OPEN BANKING AND PRIVACY

EU tackles technological challenges and consumers protection issues of the market for digital payments mainly through PSD (Directive no. 2007/64/EC) and PSD2 (Directive no. 2015/2366/EU). The first allows entities other than banks (IMEL and IP) to carry out payment services; the second implements Third Party Providers' (TPP) organization and activity.

TPP are not a party to the contractual relationship between the user and the account servicing payment service provider (ASPSP), but can access the payment account to perform certain services on behalf and at the request of the user. These services consist of the payment initiation service, carried out by the PISP (*Payment Initiation Service Provider*), and the account information service, carried out by the AISP (*Account Information Services Provider)*. The PISP intermediates between the user and the user's online account, allowing the user to issue a payment order without disclosing account number or credit card references to the beneficiary. The AISP offers the user an immediate overview of his financial situation by aggregated online information taken from one or more payment accounts held with different payment service providers without access to such accounts but rather via online interfaces of the ASPSP.

The increased number of intermediaries involved in the payment procedure contributes to the significant development of the so called open banking and, at the same time, triggers the need for an easy exchange of data and information between the same intermediaries for the completion of any transaction. In this scenario, user's data are material both as data necessary for the execution of the payment and as personal data of the user. Therefore, user's data are subject to regulation of payment services and to regulation on personal data protection and processing, as recently amended by Regulation no. 679/2016 (GDPR). GDPR aims to adapt privacy notion and protection of personal data to rapid technological developments. The main purpose is to encourage personal data transfer, granting data subjects protection from any abuse and control over their own personal data.

The paper offers a preliminary analysis of the involvement of different intermediaries in the digital payments to further investigate certain issues of the intermediaries' role.

Then the paper focuses on interactions and possible conflicts between digital payments and personal data protection and processing rules, identifying and addressing certain issues.

Firstly, the paper refers to cases where the TPP and PSP can lawfully use personal data [art. 4(1), n. 1, GDPR], since PSD2 provides for a rather rigid regime, while GDPR allows a broader treatment. PSD2 provides for two circumstances. In the first circumstance (the service provision requested by the user), there is a divergence between the two pieces of legislation on the user's consent. The issue is to be resolved in the sense that the consent required for the execution of a payment transaction absorbs that required for processing. In

the second circumstance (the prevention of fraud), the occurrence of a legitimate interest of the intermediary is the condition which makes the processing lawful.

The second issue discussed and solved in the paper refers to cases not expressly provided for by PSD2, namely processing of data for profiling and marketing purposes and processing of user's biometric data. Processing of data for profiling and marketing purposes is prohibited by PSD2 as not necessary for the execution of the payment transaction, while it is allowed by the GDPR within certain limits. Biometric data, whose processing is exclusively allowed in specific cases set out by GDPR, may be material for payment purposes as user's personalised security credentials. In such a case biometric data should be considered as sensitive payment data and as such their use will be subject to even stricter rules applicable to TPP.

Thirdly, the paper deals with the position of the payee, whose personal data are transferred to the payer's PSP outside any direct relationship between the latter and the payee. The paper argues to reconcile, on the basis of the GDPR, the interest of the intermediary, to execute the transaction in a short time, with the interest of the beneficiary, to avoid an uncontrolled use of personal data.

The final part of the paper focuses on cases of unlawful use of users' personal data and the distribution of responsibilities and liabilities between intermediaries.

As for protection of the user, PSD2 (art. 73) and GDPR (art. 82) share the common principle that damages and losses caused by an infringement of the rules by one or more intermediaries have to be indemnified. Additionally, PSD2 (art. 73) states that further financial compensation may be determined in accordance with the applicable law of the contract between the user and the PSP or the PISP. The paper discusses how to coordinate those provisions to pursue full compensation of the aggrieved user avoiding duplication of the indemnification.

The distribution of liability between ASPSP and TPP is to be framed within the GDPR. The liability regime depends on who has actually processed the user's personal data, whether processor, controller or joint controller. Since the processor processes personal data on behalf of the controller, he should not be liable unless he has infringed GDPR obligations or the controller's instructions. Therefore, ASPSP and TPP could be liable only as controllers or joint controllers. This is relevant for the internal sharing of the liability once one of the intermediaries has restored the damages. In the case of joint controller (i.e. two or more controllers who jointly determine purposes and means of data processing), the distribution of the responsibility is determined by an agreement between them (art. 26, GDPR). If, on the other hand, each intermediary is the controller, the one who has paid may claim back from the other controllers a share of compensation corresponding to the damages caused by each of them. Besides these rules, GDPR does not provide any

further indications, therefore the liability regime must be construed on the basis of the applicable national law.