NEW ACT ON PAYMENTS
ADOPTED BY THE DANISH PARLIAMENT – SET TO TRANSPOSE PSD2 IN DENMARK

6.2.2017

On 2 June 2017, the Danish Parliament adopted a new Act on Payments (in Danish: Lov om betalinger). The Act will enter into force on 1 January 2018, subject to certain transitional rules, and will transpose PSD2 into Danish law and replace the existing regulation set out in the Act on Payment Services and Electronic Money. Get a brief on certain aspects of the Act, which in our assessment are of particular significance compared to the existing regulation.

Enhanced ability to process data showing where payers have used their payment instrument and what they have purchased

The existing regulation includes a ban on the processing of data showing where payers have used their payment instrument and what they have purchased unless such processing:

- is necessary for the completion of correction of the payment transactions or other functions with which the issuer has combined the payment instrument;
- is necessary for law enforcement or preventing abuse; or
- is authorised by other legislation.

The ban is based on a special Danish rule which is not reflected in PSD (2007/64/EC) or PSD2 (2015/2366/EU) and has prohibited payment service providers from processing data showing where payers have used their payment instrument and what they have purchased for the purpose of for example customer loyalty schemes or similar marketing activities. The ability to allow for the processing of such data has been one of the most debated parts of the Act of Payments (the "Act") during the public consultation on the proposal for the Act and the readings in the Danish Parliament.

In general, the Act will allow businesses to process data showing where payers have used their payment instrument and what they have purchased, subject to the following conditions and principles:

1. the payment data is only processed in connection with:
   a) the execution or correction of a payment transaction,
   b) the provision of services that are directly intended for the user, i.e. services that the user has actively requested; or
   c) the anonymisation of the payment data;
2. with respect to b) above, the user has given its prior explicit consent to the processing of the payment data for this purpose;
3. payment service providers may not condition prices and terms for the use of its payment services or payment accounts upon the payment service user giving such
consent to the processing of data;
4. the payment data is not processed for the purpose of setting individual prices and terms for the same product or service to different users; and
5. the payment data is processed in accordance with the general rules on the processing of personal data in the Danish Data Protection Act.

The liberalisation of Danish law, which the Act represents, will be welcomed by the offerors of loyalty schemes and Fintechs alike.

Full implementation of "limited network exclusion" and abolishment of the requirement for providers of payment instruments with limited application to obtain authorisation

The Act implements the limited network exclusion in Article 3, litra k) of PSD2 and thus abolishes the existing gold-plating which required providers of services based on payment instruments with limited application (e.g. store cards, fuel cards, membership cards, parking ticketing or vouchers for specific services) to obtain a restricted authorisation with the Danish FSA.

Providers that are able to rely on the limited network exclusion will therefore going forward not need to obtain a restricted authorisation with the Danish FSA in order to provide services based on payment instruments with limited application. Accordingly, such providers will also be excluded from the regulations in the Act on Measures to Prevent Money Laundering and Financing of Terrorism, which – in the context of payment services – only applies to providers of payment services that are required to be authorised with the Danish FSA.

Certain parts of the Act pertaining mainly to consumer protection will, however, still apply to providers that are able to rely on the limited network exclusion. In addition, such providers will have to report to the Danish FSA if the total value of the payment transactions effected in the preceding 12 months exceeds EUR 1 million in order for the Danish FSA to assess the basis for such providers' exclusion from the Act.

Providers of payment services where the monthly average of the preceding 12 months’ total value of payment transactions does not exceed EUR 3 million will still need to obtain a restricted authorisation with the Danish FSA. However, such providers will going forward be relieved of the duty to safeguard users' funds as this requirement has generally been found to be unproportioned (despite such duty being recently introduced under the existing regulation in 2014).

Third party access to accounts held with other payment service providers

With the aim of regulating third party providers, the Act introduces "payment initiation services" and "account information services" as new types of payment services.

- Providers of payment initiation services initiate payment orders at the request of a payment service user with respect to a payment account held at another payment service provider.
- Providers of account information services provides consolidated information online on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.

Being one of the debated parts of PSD2, a customer (payer) with a payment account, which is accessible online, will under the new Act have the right to make use of a third party payment service provider to obtain payment initiation services or account...
information services.

The European Banking Authority (EBA) is expected to publish guidance before 2018 as to the basis on which market actors are to implement this third party right of access to accounts, including, in particular the use of Application Programming Interfaces (APIs), which are foreseen to be the software that from a technical standpoint will allow payment initiation service providers and account information service providers to connect to accounts held with other payment service providers in a secure manner.

Many Fintech start-ups are eagerly awaiting the opportunity to access bank account information of consumers with their consent.

Rules on access to credit institutions’ payment accounts services

In order to allow payment institutions to provide payment services in an unhindered and efficient manner, the Act also introduces an obligation on credit institutions to make it possible for payment institutions to open bank accounts with them and thus have access to payment accounts services on an objective, non-discriminatory and proportionate basis. Credit institutions must provide the Danish Competition and Consumer Authority with duly motivated reasons for any rejection to grant a payment institution access to its payment accounts services.

Requirement to use "strong customer authentication"

The Act tightens the security measures on the identity verification procedures and introduces an obligation for payment service providers to use "strong customer authentication" where a payment service user:

- accesses its payment account online;
- initiates an electronic payment transaction; or
- carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

"Strong customer authentication" is an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent. According to the preparatory works to the Act, the use of NemID will qualify as strong customer authentication. EBA is expected to develop regulatory technical standards on the requirements for strong authentication procedures and the exemptions from the application of this requirement.

Users' liability – strong incentives to opt for strong customer authentication

Under the current regulation payment service users are liable for an amount of up to DKK 1,200 for loss suffered due to unauthorised use of a payment instrument where the personalised security features of the payment instrument (e.g. PIN-code) have been applied. The Act lowers this threshold to DKK 375. However, with the aim to enhance incentives for payment service providers to opt for strong customer authentication, the payment service users' liability for unauthorised transaction is zero, if the payment service provider has not used strong authentication. This means that the party to the payment process that does not use strong authentication will be liable for any loss in case of unauthorised transactions.