PSD2 implementation in the Grand Duchy – six months later

NautaDutilh
AVOCATS LUXEMBOURG

10 May 2019 | Contributed by NautaDutilh

Banking, Luxembourg

- **CSSF's implementation of PSD2**
- **Local stakeholders' implementation of open banking**
- **The Grand Duchy: the next European payment hub?**

Following a precedent publication on the implementation of the E
U Payment Services Directive (PSD 2) in November 2018, the Luxembourg Financial Supervisory Authority (CSSF) has been active and the industry is preparing for the open banking wave. The changes in response to PSD 2 aim for a generally positive evolution of the payment scene in Luxembourg.

CSSF's implementation of PSD2

The CSSF has published the fallback exemption request form and adopted several circulars that are applicable to payment service providers (PSPs).

Fallback exemption

In the context of open banking, account servicing payment service providers (ASPSPs) must provide access to account interfaces to allow third-party providers (ie, account information service providers, payment initiation service providers and PSPs that issue card-based payment instruments) to offer their services to payment service users.

In order to do so, ASPSPs can either:

- allow third-party providers to access online banking interfaces intended for payment service users; or
- implement a dedicated interface.

In the event that the second option is chosen, contingency measures must be implemented and, in the event of unavailability or performance issues, the third-party provider will be allowed to use the payment service users' interface as a fallback. This rule thus drastically limits the appeal of having a dedicated interface. To counter this, the European legislature added an exception to this rule. Competent authorities may exempt ASPSPs from having to have a fallback solution in place if the ASPSP can prove that its dedicated interface fulfils the criteria established in the European Banking Authority (EBA) guidelines in relation to Article 33(6) of EU Regulation 2018/389.**(1)**

In this context, the CSSF published application forms for banks, payment and electronic money institutions and POST Luxembourg to request such exemption. To be exempt from the fallback mechanism on 14 September 2019, the relevant institutions had to submit the application no later than 1 May 2019.

In addition thereto, the CSSF stated in a February 2019 communique that the recourse to a provider (within the group or a third party) for the development and management of the dedicated interface, for which the fallback exemption is requested, qualifies as a material outsourcing. Thus, the ASPSPs must request an outsourcing authorisation (or make an outsourcing notification if the service provider is a support professional of the financial sector) in accordance with CSSF Circulars 12/552 and 17/656.**(2)** Further, the CSSF stated that the compliance obligation relating to the fallback exemption remains solely incumbent on the ASPSP.**(3)**

CSSF circulars

In addition to the fallback exemption form, the CSSF has published several circulars that are applicable to PSPs, in particular in relation to the EBA guidelines.

Circular 18/704: Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10)

Pursuant Article 105-2(1) of the Law of 10 November 2009 on payment services (LPS), PSPs must report "major operational or security incidents to the CSSF without undue delay". Complementing this provision, Circular 18/704 and the EBA guidelines contained therein set the criteria to identify 'major operational' or 'security incidents' and determine the format and procedures to communicate them.

Circular 18/704 also linked to a report template and gave delivery instructions. Concerning the option set out in the EBA guidelines to allow the delegation of reporting obligations of major operational or security incidents, the CSSF expressly stated that such a delegation would not be accepted in Luxembourg.

Circular 18/704 has been applicable since 17 December 2018.

Circular 19/712: Guidelines on reporting requirements for fraud data under Article 96(6) PSD2 (EBA/GL/2018/05)

In accordance with Article 105-2(3) of the LPS, PSPs must provide the CSSF with statistical data (at least annually) on payment fraud. The CSSF then shares this aggregated data with the EBA and the European Central Bank.

The EBA guidelines on reporting requirements for fraud data provide details on the scope of the reporting obligation (eg, types of transactions to be reported, reporting frequency, timelines and period) incumbent on PSPs (with the exception of account information service providers). The detailed technical instructions for sending the fraud reporting data will be published separately on the CSSF website at a later stage.

Circular 19/712 will be applicable from 1 January 2020 and the first reporting will be due by 30 September 2020.

Circular 19/713: Guidelines on the security measures for operational and security risks of payment services under PSD2 (EBA/GL/2017/17)

As per Article 105-1(2) of the LPS, PSPs will provide the CSSF (at least annually) with an up-to-date and exhaustive assessment of the operational and security risks of the payment services they provide and information regarding the adequacy of the mitigating measures and control mechanisms implemented in response to these risks.

The content and the frequency of this assessment, and in particular of the audit as regards security measures taken and of the reporting as regards major operational and security risks, are stipulated in the abovementioned EBA guidelines.

Hence, the security measures must be audited once a year by the PSP's internal auditor. The reporting must be provided to the CSSF either:

- as soon as possible after the closure of the financial year and no later than 30 April of each year (for credit institutions);
- at the latest on the last day of the third month after the closing date of the financial year (for payment and e-money institutions); or
- at the latest one month after the annual general meeting approving the annual accounts of the PSP (for POST Luxembourg).

Circular 19/713 has been applicable since 14 March 2019.

Circular 19/714: Update of Circular 17/654 on IT outsourcing relying on a cloud-computing infrastructure

The CSSF amended its Circular 17/654 on IT outsourcing relying on a cloud-computing infrastructure (which is applicable to payment and electronic money institutions) in order to make the notification process less burdensome. As an example, the necessity to notify the CSSF of cloud-computing outsourcing of non-material activities has been replaced by the obligation to maintain a register of all cloud-computing infrastructure outsourcing.

Local stakeholders' implementation of open banking

'Open banking' means that ASPSPs must grant third-party providers access to information or let them initiate payments, based on ASPSPs' clients' (ie, payment service users') consent.

The first deadline in this context was 14 March 2019. For the ASPSPs that will be launching their access interfaces on 14 September 2019, a testing facility and the related documentation had to be published by mid-March.**(4)** In line with this requirement, certain banks established in Luxembourg displayed their testing application programming interface (API) on their own environment, such as the Banque Internationale à Luxembourg and KBL, whereas others displayed their testing API on the marketplace of their service provider (eg, LUXHUB).

The Grand Duchy: the next European payment hub?

Brexit appears to offer Luxembourg the opportunity to strengthen its position on the payment scene. During the past few months, three e-money institutions have obtained a licence (Alipay, Satispay and PPRO) and they will probably not be the last to do so in 2019. The Grand Duchy currently houses eight electronic money institutions and 10 payment institutions.

For further information on this topic please contact Josée Weydert, Vincent Wellens or Anne-Sophie Morvan at NautaDutilh Avocats Luxembourg by telephone (+352 26 12 29 1) or email (josee.weydert@nautadutilh.com, vincent.wellens@nautadutilh.com or annesophie.morvan@nautadutilh.com). The NautaDutilh Avocats Luxembourg website can be accessed at www.nautadutilh.com.

Endnotes

(1) Article 33(6) of EU Regulation on Regulatory Technical Standard on Strong Customer Authentication and Common Secure Communication (2018/389); EBA/GL/2018/07.

(2) In its communique, the CSSF mentions solely "a non-objection" for both types of outsourcing. This choice of wording reflects the actual CSSF practice which seems to consider that notification process as a non-objection procedure.

(3) Communique dated 28 February 2019 – obligations regarding strong customer authentication and common and secure open standards of communication under EU Commission Delegated Regulation 2018/389, Lit H.

(4) Articles 30(3) and (5) of the EU Commission Delegated Regulation of 27 November 2017 supplementing EU Directive 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.


Josée Weydert


Vincent Wellens


Anne-Sophie Morvan