DIGITALEUROPE

16 SEPTEMBER

DIGITALEUROPE response to the European Data Protection Board's consultation on the Guidelines 6/2020 on the interplay of the PSD2 and the GDPR

Executive Summary

DIGITALEUROPE welcomes the European Data Protection Board (EDPB) draft guidelines on the Interplay of the Second Payment Services Directive (PSD2) and the GDPR and the opportunity to respond to this consultation.

The PSD2 encourages the creation of innovative and competitive services, such as open banking, that enable broader access to payment services and boost financial inclusion. We fully endorse the EDPB's emphasis on accountability and the need to embed privacy safeguards into the design of all payment services, products and technologies. At the same time, we also encourage a more pragmatic approach to interpreting the PSD2 to ensure its aims and potential are fully exploited.

In particular, we encourage the EDPB to:

- revisit its approach to further data processing in the context of open Banking and clarify that legitimate interest is not excluded by default as a legal basis as long as necessary legal requirements are met. A restrictive interpretation of the notion of legitimate interest will exclude processing operations that are legitimately expected by the consumers, such as fraud detection and prevention as well as product development and improvement. It will ultimately undermine innovation in payment services.
- provide a more nuanced approach to the processing of silent party data. The guidelines should allow data controllers to make their own independent assessment of the relevant legal basis, as well as consideration to balance data subjects' fundamental rights and freedoms with their own or third parties' interest. It is the responsibility of data controllers to define if and what appropriate risk mitigation measures are needed.
- clarify in the guidelines that it is the responsibility of each data controller to undertake its own assessment and determine the scope of data minimisation in relation to the intended purposes and the risks involved. This is without prejudice to our support to the EDPB's emphasis on

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

privacy-enhancing measures necessary to ensure data processing complies with legal requirements.

Table of Contents

General comments

The PSD2, recently implemented, has set a new legal framework for payment services and data sharing ecosystems. It has encouraged the creation of innovative services for consumers, broadening access to payment services and enabling financial inclusion. It has also stimulated competition, by making payment services more available to consumers.

It supports, too, the ambition of developing new business models that rely on access to data and data sharing, a key pillar for innovation in Europe and beyond.

DIGITALEUROPE welcomes the EDPB's draft guidelines as they aim to clarify a complex legal environment. We acknowledge there is a need to set fair, ethical, accountable and legally compliant conditions for the further development of this market. We fully endorse the EDPB's emphasis on accountability and the need to embed privacy safeguards into the design of all payment services, products and technologies, and ensure the highest standards for security, transparency, data minimisation and accountability.

However, as the EU aims to stimulate open data sharing, we are concerned that a restrictive approach to processing in the PSD2 will impact how stakeholders are using data to innovate. Overregulating this space or imposing onerous requirements might ultimately undermine the spirit and the intention of this Directive. There is a need for a pragmatic approach that preserves its original goals.

Further processing

In the draft guidelines, the EDPB takes a restrictive approach to interpret what is necessary for the contract in the context of account information and payment initiation services. The EDPB is also restrictive in excluding any further processing of personal data beyond the contract if the processing is not based on consent or legal obligation.

The EDPB excludes legitimate interest as a legal basis for such further processing, even if the consumer had reasonable expectations that such further processing would take place. This interpretation means that **data processing activities based on legitimate interest would not be possible.** The consequences would be far-reaching. They would impact, for example:

- **Fraud detection and prevention:** most, if not all consumers, have a reasonable expectation that the services they are seeking are secure, and that all the payment service providers involved take the necessary measures to monitor, prevent and eradicate fraud.

  Requiring consent in the context of fraud is not feasible, nor practical nor reliable. The security and stability of the payment systems cannot depend on individuals' consent. In addition, such consent would not be practically feasible in the absence of direct consumer relationships, as may be the case for stakeholders other than Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

  Article 94(1) of the PSD2 includes a direct mandate to permit processing of personal data when this is necessary to safeguard the prevention, investigation and detection of payment fraud. **We would welcome if the EDPB clarified whether Article 94(1) of the PSD2 constitutes a sufficient legal basis for further processing for the purpose of fraud prevention in payment services.**

- **Service development and improvement, data analysis:** the EDPB's restrictive approach to processing undermines the essence of the open banking services in the PSD2. As these services are built on innovative solutions, there needs to be room for legitimate data uses that boost innovation and create new services or functionalities transparently communicated to Payment Service Users (PSUs), in accordance with their reasonable expectations and market trends.

  For instance, open banking presents unique opportunities to enable financial inclusion to consumers that have so far had no or limited access to banking services. By enabling data sharing, consumers can build a legitimate financial profile and transaction history. Consumers that would likely be rejected for loan services have a chance to use service providers that understand their risk profile when considering loan applications. These consumers may also have better opportunities to use efficient loan repayment possibilities that suit their needs.

  Data analysis is key to understand market needs and trends to boost financial inclusion. It is crucial to make these opportunities available to all segments of society. Consent will not always be feasible in pursuing financial inclusion goals. De facto prohibiting further use of data will effectively undermine the potential to develop these services and the goals of the PSD2.

- **Data aggregation and anonymisation:** open banking can help improve credit scoring algorithms by enabling the aggregation of transaction histories from various banks and encouraging innovation in this area. Prohibiting further data use for legitimate interest would significantly reduce the possibility to aggregate and anonymise data. Data aggregation and anonymisation are used in payments as measures to achieve data minimisation, a principle the EDPB emphasises in the guidelines. In most cases, these measures rely on legitimate interest as a legal basis. Severely restricting their use would thus be inconsistent with the overall spirit of the EDPB guidelines.

As a rule, under the GDPR a data controller may process personal data for multiple purposes in the context of a relationship or service. These purposes may rely on various legal grounds as long as they meet the relevant requirements, such as transparency obligations or the need to perform a ‘’balancing test’’ when legitimate interest is used as the legal basis.[1]

The EDPB Guidelines 2/2019 on the processing of personal data under contractual necessity support this view. They state that where some services cannot be justified by contractual necessity, they may still be justified by legitimate interest if relevant requirements are met (point 37 of the 2/2019 Guidelines).

We would therefore welcome confirmation from the EDPB that even if contractual necessity in the context of account information and payment initiation services is interpreted narrowly, it is still possible for the controller to rely on other legal bases for purposes going beyond the services provided, as long as necessary criteria are met.

Silent party data

We welcome the EDPB’s acknowledgement that legitimate interest is a relevant legal basis for the processing by the data controller of ‘’silent party’’ personal data. Yet, we are still concerned that the EDPB takes an overly restrictive approach on this issue, in which no further processing is permitted for ‘’silent party’’ data.

We see a risk that a narrow interpretation of the legal bases for data processing in this context will undermine the potential to keep developing open banking

[1] Such ‘’balancing test’’ requires that data controllers consider and balance data subjects’ fundamental rights and freedoms with their own or third parties’ interests.

services. We are concerned such restrictive interpretation will limit the benefits of these services to consumers and the payment service ecosystem in general. By allowing open access to transaction data, open banking can help stimulate innovation in new services targeting the underbanked. It can also help build credit capacity and offer alternatives to existing credit opportunities.

The GDPR does not prohibit the processing of personal data of data subjects whose personal data have not been collected directly. Art. 14 of the GDPR sets out conditions for transparency in this context.

We would therefore welcome clarification from the EDBP that further use of ''silent party'' data is not prohibited as such, but permitted if the relevant conditions for transparency and validity are met. Further processing of such data should be a case-by-case assessment. It should be up to each data controller to ensure transparency and determine the legal basis for data processing. In the case of legitimate interest, it is also the responsibility of each data controller to assess the reasonable expectations of the individual, perform the ''balancing test'' under the GDPR and assess the related risks.

Sensitive data

The EDPB's approach in the guidelines is that payment transactions can reveal sensitive data. If the consumer has not provided explicit consent or there is no substantial public interest based on EU or Member State law, the guidelines state sensitive data must not be processed. As a silent party's consent is not possible, technical measures must be implemented to exclude access to its sensitive data.

The EDPB's interpretation of payment transactions revealing sensitive data is overly broad. Payments or donations to recipients in the area of healthcare, to religious bodies, to political parties or to trade unions are not as such intended to reveal a person's health, political affiliation or religion. They can be done for various purposes unrelated to the underlying sensitive data.

Only additional processing to derive such health, religious, political or trade union information should qualify as processing of sensitive data as such. We would therefore welcome a more nuanced approach where payments data is not considered as inherently sensitive data.

The EDPB appears to suggest that a Data Protection Impact Assessment (DPIA) is required when payment transaction data is processed, because sensitive data may be part of it. Yet, payment transaction data is processed for the sole purpose of payment services, not for that of processing sensitive data. The

EDPB's interpretation as shown in the guidelines is too far-reaching, as well as potentially onerous. It would require a DPIA for every single payment transaction service, despite the low and easily mitigable risks to reveal sensitive information. We would welcome if the EDPB clarified this issue.

Moreover, the EDPB suggests in its guidelines to implement data minimisation techniques to redact sensitive data from payment transactions whenever there is no derogation to process such data, i.e. no valid consent of the data subject and no substantial public interest based on EU or Member State law.
We believe it is the task of each data controller involved in data processing to assess and determine the scope of data minimisation in relation to the intended purposes and the risks involved.

The guidelines could be clearer that each data controller should undertake its own assessment and measures to minimise data. The guidelines seem to suggest that Account Servicing Payment Service Providers (ASPSPs) should monitor data sharing and minimise data for the Third-Party Payment Service Providers (TPPs). If only ASPSPs were to minimise data, this would make them redact data provided to Account Information Service Providers ('AISPs'), and consequently redact this data for the consumers. This would put the ASPSP at a violation of the PSD2, which requires that the AISP is allowed to have access without discrimination to the same data the PSU would normally access.[2] This would also impair the reliability of the services provided by the AISP, as they would be based on partial datasets.

Explicit consent

We would welcome if the EDPB confirmed what stated in its earlier opinion,[3] namely that explicit consent in Art. 94(2) of the PSD2 is a contractual consent, different from explicit consent under the GDPR. The EDPB's guidelines in this consultation include additional requirements for the validity of such contractual consent, namely (i) additional transparency, (ii) making clauses clearly distinguishable, (iii) specific acceptance. These additions raise practical questions.

The GDPR regulates comprehensively the requirements for a privacy notice and the EDPB has already provided comprehensive guidance on content and format

[2] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

[3] EDPB, Letter regarding the PSD2 Directive, 2018

of the notice. The relationship between privacy notice under the GDPR and the additional “privacy” information under the EDPB’s guidelines is unclear, in particular over whether the “privacy notice” under Art. 94(2) of the PSD2 is the same privacy notice as that under the GDPR, or whether it is a subset of the GDPR privacy. If it were the latter case, it is unclear what would be the expectations in terms of the granularity of information to be provided, and whether the controller may simply refer to the privacy notice under Art. 94 (2) of the PSD2. We highlight how the information required by the EDPB should be already included in the contract with the PSU. Not only is it onerous to display multiple times the same information, but it might also lead to information fatigue for the consumer.

In the context of open banking, we would welcome clarification from the EDPB that controllers do not need to display once again the same information whenever the latter is already provided in detail, either via the contract with the PSU or a privacy notice.

Accountability and privacy safeguards

DIGITALEUROPE welcomes the EDPB’s emphasis on privacy-enhancing measures necessary to ensure data processing complies with the legal requirements. Market-driven solutions are being developed to satisfy the GDPR accountability and transparency requirements, and we fully adhere to the use of technology to help data controllers meet their obligations. We have the following comments:

- **Data minimisation:** the EDPB encourages the use of digital filters to support AISPs in their obligation to only collect personal data that is necessary for the purposes for which they are processed. It is the responsibility of each data controller to respect the principle of data minimisation. The guidelines should avoid suggesting that ASPSPs would need to monitor data collection by AISPs and PISPs. They should clarify that each data controller involved in processing activities is responsible for its own compliance with the data minimisation obligations.

  On the scope of data to minimise, the decision should belong to the data controller. According to the PSD2, the AISP needs to be allowed to have access to the data that the PSU would normally access. Limiting the information available to the AISP would impact on transparency for the PSU, and undermine the purpose of data minimisation.

- **Transparency**: the guidelines should avoid ambiguity about which entity is obliged to ensure accountability and transparency. This is important in particular for privacy dashboards that inform the data subject or allow for the withdrawal of consent in the PSD2. These dashboards tools are provided by the entity that has a contractual relationship with the consumer. It is the role of this entity to ensure the PSU's notice and consent.
- **Profiling:** the guidelines are somewhat ambiguous on profiling. They appear to imply that when automated decision-making takes place, the data subject has in certain circumstances a right to object to profiling, regardless of whether profiling-specific activities take place. The guidelines should clarify that data processing cannot be objected when there is a need to comply with a legal obligation (e.g. anti-money laundering) or when profiling is necessary for the performance of a contract (e.g. authentication of the payment user as required by the PSD2).

FOR MORE INFORMATION, PLEASE CONTACT:

Ray Pinto

Digital Transformation Policy Director

ray.pinto@digitaleurope.org / +32 472 55 84 02

Vincenzo Renda

Senior Policy Manager for Digital Industrial Transformation

vincenzo.renda@digitaleurope.org / +32 490 11 42 15

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK