COMMENTS ON THE GUIDELINES 06/2020 ON THE INTERPLAY OF THE SECOND PAYMENT SERVICES DIRECTIVE AND THE GDPR

Response to the European Data Protection Board's Public Consultation

16 September, 2020

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Finanzmarkt

Rudi-Dutschke-Straße 17
10969 Berlin

finanzen@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

CONTENT

I. GENERAL

The Federation of German Consumer Organisations – Verbraucherzentrale Bundesverband (vzbv) welcomes that the European Data Protection Board (EDPB) has agreed upon guidelines to clarify the interplay between the General Data Protection Regulation (GDPR) and the Second Payment Services Directive (PSD2). A thorough and consistent application of data protection law is a prerequisite for trustworthy digital financial services that can benefit consumers. While the objective of increased competition between banks as well as between banks and tech companies can improve consumer welfare, it will not do so if consumers lose control over their personal data and suffer the consequences of illegitimate data processing, like fraud, ubiquitous profiling and discrimination. Against this background, vzbv appreciates the opportunity to give a response to this consultation.

II. LAWFUL GROUNDS

First of all, vzbv welcomes that the guidelines clarify that the “main legal basis for the processing of personal data for the provision of payments data is Article 6 (1) (b) of the GDPR” (14) and “that controllers have to assess what processing of personal data is objectively necessary to perform the contract” (15). Whenever third party providers (TPPs) want to go beyond what is absolutely necessary, data subjects need to express their (explicit) consent. These provisions are important to consumers because they limit the uncontrolled processing of personal data.

Paragraph 18 states that there must not be bundling of services and that data subjects must not be confronted with “take it or leave it” situations. This is important as it protects consumers’ freedom of choice.

In practice, applications will often combine several services. The guidelines rightly demand that “the applicability of Article 6 (1) (b) should be assessed in the context of each of those services separately.” However, it is likely that in the practical application there will be conflicts over what constitutes the core service and what goes on top and whether a certain service can be performed without the other.

- It might be helpful if EDPB provided some examples to clarify what constitutes “objectively necessary […] processing of the personal payment account data” to prevent conflicting interpretations.

For example: A credit broker that uses an Account Information Service Provider (AISP) as an aggregator to collect payment account data which is forwarded to banks to calculate credit offerings: What processing of personal data is objectively necessary to perform the contract and by whom? Do banks need to process more than regular income, rent and other fixed expenses? Does the credit broker need to process any of these personal data to objectively perform the contract?

vzbv also welcomes the clarification that, in general, the processing for another purpose is not allowed, unless the data subject has given consent pursuant to the GDPR (paragraph 22 of the guidelines).

III. EXPLICIT CONSENT

vzbv supports the view that explicit consent of the PSD2 is not identical with explicit consent of the GDPR, but has to be regarded as an “additional requirement of a contractual nature” (35) and that it should “be understood in coherence with the applicable data protection legal framework” (38).

IV. SILENT PARTY DATA

If a consumer makes payments to a recipient and uses a payment service, the recipient’s data will be processed as silent party data. vzbv welcomes that the guidelines set strict limits to silent party processing. However, the guidelines currently leave room for interpretation concerning the consequences of silent party processing of special categories of data where explicit consent is a prerequisite for data processing but is not feasible for technical reasons. Again, examples might be helpful.

V. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The guidelines rightly acknowledge that “the chances are considerable that service provider processing information on financial transactions of data subject also processes special categories of data.” (51) While examples for special categories of data, like political opinions and religious beliefs, are provided, there is still room for interpretation. This could constitute an easy target for controllers who want to avoid article 9 provisions. In addition, the guidelines do not clearly distinguish between the data itself and the processing of data.

- The guidelines should provide more examples for what constitutes special categories of data as well as what constitutes processing of that data.
- The guidelines acknowledge that controllers that process payment data always risk processing special categories of data. This begs the question: Shouldn’t controllers always act as if they were processing special categories of data?

Payments services may be of substantial public interest (55). Consumers and business rely on efficient and reliable payments processing. However, substantial public interest (Article 9 (2) j)) does not extend to the provision of AISPs and should hence not be confused.

- The guidelines should clarify that substantial public interest might cover payments services in a narrow sense, yet does not extend to services that may or may not be of value but are clearly not vital to the economy.

Building on this premise, vzbv welcomes the provision that controllers need to obtain explicit consent to process special categories of personal data. (56)

VI. DATA MINIMIZATION, SECURITY, TRANSPARENCY, ACCOUNTABILITY AND PROFILING

vzbv welcomes the strong commitment to data minimization and that "[a]s a principle, the access to the personal data should be limited to what is necessary for the provision of payment services" (61). This condemns current practices, where consumer data is broadly collected and measures to minimize data collection are just not existent.

(64) Currently, TPPs have broad access to consumers' payments account data. Depending on the application interface, controllers have access to PSD2-data categories only or to the full banking account (including services that go beyond checking accounts, like credit cards, consumer credit, investment portfolios). vzbv welcomes that the guidelines clarify that these practices are not in line with GDPR.

(63) The provision of filters will ensure that consumers no longer need to trust blindly that controllers will, while having access to them, actually ignore irrelevant data but only process data that is necessary for the provided service.

(66) Aggregators with PSD2-licenses offer their services to providers that need access to consumer data but lack the necessary licenses to access bank accounts. If a controller systematically transmits data to unregulated third parties, this raises the question of how data protection is ensured. In particular, how can data minimization be safeguarded at all?

- The guidelines should point out the requirements for aggregators and clarify what constitutes a legal mode of operation.

For example, this would include how data protection by design and default would have to be implemented. Additionally, the guidelines should clarify aggregators' obligations towards unregulated third parties: How do aggregators safeguard that personal data (which potentially constitutes Article 9-data) is handled appropriately by unregulated third parties? Again, the example of a credit broker who uses an aggregator to channel payment data to banks could serve as an illustration.

Privacy dashboards are important tools to provide consumers with control over their data. These tools should not only provide an overview but also "the possibility to withdraw a specific explicit PSD2 consent" (77). While support for privacy dashboards is good, the wording of this paragraph might be too soft. It is likely, that data protection authorities face conflicts with financial supervisors and TPPs who argue that interventions of banks in the management of consent are – as a matter of principle – obstacles to competition as laid out in the Regulatory Technical Standards (RTS).

- The guidelines should further elaborate on the tension between "competition" as interpreted by RTS and data protection.

For example, there could be a clarification that privacy dashboards should not be deemed obstacles to the TPPs' right to provide services in accordance with PSD2 as a matter of principle but rather that TPPs need to demonstrate that the specific design of a privacy dashboard constitutes an obstacle to their rights.

VII. CONCLUSION AND OUTLOOK

vzbv welcomes the scope, ambition and rigor of the guidelines. Looking ahead, it is important that the rules laid out are enforced. Data protection is vital as it constitutes the basis for digital finance that serves consumers' needs and interests. Since TPPs are regulated by financial supervisors there needs to be close cooperation between data protection authorities and financial supervisors. Supervisors should investigate TPPs' data processing from within.