Broadcom's comments on EDPB's consultation on Guidelines 06/2020 on the interplay of GDPR and PSD2

Brussels 14th September 2020

Introduction

We would like to thank EDPB for giving us the opportunity to provide comments on this important discussion. Broadcom is approaching this issue from a unique point of view as it is both a provider of payment security and fraud prevention services to the different providers operating under PSD2 as well as a provider of cybersecurity products and services that enable the PSD2 providers to secure their networks and systems from cybercrime. It is important to note however that Broadcom does not interact directly with data subjects as customers of Broadcom using payment services but rather acts usually as a data processor on behalf of the different PSD2 entities, usually either the Payment Initiation Service Provider (PISP) or the Account Servicing Payment Service Provider (ASPSP). Broadcom may interact with data subjects as part of the strong authentication service it provides to PISP and ASPSP customers to enable their PSD2 compliance.

As a general principle we are aligned and in agreement with the direction the guidelines are taking, and the recommendations put forward by EDPB. We are convinced that the provision of fraud prevention services meets the requirements put forward by EDPB and can be done in a manner which is privacy friendly and least intrusive for data subjects, while providing the maximum possible level of assurance for the PSD2 providers. Our policies and practices are driven by the desire to offer a truly competitive technology that meets the requirements of our customers in preventing fraud and abuse of the financial system, the limitations put on the technology by the requirements of PSD2 in the form of RTS and our strong belief that ensuring a high level of data protection is critical for the success of our business.

How payment security and fraud prevention work

As mentioned, payment security services for PSD-2 SCA are delivered both to PISP and ASPSP as a data processor in the form of a software as a service (SaaS). When a PISP will initiate a payment or when an ASPSP will process payment information they will utilize data that is collected by the service recipient in line with the requirements of the Regulatory Technical Standards (RTS) mandated by PSD2. This information will be processed by the SaaS solution to provide a secure communication protocol (following the 3-D Secure 1.0.2 and EMV 3-D Secure industry standards) to enable communication with the ASPSP and application of strong customer authentication (SCA) in compliance with the PSD2 obligations. In addition, for the cases of ASPSP the SaaS will also provide risk analytics in line with the PSD2 obligations to manage risk, as per Article 2 of the RTS. More specifically this means that the ASPSP will receive a score that will indicate the assessment of the probability of the transaction being fraudulent or not. It should be noted that the service doing the risk analytics does not identify or profile the transacting parties and it relies on strong pseudonymization. The decision how to apply this risk evaluation and determine whether a transaction should be permitted or not is for the ASPSP to take in accordance to their own policies, controller entirely by the ASPSP.

The SaaS infrastructure and service are subject to numerous certifications such as SOC2, PCI-DSS and PCI-3DS as well as detailed data processing agreements laying out the different processor obligations under GDPR Article 28.

Legal basis for processing

We agree with the analysis done by EDPB that demonstrates that the appropriate legal bases for processing in the case of PSD2 are the performance of a contract or the compliance with a legal obligation. We strongly believe that these are appropriate legal bases that should be narrowly interpreted and are sufficient to meet the needs of most use cases. In addition, especially in the case of fraud prevention we would argue that consent would not be an appropriate legal basis to use and should never be used as such because it is likely to require the consent of the defrauding party, which would be both unreasonable and counter-productive to request. Additionally, the onus of demonstrating consent and the potential withdrawal of consent in scenarios involving security of payments especially in cases that payment is processed or has already happened, can put at risk the reliability, confidence, non-reputability or auditability of the system. It would make ASPSP's ability to comply with PSD2 contingent on consent being obtained from potentially a fraudster. Similarly, the right to delete data should be considered differently in payment fraud prevention use cases: it would be inappropriate to honour a fraudster's request to delete the metadata relating to their activities. Consequently, our view would be that in payment security and fraud prevention, unlike other use cases, consent is not an appropriate legal basis to use unless it can be demonstrated otherwise.

Moreover, the use case of fraud prevention is one of the few cases whereby compliance with a legal obligation and contract performance as a legal basis are very closely aligned and potentially interchangeable. It is clear that PSD2 foresees risk management and fraud prevention explicitly as one of the obligations of the participants in the payment system, as well as to protect the integrity of SCA itself. Furthermore, it is reasonable to expect that as part of the performance of the contract there would be reasonable security measures in place to ensure secure payment processing and SCA, and that fraudulent payments or sca attempts are detected, recognized as such, and prevented from happening. All these requirements are met through the use of SaaS technology such as the one provided by Broadcom. Therefore, from the perspective of the data processor our view would be that as long as the data controller has in place the appropriate data processing agreements in line with Article 28 of GDPR the requirement of a suitable legal basis is met for payment security and fraud prevention.

Secondary processing purposes

A topic that is not discussed in depth in the consultation is secondary processing that a data processor may do while providing services to controllers beyond the case of silent parties. In the case of fraud prevention and payment security some secondary processing is necessary for product improvement, more specifically in order to ensure that the algorithms and methods used by the detection engine are up to date to enable detection of the latest fraud schemes that attempt to bypass existing security measures. This processing would involve taking always pseudonymized information or data related to the attributes of a payment

(such as the amount spent, or the general location from which a payment was done) and processing them as a data controller to ensure that new fraud techniques are detected by the SaaS. Usage of fully anonymized data is not possible for these purposes because full anonymity would render impossible the consistency of the results and the ability to audit and demonstrate the effective functionality of the tools. When considering the requirements for Anonymization and Pseudonymization, consider an account identifier. Anonymization may substitute the account identifier for every transaction with a unique random replacement that cannot be reversed. Pseudonymization substitutes the account identifier with a token that is not resolvable back to the account identifier but is at least consistent across transactions. When building systems to detect retail payment fraud, it is not necessarily a requirement to identify specific individuals to develop effective algorithms and methods, however it is a requirement to model the behaviour of an actor in the system consistently over time. Other financial fraud domains may have different requirements, for example in money laundering systems identification of specific actors may be a requirement.

For this kind of processing that is strictly limited in purpose, it relies on data already in the possession of the data processor, does not require identification of the data subject and utilizes for a limited period a restricted data set that is only indirectly identifiable or pseudonymous data, there could be different legal bases available. The first and obvious legal basis is the legitimate interest of the data controller. In fact, GDPR recital 47 explicitly calls out fraud prevention as one of the legitimate interests that can be pursued by the data controller when processing personal data. The legitimate interest in question would be in direct compatibility with the purpose for which the data have been originally collected, that is the rendering effective of the mechanisms that enable secure and fraud-free payment in line with the contract and the legal obligations prescribed by PSD2. In this particular case it can be convincingly argued that the ultimate recipient of the benefit of a well-functioning fraud prevention technology is not just the data processor, or the data controller, but all parties to a payment transaction such as the consumer/data subject, the merchant, the merchants acquirer, PISP, or PSP, and the society at large that does not have to carry the financial cost of fraud and that this kind of processing ensures superior data quality when payment transactions occur. Alternatively if one were to view this form of processing as secondary processing within the meaning of Article 6 paragraph 4 of GDPR, it can still be argued that the purpose of processing is compatible with the original purpose for which the data were collected (secure and fraud-free transaction) and following the guidance of EDPB, the compatibility can be demonstrated to be in line with a legal obligation provided by PSD2, in particular the obligation to provide an effective risk management and fraud-free transaction. The link with the original collection purposes can be clearly and strictly demonstrated as required in Article 6.4.a, the context can also be demonstrated in particular the data has been made available to the processor as part of the processing operation offered to the controller with all the protections and transparency GDPR requires, the nature of the data and the consequences of processing remain the same as the ones disclosed to the data subjects when the original collection took place and so does the existence of appropriate safeguards as foreseen in Article 6.4.e. Finally, such data are not used for any purpose other than the ability of the technology to effectively detect new and evolving fraud schemes in line with the requirements of Article 2 of PSD2 RTS. The strictness of how the secondary purpose is applied re-enforces the overall compatibility of processing.

Finally, a key point to be made is that the ability of fulfilling effectively the primary purpose over time depends on the ability to conduct this kind of secondary processing. Unless fraud detection systems are able to learn and adapt to new fraud schemes their efficacy will be reduced over time and the primary purposes will ultimately become unachievable. Therefore, this additional compatible or secondary processing becomes an indispensable activity on which the success of the primary purpose depends.

Overall, we agree with the recommendation of EDPB on the interpretation of legal basis and the interplay with GDPR and PSD2. However, because of the complexity of the financial supply chain we feel it is important to recognize that beyond the original controller-data subject (active or silent) relationship, there may be additional forms of processing that EDPB needs to take into account.

Proportionality and processing of personal data – How automation works

When looking at the question of proportionality in the context of PSD-2 requirements for SCA and fraud prevention for retail e-commerce transactions based on the 3-D Secure protocols, it is important to note that the data processor does not collect any personal data, but rather is either supplied with the data that the controller has collected, or is supplied with the data that another PSP to the transaction has collected. The determination of what categories of data needs to be collected for the purposes of payment authentication and fraud prevention is determined by the RTS and therefore not open to negotiation or choice.

That data is used by the SaaS to conduct the strong authentication as required by PSD2. Then it is used to enable the processing of a transaction for fraud detection. Depending on the medium that is used to perform the transaction there may be different or additional data sets collected for example in the case of a POS terminal a browser or a mobile phone. Nevertheless, the purpose of the processing from the perspective of the processor when it comes to fraud prevention is not to identify the individual doing the transaction but rather to confirm that it is a valid payment request that does not trigger any of the risk indicators that would suggest fraud.

In doing so the SaaS will process certain pseudonymous information and transaction attributes and determine a score that is provided to the ASPSP. The score will indicate the confidence of the SaaS provider whether the transaction has risk indicators that fraud is occurring or not. The score will be determined by indicators of whether the transaction in question contains elements that would be considered anomalous and thus indicating fraud risk. The SaaS is not building a profile of an individual because it is not evaluating personal aspects of a natural person, such as preferences, behaviours and attitudes, nor is it conducting analysis or predicting aspects of a person's performance in any of the areas covered under the definitions of Article 4 GDPR. In the end the decision how to act based on the scoring is with the ASPSP. It can assess the transaction, verify the validity of the transaction or outright reject it. The data processor has no control on that decision.

The data used for this kind of processing apart from enjoying a high level of cybersecurity is kept online only for a period of 6 months enabling its regular processing and usage for the purpose of payment security and fraud detection. Afterwards it is archived to provide auditability in line with legal requirements in different countries.

We agree with the EDPB recommendations to demonstrate proportionality in the guidance such as limited data sets, limited retention, relevant data collection, additional security measures. In our view the RTS determination of the limited data set, for a very clear purpose, with strong cybersecurity and pseudonymization and its limited online storage is a good example of how those recommendations can be met in practice.

Issues for EDPB to consider

Data transfers

The payment industry needs to operate on a global basis in real time. As a result of that payment infrastructure needs to be global in line with the global and cross-border nature of trade both for consumers and enterprises alike. Compliance with EU-specific regulations such as the PSD-2 RTS is often achieved through the implementation of global payment industry standards and protocols such as the 3-D Secure 1.0.2 and EMV 3-D Secure specification. Equally payment security and fraud detection need to follow those market trends to provide effective solutions to time-sensitive (near real time detection), data-intensive (large amount of transactions) and process-intensive (large amount of simultaneous service requests) requirements. Any alternative to this model is unthinkable as it would result in the inability to conduct effective e-commerce or to enjoy the benefits of shopping in another country using credit and debit paying methods. EU merchants and PSPs must be able to allow non-EU payment service users to user their services; EU ASPSs must be able to interact with other parties to payment processing worldwide.

This results in a major requirement for data transfers as a key component of any solution to enable optimal functionality, interoperability, security and resilience. The recent Court of Justice judgment on the Schrems II case has created major uncertainties for providers and customers alike on the way data transfers need to happen moving forward. The discussion is not whether data transfers need to happen, that is a must, but rather how they need to happen to satisfy the requirements of the Court.

Our view would be that whereas the data held by ASPSP are relevant to authorities because they can help demonstrate or conclusively prove illegal activity covered by PSD2 (e.g. money laundering), the data provided to and held by data processors for the purpose of fraud prevention and compliance with the PSD-2 , because of their limited set, indirect nature and pseudonymous attributes, would be of limited value. In addition, the use of strong security features including encryption in transit and at rest, coupled with the limited risk, should satisfy the Court's requirements for supplementary measures.

Security requirements and breach notice

Both controllers and processors are subject to security and breach notification requirements under GDPR. The requirements are well understood and supported. In fact, our view would be that GDPR had an overall positive effect in the increase of cybersecurity capabilities within the industry. Nevertheless, the financial industry is also subject to another cybersecurity instrument, the Network and Information Security Directive (NISD). Under the NISD providers of critical infrastructure (Operators of Essential Services – OES) are subjected to cybersecurity and breach notice requirements and supervision by competent authorities.

Financial service providers are often considered OES in different member states and as a result their data processors would be expected to assist them in meeting GDPR and NISD security and breach notification requirements. Whereas GDPR is focused on data and NISD is focused on infrastructure it is clear that security incidents overlap and rarely an incident affecting infrastructure has no impact on data and the other way around. This dichotomy creates operational, governance and investment challenges as organizations try to meet the requirements of both instruments and demand assurances of their providers that they can satisfy both requirements. As EDPB has issued guidance on the interplay between GDPR and PSD2 it would be also advisable that such guidance is issued on the interplay between GDPR and NISD.

The future of AI usage in payment security

As mentioned earlier efficient payment security requires real time detection of incidents and the management of very large volumes of data (billions of payments) in high intensity (simultaneously several thousands of transactions). As existing methods of payment become more and more electronic, new forms of payment and alternative means of payment continue to grow, so will the efficacy be pushed to its limits and new forms of fraud will emerge. It is therefore certain that payment security will be required to adopt new technological capabilities to remain effective and relevant and to continue to provide services to its customers that benefit consumers and the stability of the financial system.

One of the obvious technological choices to manage the efficiency challenges mentioned above is the use of artificial intelligence (AI) to manage volume and intensity of processing fast. The usage of AI does not necessarily deviate from the principles of security, fairness, proportionality, accuracy and data minimization. All these requirements still stand but would need to be considered in the context of large scale pseudonymous automated processing that AI could enable, without relying on profiling. In that context access to real life data that proved to be originating from a fraudulent transaction would be critical to ensure efficacy of detection as well as limitation of bias. Exercise of individuals rights, the level of transparency and auditability afforded would need to be balanced with reasonable security concerns and the ability to determine the levels of reasonable intervention on the models and data sets on which AI would run. Unlike other fields whereby AI is nascent there is already considerable level of work developed for fraud prevention in the financial services sector globally, as well as established governance models by the US Federal Reserve for AI systems applied to financial fraud. The ICO has also developed useful guidance on the interplay of AI and data protection and the European Commission has announced regulatory work on this area. We would welcome guidance from EDPB on this important point in order to achieve strong data protection, while taking into account the realities of industry.

++++++++++++++++++

We would like to thank again the European Data Protection Board for giving us the possibility to provide feedback to this important issue. We remain at your disposal to provide additional information. Please feel free to contact:

Ilias Chantzos, Global Privacy Officer and Head of EMEA Government Affairs
Ilias.chantzos@broadcom.com