Security, Privacy, Identity, Trust, Engagement, NetworkPlus

Comments on the European Data Protection Board's

Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

Submitted by SPRITE+ Future Payment Systems Working Group

Dr Geoffrey Goodell (UCL), Dr Andrea Bracciali (University of Stirling), Dr Jiahong Chen (University of Nottingham), Dr Duncan Greaves (CU Scarborough), Dr Chris Hicks (Alan Turing Institute), Dr Yang Lu (University of Kent), Dr Okechukwu Okorie (University of Exeter) and Dr Robin Renwick (Trilateral Research)

16 September 2020

1. SPRITE+[1] is a UK EPSRC NetworkPlus led by a consortium of University of Manchester (lead institution), Imperial College London, Lancaster University, Queen's University Belfast, and University of Southampton, bringing together people involved in research, practice, and policy relevant with a focus on digital contexts. In response to the current global health crisis, the Future Payment Systems Working Group,[2] with researchers from institutions across the UK, has launched an interdisciplinary project with the aim to investigate the features and impacts of future digital payment systems with respect to trust, identity, privacy and security, contributing to the identification of policies, architectures and specific technologies that best serve the public interest.

Introduction

2. We welcome the EDPB's adoption of Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, and appreciate the opportunity to comment on the current version, especially at a time when digital payment mechanisms have become an increasingly important part of people's lives.

3. The Guidelines have highlighted the key data protection aspects of the Second Payment Services Directive (PSD2) and its interactions with the GDPR. We share the EDPB's observation that 'the application of the PSD2 raises certain questions and concerns in respect of the need that the data subjects remain in full control of their personal data', and the view that further clarification by the EDPB is needed. While we agree with the general scope as well as the vast majority of the analyses in the Guidelines, there are a number of points we would like to raise, with a view to contributing to the preparation of the final version of the Guidelines.

[1] https://spritehub.org/
[2] https://spritehub.org/2020/08/20/future-payment-systems-data-technology-and-privacy-after-covid/

Further processing for contact tracing purposes

4. The Guidelines have correctly pointed out that Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) may, under certain circumstances, be obliged by EU or national laws, notably anti-money laundering (AML) legislation, to share information, including personal data, with public authorities. We feel it is important to consider the possibility of personal data of a commercial or sensitive nature being repurposed for achieving policy goals.
5. At these times of a global pandemic we are aware that, in some countries, transaction data have already been used for contact tracing.[3] While the EDPB has published several guidelines and statements on using personal data in the context of the COVID-19 outbreak[4] and has consistently maintained that strong data protection standards are crucial, even in a global health crisis, these documents have not touched on issues arising from the potential use of transaction data in this context. We believe strong data protection standards for the specific case of payment data held by payment services and their potential use in the context of public health is worth reiteration in the final version of the Guidelines.

Lawful ground for silent party data processing

6. In section 4, the Guidelines have analysed the legal basis for processing personal data of the silent party of a transaction, which seems to suggest that Article 6(1)(f) GDPR ('legitimate interests') is the most appropriate – if not the only practical – lawful ground for the primary processing of such data. Although we see the scope for an argument of the legitimate interest of the data controller in some cases, the balancing test involved in this provision operates on a case-by-case basis, which may create grave legal uncertainties among service providers and consumers alike. This is particularly problematic when determining the 'reasonable expectations' of the data subjects may be seen as somewhat arbitrary. We welcome some clarity on this matter, noting that the processing of data related to a silent party can result in harm to that party and that the mechanisms involved in that data processing can be opaque.
7. We therefore urge the EDPB to elaborate on the possibility of relying on a legal obligation set out by law (Article 6(1)(c) GDPR) as the legitimising basis, and where appropriate, encourage Member States to identify the specific rules and safeguards that would enable that possibility. Articles 48, 49, 57, 58, 66 and 67 of the PSD2, for example, have clearly envisaged the scenarios where processing of the data concerning the silent payee is needed for the completion of the transaction, and have also specified the sole purpose of such processing. Once transposed into Member State laws, these provisions may provide a more predictable legal basis for uses of silent party data. This approach also comes with the benefits of harmonising the safeguarding measures across the industry, as well as providing extra, statutory protections that are typically unavailable to data subjects where the lawful ground is legitimate interest (e.g. right to erasure and right to data portability).

---

[3] https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html; https://www.nature.com/articles/d41586-020-00740-y

[4] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en; https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en; https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-concerning-european-commissions-draft-guidance-apps_en; https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/statement-processing-personal-data-context-reopening-borders_en

Voluntariness of explicit consent under PSD2

8. The Guidelines have also conducted a detailed examination of the concept of 'explicit consent' under the PSD2 and the GDPR. While, in principle, we agree with the EDPB's interpretative approach and the conclusion that the 'explicit consent' requirements are not identical in the two legal frameworks, there is a need for further clarification on the 'freely given' nature of this mechanism. Under the GDPR, 'consent' and 'contract' are considered two separate legitimate grounds, with the former being able to be unconditionally and unilaterally withdrawn by the data subject at any time, whereas the latter usually subject to consensual termination unless provided by the terms otherwise. It is unclear how this distinction plays out under the PSD2 when the Guidelines state that '"[e]xplicit consent" referred to in Article 94 (2) PSD2 is a contractual consent'. The GDPR has set out a rather strict test of voluntariness with additional conditions such as granularity and unbundling. The extent to which these elements also apply to the notion of explicit consent under the PSD2 is unclear, requiring further guidance by both data protection and financial regulators. Clarification on the voluntariness of explicit consent is particularly relevant as this aspect is being affected by the fact that more and more transactions have moved online and that digital payments have become more of a requirement than an option in everyday life.

Transparency and understandability

9. The Guidelines have outlined how 'Article 5 (1) (b) of the GDPR provides for the purpose limitation principle, which requires that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.' We welcome this acknowledgment, but feel it is necessary to clarify the importance of understandability and transparency in any communication between AISPs and data subjects. For example, catch-all terms such as 'personal finance advisory services' or 'personal financial planning' may provide the lawful basis for analysis and profiling to a depth that the data subject may not fully be aware, nor understand. We urge the EDPB to clarify in greater detail that for specific cases, separate and explicit consent may be required from the data subject, including their acknowledgment that they understand the nature and scope of the data analysis conducted by the AISPs and their deployed tools – especially in the case of AI/ML powered tools for data analytics. Additionally, given that data subjects generally cannot know with certainty how data are used once collected, we urge the EDPB to clarify the rights of data subjects to demand that data that are not needed for the aforementioned specified, explicit, and legitimate purposes are not collected in the first instance.

The role of AML regulatory frameworks

10. The Guidelines have rightly acknowledged the nuanced interplay of existing and evolving AML obligations that should be viewed alongside GDPR and PSD2. We feel it is important to provide more gravitas to this evolving interrelation, especially as it relates to harmonisation bodies such as the Financial Action Task Force (FATF), who provide guidance and recommendations to specific jurisdictional bodies. As recent publications from the FATF have touched on aspects of identity and privacy, we feel it is important to consider how this may impact on evolutions of GDPR in the future. While we agree that the potential emerging interactions are out of direct scope of this particular set of Guidelines, we feel that it would be useful to point to potential risks regarding the ongoing interplay of regulatory frameworks. We have seen similar contentious issues emerge in the past, such as those outlined in prior communications from the Article 29 Working Party regarding the processing of

personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[5] Moving forward, we call for the EDPB to consider issuing further opinions on how this conversation may be impacted by such initiatives as:

i) the impact assessment due from the Commission's Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing[6];
ii) the *Schrems II* decision, especially issues surrounding EU-US data transfers for payment services;
iii) the transfer of data to third-countries, and standard contractual clauses (SCCs).

11. We feel these three topics factor strongly into conversations and opinions regarding the cross-jurisdictional sharing of personal data.

Sensitive data and data protection

12. The Guidelines have noted the delicate nature of 'sensitive personal data' being shared across controllers and processors, and concluded that a DPIA should be conducted if specific data sharing of this nature is taking place. We feel that a more substantial opinion should be provided on this matter, especially given the potential harms that might befall the data subject if such sensitive data was being shared amongst PISPs and AISPs. Currently it would seem the financial system does not account for specific encryption or technical measures that could be applied to payments or meta-data associated with payments (whether classified as personal or not). However, within the private sector suitable techniques and protocols that support robust and verifiable data protection are available, such as account pseudonymisation, privacy-preserving methods to protect amounts, and robust cryptographic techniques to ensure separation of specific data elements. We also feel it worth noting at this time that some PISPs are using specific payment mechanisms in the private sector that may pose a high degree of risk to the data subject. These payment mechanisms are often associated with 'publicly viewable ledgers', and do not necessarily contain the adequate technical measures for data protection as may be required for such data processing.

Conclusion

13. Overall, the EDPB's adoption of the Guidelines represents a helpful step forward in tackling the complex data protection issues in the digital payment sector. As much as we agree with most of the analyses of the Guidelines, we also call for the EDPB to provide further elaboration on certain points as highlighted above, not least with regard to the impact of the COVID-19 pandemic, and the emerging interrelated regulatory frameworks, and the private sector solutions that are being offered to the market regarding value transfer.

14. We would be happy to be contacted for further discussion, and for our comments to be published in full.

[5] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf; https://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2006/pr_swift_affair_23_11_06_en.pdf
[6] https://ec.europa.eu/finance/docs/law/200507-anti-money-laundering-terrorism-financing-action-plan_en.pdf