The Legal 500 & The In-House Lawyer

Hot Topic | Banking & Finance

The recast Payment Services Directive and its proposed transposition into Greek Law

Directive 2015/2366/EC, known as the recast Payment Services Directive (PSD2), entered into force on 12.01.2016 and requires Member States to ensure compliance with its provisions by 13.01.2018. According to its Preamble, the PSD2 seeks to achieve alignment with the developments in the market and the emergence of new technologies and types of payment services, to ensure consumer protection against security risks and to establish transparency in the sector. Apart from that, the amendments brought by the PSD2 were needed to modernize the previously applicable PSD (Directive 2007/64/EC) towards the integration of the internal market for safe electronic payments.

As far as Greece is concerned, a bill implementing the PSD2 and replacing Law 3862/2010 (which transposed, among others, the PSD into Greek law) has been the subject of a public consultation in early November. This bill consistently transposes the provisions of the Directive, corrects some failures of the existing law and specifies certain regulatory provisions by defining the scope of the competent authorities' powers. Until the end of 2017, the bill was not introduced to the Parliament for discussion and voting.

Extension of scope. As PSD2 does, the bill has a wider scope than its predecessor in both geographical terms and in terms of the nature of the entities it regulates.

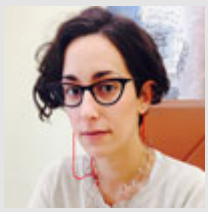
It applies to payment services provided in Greece. To be noted that the existing law, most probably due to a clerical error, seemed to apply to all payment services provided in the Union. Still it is

Topic Author: Rokas

Rokas International Law Firm

The Legal 500

Viktoria Chatzara, Senior Associate
v.chatzara@rokas.com



Chloe Iordanidou, Associate
c.iordanidou@rokas.com

unclear whether the bill applies to cover payment services provided to Greek residents only by Greek PSPs, or also by non-Greek PSPs, regardless of the residence of the service receiver.

Moreover, the bill's provisions on the transparency of terms and information requirements cover all transactions conducted in an EEA currency not only where both the payer's and the recipient's PSPs, but also where only one thereof is located in the EEA. Some of the provisions contained in the bill apply to all payments between PSPs domiciled in the EEA, regardless of whether such payments are conducted on an EEA currency.

The bill covers transactions made through a commercial agent acting for both parties, and exempts such transactions only if the agent acts for one of the parties; it also provides clarifications in relation to the limited network exemption contained in the existing bill.

The Directive prohibits the provision of payment services to non-PSPs and to entities not specifically excluded by the aforementioned exemptions. A relevant prohibition has also been included in the Greek bill.

Under the Directive, Member States are to provide for penalties applicable in cases of infringement of the provisions of the Directive, as implemented into local law. Under the Greek bill, PSPs that do not comply with its general requirements are not allowed to provide payment services and the Bank of Greece (BoG) as the regulatory authority is vested with the power to impose penalties or even to revoke the license.

New entrants. The bill covers third party payment and account information services providers, such as Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). PISPs offer customers the ability to enter into transactions by managing their money directly from their accounts, thus rendering credit and debit cards redundant. AISPs offer customers a consolidated view of the accounts they hold and enable payment service users to go over their spending habits.

These third party PSPs have been operating unregulated, since they do not fall within the scope of the existing law. Under the new law, they will have to secure personal details (such as PIN codes) provided to them by their customers, and avoid storing sensitive payment information. Third party PISPs and AISPs must only request such data from payees as necessary to provide their services and cannot use, access or store any data for any other purpose than for the completion of their services. These data-related provisions supplement and by no means replace the law which has harmonised the currently applicable Data Protection Directive or the General Data Protection Regulation (GDPR) which will apply as of 25.05.2017. In this regard, said third party PSPs will have to comply with the transposed PSD2 provisions along with the new, strict provisions of the GDPR. At the same time, from a privacy law aspect, the anticipated new e-Privacy Regulation could also affect PSPs, upon adoption and entry into force.

PISPs will be subject to regulatory authorisation. They will have to put in place professional liability insurance and fulfill newly introduced capital requirements. In case of a delayed, incorrect or unimplemented payment conducted by a PISP, the bank where the payment account is maintained will be liable towards the account holder but will be entitled to reimbursement by the PISP, if the

latter has been culpable for the incident. On the contrary, AISPs are only required to have professional liability insurance in place; the bill does not provide for any capital requirements for such entities.

PISPs will need to safeguard all funds they receive from customers or through another PISP during a transaction, by following one of the procedures prescribed by the new law, for example by ring-fencing such monies in separate bank accounts. However, as noted during the public consultation of the Greek bill, the proposed law could be improved so as to ensure the protection of these accounts against foreclosure.

Under the new regulatory regime, financial institutions, e-money institutions and payment institutions that hold payment accounts must, subject to the consent of the PSP user, offer PISPs and AISPs access to the users' accounts through a technical interface that will be established specifically for this purpose. The access will have to be wide enough to allow PSPs to provide their services efficiently and unobstructed. As far as AISPs are concerned, banks will have to offer them access to all information available to the customer, as long as they do not reveal "sensitive payment data", which are defined as including all data that can be used to carry out fraud.

The access-to-account right is regarded as the most critical change introduced by the Directive. On the one hand it will raise security, data breach and fraud risks, and will thus generate compliance costs and IT costs. On the other hand it is expected to create a level playing field for all PSPs and encourage competition and innovation. Moreover, the interplay between this right and the GDPR is yet to be clarified, as it is not clear which party, i.e. the PISP/AISP or the institution holding the account, must obtain the payer's consent, which is required for access to be granted. Furthermore, the definition of "sensitive payment data" is rather vague, and consequently banks may need to take a very cautious approach when redacting any data that could possibly be classified as sensitive, in order to ensure compliance with both the new law and GDPR.

Security and consumer protection. The Greek bill establishes numerous provisions that will have a positive effect on the protection of payment services users against security breaches and fraud, as well as to the overall regulation of the market. Taking into account that over the last years security risks have increased, such provisions were necessary for the sustainability of the payment services market.

Enhanced regulatory powers and risk management obligations. The PSD2 vests the competent authorities of the Member States with wider supervisory powers over PSPs, giving them, among others, the ability to implement preventive measures in case of emergency events (e.g large scale fraud).

In Greece, these supervisory powers remain divided between the BoG and the General Secretariat of Trade and Consumer Protection (GSTCP), which takes the place of the currently competent General Consumer Secretariat. The interplay between the two authorities could become a challenge, since the provisions delegating their powers are complex and could create confusion in relation to the competence of each Office.

Under the bill, the licensing and supervision of PSPs as well as the transposition of PSD2 remain

incumbent upon the BoG, which shall monitor compliance. As such, it will need to define the content of an application for authorisation, as well as to establish the procedure, documentation and requirements that will apply for the authorisation of PSPs.

The BoG also has the authority to adopt measures against PSPs, their Directors or any other person responsible for breaches of the law. These measures include, among others, the revocation of the PSP's licence and the imposition of fines up to 5 million euros.

The GSTCP shall be responsible to ensure compliance with the transparency of terms and the information requirements that apply to the payment services (information provided to the payer and to the payee, requirement of consent, liability for unauthorized payments, etc). In exercising its authority, the GSTCP can carry out audits and impose on PSPs measures similar to those that can be imposed by the BoG.

Risk management obligations. PSPs shall devise a security policy document and conduct a detailed risk assessment, describing a reaction plan to potential security breaches and similar incidents. Similarly, effective incident management procedures will have to be introduced, and several documents will have to be reported by PSPs to the BoG, including an assessment of the potential operational and security risks.

More importantly, the bill grants customers increased protection due to the obligation imposed on PSPs to inform customers directly in the event of an incident impacting on their financial interests. PSPs must also notify the BoG in the event of a major operational or security incident.

Customer authentication and other measures. Comparing to the currently applicable regime, and in accordance with the provisions of the PSD2, the customer authentication process will become stricter under the new law, requiring customers to provide two elements out of three categories, i.e. something they know, such as a code, something they are, such as a fingerprint, and something they own, such as a payment card, in the following circumstances:

a) where the payer accesses its account online;

b) where the payer initiates an electronic payment transaction; and

c) where the payer carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

This will most likely render electronic transactions safer. For instance, if an account holder loses his payment card, or if the card gets stolen, he will no more have to cancel such card, since the card alone will no longer suffice to conduct any type of electronic, online or remote transaction.

In order to initiate remote electronic transactions, PSPs must ensure that the transaction is connected to a specific amount and a specific payee. If not, any resulting loss will only be borne by the PSP and not by the payer, unless the payer has acted fraudulently. This set of requirements will only come into force towards the end of 2018 or the beginning of 2019.

Moreover, in the event of an unauthorized payment, the payer will be liable for up to € 50 (instead

of € 150 under the existing regime). However, the payer will be obliged to bear all losses, if he has been fraudulent or has intently or negligently failed to comply with the terms and conditions of the payment instrument or if he did not notify the PSP in time about the loss, theft, misappropriation or unauthorised use of the payment instrument.

In conclusion, the implementation of the PSD2 into Greek law is expected to cause significant changes to the regulatory framework of the payment services industry. Such changes are expected not only to promote innovation and competition, but also to contribute to consumer protection. A few changes in the draft bill would enhance clarity and result in a clearer division of regulatory powers between the two competent authorities. Banks, PSPs and other institutions or businesses that fall into the scope of the bill will have to proceed with gap analyses and determine the necessary measures to readjust their organisation and operations to the expected law.