

Information on the data protection requirements for network operations, i.e. acquiring, as well as in other payment services for BS PAYONE merchants

BS PAYONE GmbH (hereafter referred to as BS PAYONE) is a European payment institute approved by the Federal Financial Supervisory Authority (BaFin).¹ As network operator/acquirer for international payment systems (including VISA Europe, MasterCard, American Express), BS PAYONE processes cashless transactions on behalf of merchants that are willing to accept credit/debit cards issued by the payment systems and then completes the payment runs for the connected merchants. Moreover, BS PAYONE offers its customers additional services in connection with payment transactions via its web-based merchant platform (PAYONE Merchant Interface; for short: PMI).

For your information, the following outlines the requirements under data protection laws for the implementation of network operations/acquiring and other services:

A) Network operations/Acquiring

1. It is not necessary to conclude an agreement for contract data processing

There is no need for an agreement for contract data processing according to Article 28 GDPR² for BS PAYONE to provide network operations/acquiring, as the relevant tasks do not fulfil the definition of contract data processing. Under data protection laws, (Article 4 (7) GDPR), BS PAYONE is the controller and therefore independently responsible for data processing in connection with network operations/acquiring.

Merchants do not have a right to issue instructions to BS PAYONE in regard to the necessary processing of cards/transaction data in the payment procedure. The data required for processing of the transaction are collected when the merchant initiates the payment procedure at the terminal and are then transmitted to BS PAYONE in order to complete the payment transaction. BS PAYONE receives the data, performs all necessary processing steps and transmits the payment run data to the relevant payment system for processing of the transaction. The merchant cannot influence this process in any way.

Hence, BS PAYONE ensures fulfilment of the payment transaction and the legality of associated data processing on its own authority. Neither does the merchant have the ability to assess the content of the processing procedure itself, nor can it influence the individual stages of processing.

The processing of cashless transactions is an autonomous, original task of BS PAYONE. The necessary processing of cards/transaction data takes place in the interests and for the purposes of BS PAYONE. It does not constitute data processing on

¹ Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht)

² EU General Data Protection Regulation. Upon introduction of the GDPR on 25 May 2018, the corresponding provisions of the Federal Data Protection Act (old; BDSG) will no longer apply.

behalf of the connected merchant, as the entire underlying task is assigned to BS PAYONE for completion on its own authority. It is not an “auxiliary function” on behalf of the merchant.

From a perspective of data protection laws, network operations/acquiring constitutes the engaging of external technical services from an independent controller, for which, in order to perform processing (previously: “transfer of functions”), there must be a legal basis in³ Article 6 GDPR⁴.

2. It is not necessary to conclude a “transfer of function” contract

In addition, there is no need to conclude a “transfer of function contract” in regard to the services provided by BS PAYONE. The GDPR does not contain the construct of “transfer of function” and hence does not specify a transfer of function contract. Moreover, a contract of this kind is not necessary, as the network operations/acquiring contract with the merchant, in conjunction with the relevant statutory provisions on data protection, already provide for the nature, scope and purpose of permissible data processing by BS PAYONE to a sufficient extent.

3. It is not necessary to conclude an agreement as joint controllers

There is also no case of joint control as set out in Article 26 GDPR as a new legal institution that requires a separate agreement between the parties. Joint control is predicated upon several data processing controllers deciding together on the purpose and means of processing. In turn, a “joint decision” on the purpose and means of processing assumes that each party exerts a certain influence on the data processing.⁵ As described earlier, the merchant has no way of influencing the transaction payment run. The fulfilment of payment transactions is an autonomous area of responsibility over which the merchant has no influence whatsoever, and which is under the exclusive control and responsibility of BS PAYONE as the payment institute. Hence, it is not necessary to conclude an agreement according to Article 26 (1) GDPR.⁶

4. Data processing on the basis of a legal foundation

The processing by BS PAYONE of card/transaction data needed to fulfil cashless payment transactions takes place based on a legal foundation and is hence permissible under data protection rules.

³ Refer to: Short Paper no. 13 by DSK (Data Protection Conference) on contract data processing, Article 28 GDPR, Appendix B.

⁴ The construct of “transfer of function” is not included in the GDPR and will no longer be used in future. The applicable principle – without legal distinction – is data transmission to an independent controller; refer to Short Paper no. 13 by DSK, page 1 and Appendix B.

⁵ Refer to: Short Paper no. 16 by DSK (Data Protection Conference) on joint processing controllers, Article 26 GDPR, page 2.

⁶ Therefore also: Short Paper no. 13 by DSK (Data Protection Conference), Appendix B (in a comparison with ppendix C).

Where information relating to the merchant is processed by BS PAYONE for transaction fulfilment, it is justified by Article (6)(1)(1)(b) GDPR for the fulfilment of the network operations/acquiring contract with the merchant. Where data belonging to the paying card holder (in particular bank details or credit card number) are processed, the legal foundation is also provided for in Article 6 (1)(1)(b) GDPR. Data processing in regard to payments is necessary in order to fulfil the purchase agreement between the merchant and the card holder and is hence justified by the need to execute the contract.

It is therefore not necessary under data protection laws to conclude contracts other than the network operations/acquiring contract.

B) Other services

BS PAYONE offers its contractual partners (connected merchants) the following additional services via the web-based merchant platform (PMI):

- Payment (processing of payment transactions in e-commerce)
- Risk management (fraud prevention and creditworthiness checks)
- Invoicing (generation and dispatch of invoices)
- Claims management (dunning and transmission to collection agencies as necessary)
- Subscription processing (management of recurring payment processes)
- Aggregated micropayments (aggregation of claims for processing in one payment transaction)

It is therefore not necessary under data protection laws, in order to provide the services outlined above, to conclude contracts other than the main/services contracts for the respective services.

Again, the services cannot be legally classified as contract data processing in accordance with Article 28 GDPR, as BS PAYONE is not continuously required to observe instructions from merchants, as would be necessary for this legal provision to apply. Moreover, there is no joint control according to Article 26 GDPR, as the merchant does not have any dominant influence on the purpose and means of data processing in these other services.

Although the requirements for joint control may be satisfied when individual parties are separately responsible for certain areas or phases of data processing, this is predicated on the collection of data on a shared platform.⁷ In this case, however, the merchant platform (PMI) does not constitute a “shared platform”, as the merchant is unable to exert a dominant influence on operation of the platform.⁸ Merchants merely have restricted operative and access rights on the PMI. Hence, like fulfilment of the services for payment transactions, operation of the platform is the sole responsibility of BS PAYONE and is subject to its

⁷ Refer to: Short Paper no. 16 by DSK, page 3.

⁸ Insofar as a dominant influence on the operation of the platform (here: PMI) might exist, joint control would still be restricted to the operation of the platform and would not automatically encompass the services provided via the platform, loc. cit.

exclusive control. A legal or factual influence by the merchant on the purposes and means of data processing does not apply in either case.

Data processing is either necessary in order to execute the contract with the merchant and can hence be based on Art. 6 (1)(1)(b) GDPR, or it takes place to accommodate the justified interests of BS PAYONE, Article 6 (1)(1)(f) GDPR.