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

Adopted on 19 May 2021

The European Data Protection Board

Having regard to Article 70(1)(e) of the 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,

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

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS:

1. In the context of the COVID-19 pandemic the digital economy and e-commerce continuously developed. Analogously the risks of using credit card data online has increased. As stated by the Article 29 Working Party in its guidelines on Data Protection Impact Assessments, credit card data violations "*clearly involves serious impacts in the data subject's daily life*", as financial data can be used for "*payment fraud*"[1].

2. Therefore, it is very important that controllers put in place the appropriate safeguards for the data subjects, and to ensure them the control over their personal data, in order to decrease the risk of unlawful processing and foster trust in the digital environment. The EDPB deems this trust vital for sustainable growth of the digital economy.

3. For this purpose, these recommendations aim to encourage a harmonised application of data protection rules regarding the processing of credit card data within the European Economic Area (EEA), and to guarantee a homogeneous protection of data subject's rights, in full respect of the fundamental data protection principles as required by the GDPR.

4. More specifically, these recommendations deal with the storing of credit card data by online providers of goods and services, for the sole and specific purpose of facilitating further purchases by data subjects[2]. They cover the situation where a data subject buys product or pays for a service via a website or an application, and provides his/her credit card data, generally on a dedicated form, in order to conclude this unique transaction.

5. As with any processing, the controller must have a valid legal basis under Art 6 GDPR to store those data. In this regard, it should be noted that a number of the legal bases mentioned in Article 6 GDPR would not be applicable to this situation and have to be excluded. The storage of credit card data following a transaction, in order to facilitate further purchases, cannot be considered necessary for compliance with a legal obligation (Art. 6(1)(c) GDPR) nor to protect the vital interest

[1] ARTICLE 29 DATA PROTECTION 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.

[2] It should be noted that they do not cover payment institutions operating in online stores, nor public authorities. Neither the storage of credit card data for any other purpose, for instance for compliance with a legal obligation, or to establish a recurring payment in cases of contract of continuing performance or subscription for a long-term service (e.g. a contract which stipulates the supply of a certain good every month, or the subscription for a music or movie streaming service).

of a natural person (Art. 6(1)(d) GDPR). The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(e) GDPR) cannot be considered as an adequate legal basis either.

6. In addition, the storage of the credit card data after the payment for goods or services is not, as such, necessary for the performance of a contract (Art. 6(1)(b) GDPR). Whereas, in the first place, the processing of the data related to the credit card used by the client to pay is necessary to fulfil the contract, thereby triggering Article 6 (1)(b) GDPR, the storage of these data is only useful in order to facilitate the potential next transaction and facilitate the sales. Such purpose cannot be considered as strictly necessary for the performance of the contract for the provision of the good or service that the data subject has already paid[3].

7. When it comes to a processing necessary for the purposes of the legitimate interest of the controller or a third party[4], the EDPB notes that for the controller to be able to rely on Article 6(1)(f) GDPR, the three conditions laid down by this article must be satisfied[5]. This legal basis requires, first, the identification and qualification of a legitimate interest pursued by the controller or by a third party. The interest of the controller or third party may be broader than the purpose of the processing and must be present and effective at the date of the data processing[6].

8. The legitimate interest legal basis requires, second, the need to process personal data for the purposes of the legitimate interest pursued. For what regards this last condition, provided that the controller has a legitimate interest as outlined above, it is not evident that the storage of the credit card data to facilitate future purchases is necessary to pursue that legitimate interest. Indeed, the actual conclusion of another purchase depends on the consumer choice and is not determined by the possibility to realize it "in one click".

9. Finally, the third condition requires the performance of a balancing test: the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject, including data subject rights to data protection and privacy. The balancing test requires taking into consideration the particular circumstances of the processing[7]. An essential component of the balancing exercise is the potential impact on the data subject's rights and freedoms resulting from the processing[8]. Such impact can depend on the nature of data, specific method of processing and access to such data by third parties. Regarding the nature of

[3] See as well 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 subject, in particular on page 10.
[4] See Article 29 Working Party Opinion on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, currently under revision by the EDPB (see the EDPB Work program 2021/2022 adopted on the 16 March 2021).
[5] See CJEU judgement of 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme', Case C-13/16, ECLI:EU:C:2017:336, point 28.
[6] See CJEU judgement of 11 December 2019, TK v Asociaţia de Proprietari bloc M5A-ScaraA, Case C-708/18, ECLI:EU:C:2019:1064, point 44.
[7] See CJEU judgement of 24 November 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, points 47 and 48; CJEU judgement of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779, point 62.
[8] See CJEU judgement of 24 November 2011 abovementioned, point 44; CJEU judgement of 11 December 2019 abovementioned, point 56.

data criterion, it should be noted that financial data have been qualified by the Article 29 Working Party as data of a highly personal nature because their violation clearly involves serious impacts in on the data subject's daily life[9]. Hence, notwithstanding the controller's obligation to implement technical and organisational measures to ensure appropriate security of the credit card data pursuant to Article 5(1)(f) GDPR and the fact that those data may be stored for other purposes, their processing to facilitate further purchases may involve an increasing risk of credit card data security breaches as it implies processing in other systems. Another important element of the balancing test that could be taken into consideration to assess the impact of the processing on data subjects' is the reasonable expectations of data subjects based on their relationship with the data controller, the context and the purpose of personal data collection[10]. Yet, it appears that at the time of purchase, while providing credit card data for the payment, the data subject does not reasonably expect his or her credit card data to be stored for longer than what is necessary to pay the goods or services he/she is buying. Consequently, the fundamental rights and freedoms of the person concerned by the data protection would likely take precedence over the controller's interest in this specific context.

10. Those aspects lead to conclude that consent (Art. 6(1)(a) GPDR) appears to be the sole appropriate legal basis for the above-described processing to be lawful. Indeed, to address the security risks, to allow the data subject to keep control over his/her data, and to decide actively of the use of his/her credit data, the specific consent of the data subject should be obtained before storing his or her credit card data after a purchase. This consent will enable the controller to demonstrate the individual's willingness to facilitate his/her further purchases through the specific website or application, which cannot be presumed by the simple fact he/she concluded one, or several, isolated transactions.

11. This consent cannot be presumed, it must be free, specific, informed and unambiguous[11]. It must be delivered by a clear affirmative action, and should be requested in a user-friendly way, such as through a checkbox, which should not be pre-ticked[12], directly on the form used for the data collection. This specific consent must be distinguished from the consent given for terms of service or of sales and not be a condition to the completion of the transaction.

12. According to the Article 7(3) GDPR, the data subject shall have the right to withdraw his or her consent for the storing of credit card data for the purposes of facilitating further purchases at any time. The withdrawal must be free, simple and as easy for the data subject, as it was to give consent. It must lead to the effective deletion by the controller of credit card data stored for the sole purpose of facilitating further transactions.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[9] ARTICLE 29 DATA PROTECTION 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.
[10] See recital 47 GDPR.
[11] See EDPB Guidelines 05/2020 on consent under Regulation 2016/679.
[12] *Ibid*.