



## Comment on the EDPB's Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions

Data Protection Association as the biggest privacy professional organisation in the Czech Republic welcomes European Data Protection Board's recommendation 2/2021. The importance and number of online payments has significantly raised since beginning of the COVID-19 pandemic. At the same time, the importance of data protection aspects of online shopping and online payments raised too.

Our Association would like to highlight a few points connected to the recommendations and ask the EDPB for their clarification.

### 1. Recommendations publication without public discussion

Our Association is fully aware that it is not the EDPB's obligation to provide public consultation to all methodological documents. On the other hand, we really appreciate current EDPB's practise consisting in the public consultation of most published documents, mainly guidelines. Commented recommendations affect a big number of data controllers and data subjects and the whole e-commerce sector.

In practice, the processes associated with online payments can be much more complex. Big part of the online payments is processed via the payment gateways provided by third parties or could be done by the payment button provided by other categories of financial institutions. Both payment gateways and the payment button providers are regulated financial institutions and independent data controllers in most cases. A standard public consultation would perhaps also help to clarify these related issues.

**We would appreciate if documents with similar importance will be published to public comments in the future.**

### 2. Scope of the recommendations

The recommendations aim is defined as “harmonised application of data protection rules regarding the processing of credit card data within the European Economic Area (EEA)”. According to statistics,

only about one half of card payments in the EU is done by credit cards, the other half is executed by debit cards.<sup>1</sup>

Despite the different financial services behind the two kinds of cards (credit card is connected with a loan, for debit card payments client's own money is used), we see very similar data protection risks connected with processing of both credit and debit card data.

**Our Association would welcome clarification why the scope of the recommendations is limited only to credit card payments and data and what are the major differences in comparison with debit card data.**

### 3. Legal basis for the processing of card data

We fully agree that a different legal regime (legal basis) could be applicable for long-term relationship with e-commerce provider or another merchant. The legal basis of contract performance could be used for the recurring payments for long-term services.<sup>2</sup>

On the other hand, we would like to extend the possibility to apply the legal basis of the performance of a contract [art. 6(1)(b) of GDPR] for card data storage by an online store under other circumstances too. A particular store could for example offer to its clients the possibility to store the card data for future payments as part of additional services going beyond the pure purchase of goods or services. Such services, e.g., in the form of a customer loyalty club, are rather based on a contract between an e-commerce provider and the customer than on a consent and the related personal data processing is carried out on the basis of the performance of the contract. Another important aspect we would like to highlight is that payment card information is neither special category of data nor more sensitive data in general meaning. It is not possible to know or derive information about customers financial situation just from the payment card data.

**Our Association would welcome if the possible use of the performance of a contract as the legal basis for the processing of card data could be discussed in this context as it is common market practise not lowering level of customer's data protection given all requirements are followed, particularly the transparency principle.**

**Prague, 28 June 2021**

**Vladan Rámiš**, Chairman of the Committee

**František Nonnemann**, Member of the Committee

**Jakub Hruška**, Member of the Financial Sector Working Group

---

<sup>1</sup> <https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2019~71119b94d1.en.html>

<sup>2</sup> Par. 4 of the recommendations, respectively footnote no. 2. In practice, there are also other forms of data processing in this context, for example online shops could store only parts of the card numbers to be able to resolve complaints. Although the scope of the Recommendation is limited to storage for the purpose of facilitating further payments, it could be helpful to explicitly mention that such processing is not affected by this Recommendation.