a) Grammatical interpretation

The term *payment service user* is legally defined in Article 4 no. 10 PSD2. It is a natural or legal person who makes use of a payment service in the capacity of either payer or payee or both. The payer himself is defined in Article 4 no. 8 PSD2 as 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 authorizes a payment transaction. The fact that the payer, and hence the payment service user, can only mean the company and not, for example, the person for whom the travel is booked, is because it is the payment service user who concludes the relevant contracts (see Article 55 et seq.). The same applies to the payer. For example, if a lodge card is deposited at a travel agency and a payment is initiated from there, this is always done on behalf of the company. However, since consent under data protection law can never be given by a legal entity on behalf of the data subject, consent by the payment service user has no relevance under data protection law in the B2B sector. This only allows the conclusion that Article 94 para. 2 PSD2 is not applicable in the B2B sector.

Furthermore, the interpretation of Article 94 para. 2 PSD2 does not allow the conclusion that a contract with corresponding content must be concluded with the data subject, because the

payment service user is explicitly mentioned here. Even if, contrary to the view taken here, it is assumed that, in the context of a B2B relationship, the data subject entitled to use the payment means, falls within the definition of the payment service user, there is no such requirement.

Article 94 para. 2 PSD2 does not indicate that the processing of personal data during the provision of payment services may only be carried out on the basis of a contract. While recital 71 of the PSD2 states that a contract is necessary for the provision of payment services, it makes no reference to the processing of personal data.

This does not change even if the basic requirements for AISP and PISP in Articles 66 and 67 of the PSD2 are included in the interpretation. Articles 66 and 67 of the PSD2 impose restrictions on the payment service provider as to the lawfulness of the processing of personal data in relation to the provision of its core service, but do not indicate on what legal basis the processing is actually based.

In summary, it does not follow from the overall circumstances of the PSD2, the recitals, or the individual provisions relevant here that the requirement under Article 94 para. 2 PSD2 can be fulfilled exclusively by the conclusion of a contract.

b) Teleological interpretation, alternatively restrictive interpretation

In the B2B sector, i.e. if the underlying contractual relationship is always established between a company and a payment service provider, it thus becomes clear that an explicit consent of the payment service user is futile and therefore cannot correspond to the purpose of the provision of Article 94 para. 2 PSD2.

With regard to the purpose of the provision, the EDPB merely states that the provision is intended to ensure transparency and a certain degree of control of the payment service user.

In principle, the requirements for compliance with the rights of data subjects, in particular the obligation to provide information and transparency, are conclusively regulated in the EU-GDPR. However, Article 94 para. 2 PSD2 contains no reference whatsoever to the transparency requirements in Chapter 3 of the EU-GDPR. If Article 94 para. 2 PSD2 is interpreted in the sense of a requirement for transparency of data processing, in the B2B sector, especially in BTM, then the payment service user is the wrong addressee.

It is also not apparent that in the B2B sector, especially in BTM, from the point of view of the data subject, a higher degree of transparency is required which goes beyond the general requirements of Chapter 3 of the EU-GDPR.

The legislator has not designed the PSD2 for the area of direct use of means of payment (lodge cards, conventional credit cards, virtual credit cards). The following arguments speak in favour of this: the PSD2 creates new rules for third-party services. These are AISPs and PISPs. PISPs allow customers to pay for online purchases immediately by sending online banking access data and a transaction number (TAN) directly to a payment service provider linked to the online merchant. In the case of AISPs, the account-holding payment service provider must provide access to the bank's back-end systems to enable the respective account information service to access accounts and transactions. The services that can be used here are manifold. In this context, personal data from a transaction are also forwarded by the bank to the account information service. For these new payment services, this provision may therefore be appropriate in principle in order to create the transparency necessary from a data protection point of view.

In particular, the legal regulation focuses on the use of the payment service by a consumer. In view of the modus operandi of AISPs and PISPs, "sensitive" personal data will be accessed in the case of consumers and, if necessary, exchanged between the service providers involved. There is a fundamental risk that, e.g. when accessing turnover data of a consumer account or assessing creditworthiness, not only the minimal amount of data required for the provision of the core service will be accessed and processed, but that the data will also be used, for example, to create spending profiles or even forecasts on the future creditworthiness of the consumer. This is precisely where Articles 66, 67 PSD2 come in, limiting data processing in this area to a minimum.

However, if the contractual partner is a legal entity in the B2B sector, this risk does not exist. For one thing, because the contractual partner is not a consumer as well as the fact that data protection in relation to legal entities is only applicable in exceptional cases, if at all. In particular, the spending data accessed consists purely of business expenses, which do not enjoy any special data protection safeguards. The data on travelers that is necessarily processed in a BTM context also relates directly to their work-related activities and not to their private behavior. It should be particularly emphasized that no statement can be made about the financial situation of the data subject, but only about the situation of the contractual partner, a legal entity.

However, this does not change the necessity of data processing, especially with regard to products specifically tailored to the BTM sector. In this case, it is of course the responsibility of the respective controller to provide the necessary transparency, but even in the overall context of PSD2, reducing this requirement to the obligation to conclude a contract with the payment service user makes no sense whatsoever with regard to the rights and freedoms of the data subjects in the BTM environment.

Furthermore, the requirement to obtain consent in the B2B sector seems unnecessary. The discussion surrounding Article 97 PSD2 in conjunction with strong customer authentication

has already shown that there are industries in which the implementation of strong customer authentication a) is not possible without turning all processes between the service provider and the customer upside down, and, b) would not have contributed in the slightest to increased security, one of the primary objectives of strong customer authentication. Following intense discussions, the legislator ultimately understood the arguments of the market side and reacted accordingly. The legislator reacted wisely by allowing for various exemptions from strong customer authentication in specific scenarios, without neglecting the pursued goals of strong customer authentication.

With the additional requirement of a (contractual) consent of the payment service user, we would have a comparable situation: on the one hand, there are simply established payment processes in which a contractual consent is not possible without throwing out all the processes that have been well practiced and established for years. On the other hand, this additional requirement does not enhance the data protection standard:

The lodge card, for example, is a B2B product. The company concludes a payment service framework agreement with a payment service provider. At the beginning of the contractual relationship, the data subjects, whose personal data will be processed, are unkown. The lodge card is usually used either directly in the company or directly in the travel agency. There is therefore no (contractual) relationship between the actual data subject and the payment service provider. In particular, the payment service provider does not even have the necessary information to obtain consent at the beginning of the data processing.

The additional requirement of explicit consent would therefore throw a long-established process out of kilter, unnecessarily complicating processes for the actual customer and would ultimately not provide the data subject with any added value. In practice, a consent requirement would mean that consent would have to be obtained across the board from all potential data subjects (i.e. all employees of a payment service user), even if their data is not processed at all later on. This is unfeasible from a practical perspective and fundamentally contrary to the requirements of data minimization. Accordingly, such personal data processing would lack a legal basis.

As a result, the wording *with the explicit consent of the payment service user* in B2B in the context of the use of a travel center card is not conclusive in itself, since consent to the processing of personal data by nature can only be given by natural persons. Moreover, against the background of the meaning and purpose of Article 94 PSD2, overregulation without added value is best avoided and the provision of Article 94 PSD2 must therefore be interpreted restrictively.

II The conflict resolution rules as criteria for interpretation

From AirPlus' point of view, there are two applicable regulations that can be considered where, during the provision of its payment services, personal data may be processed: on the one hand, there is Article 94 para. 2 PSD2 or the corresponding implementation law and Article 6 EU-GDPR. In this context, the question arises as to the relationship between the regulations.

In terms of timing, the EU-GDPR was adopted after the PSD2. In accordance with the lex posterior principle, the newer provision therefore takes precedence over the older one. This would mean that data protection requirements relating to one and the same matter would be definitively regulated within the EU-GDPR. Therefore, a provision from the PSD2 cannot restrict the catalogue contained in Article 6 para. 1 EU-GDPR. This means that as long as, for example, there is a legitimate interest under Article 6 para. 1 lit. f EU-GDPR, this is a sufficient legal basis to process personal data in the context of the provision of payment services.

It is not apparent that the legislator intended to use Article 94 para. 2 PSD2 to restrict the legal bases available for processing personal data within Article 6 EU-GDPR. Such a restriction must be rejected as being incompatible witht the EU-GDPR and disproportionate.

The list of legal bases for processing personal data in Article 6 EU-GDPR is exhaustive. However, Article 6 EU-GDPR does not provide for a ranking between the individual legal bases. Rather, the legal basis that corresponds to the specific data processing in question is used. Consequently, no provision of the PSD2 indicates that only Article 6 para.1 lit. b EU-GDPR can be considered as the legal basis.

This can be seen from the fact that parts of individual data processing activities may follow different legal bases. This also applies even when the same data sets are involved. It is undisputed that the processing of personal data by payment service providers for the purpose of preventing terrorism and money laundering is governed by Article 6 para. 1 lit. c EU-GDPR.

It is not clear why the PSD2 would allow data processing under Article 6 para. 1 lit. c EU-GDPR, but should prevent the use of consent of the data subject under Article 6 para. 1 lit. a EU-GDPR (as long as it meets the associated requirements).

This does not follow from the restriction of other uses of personal data in Article 66, 67 PSD2. In terms of content, this refers only to the provision of the core service, which is typically provided on a contractual basis or on the basis of a legitimate interest. However, a (different) controller would be free to ask the data subject to disclose the relevant data outside of the provision of the payment service and to base the (new) processing of the data on the consent given. The question of the lawfulness of the processing of personal data cannot therefore depend on the position of the controller as a payment service provider.

This becomes particularly obvious when Article 6 para. 1 lit. b EU-GDPR as a legal basis is typically not available to some payment service providers. As explained above, this is particularly the case in the B2B sector.

AirPlus therefore takes the view that a limitation of the legal bases is not compatible with the EU-GDPR, as the EU-GDPR itself does not provide for such a limitation. Furthermore, it is noticeable that the PSD2 only regulates the use of personal data of the financial payment user. It does not regulate the question of how to deal with the personal data of third parties, such as recipient data in the case of transaction data in the context of AISPs or payees in the case of PISPs. Here, recourse to the EU-GDPR, which allows for a wider range of legal bases, will again be necessary. Since the PSD2 does not cover all (necessary) personal data processing activities, particularly by third parties, the PSD2 cannot be considered as a lex specialis vis-à-vis the EU-GDPR.

We remain at your disposal to provide additional information or for any questions. In this case please contact our expert team:

Stephan Kalhöfer, Lufthansa AirPlus Servicekarten GmbH, Dornhofstr. 10, 63263 Neu-Isenburg, Data Protection Officer
skalhoefer@airplus.com

Katanja Kurth-Grieser, Lufthansa AirPlus Servicekarten GmbH, Dornhofstr. 10, 63263 Neu-Isenburg, Senior Legal Expert
kkurthgrieser@airplus.com