



Eurosystem

BELGIAN CREDIT INSTITUTIONS PSD2 REQUIREMENTS INFORMATION FILE

1 PREFACE

Licensed credit institutions are allowed to provide payment services. When doing so, they are subject to certain requirements laid down in Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2) as implemented by the Belgian Law of 11 March 2018 relating to the status and control of payment institutions and electronic money institutions, to the access to payment service provider activity and electronic money issuing activity and to the access to payment system, and to the relevant Regulatory Technical Standards, Implementing Technical Standards and Guidelines.

This document clarifies the prudential expectations for the 'information file' to be submitted to the National Bank of Belgium. This information file should provide the competent authority with:

1. For credit institutions already offering payment services on the date of entry into force of the Law of 11 March 2018 (hereafter the "**already offered payment services**"): the relevant information for the verification of compliance with the new requirements stemming from PSD2 that are applicable to credit institutions;
2. For credit institutions intending to offer new (including additional) payment services after the date of entry into force of the Law of 11 March 2018 (hereafter the "**new payment services**"): the prior notification required to extend one's programme of activities by offering new payment services. In this context, payment initiation services (PIS) and/or account information services (AIS) are considered as new payment services requiring prior notification (even if already offered prior to the date of entry into force of the Law of 11 March 2018);

This document is to be used as a template to provide the required information to the National Bank of Belgium (**NBB**) regarding current and new payment services provided by your institution. It contains several sections and sub-sections to be completed by your institution.

Institutions should submit all relevant information to the NBB in order to allow the NBB to assess if the institution complies or will comply with the PSD2 requirements.

The information you provide should be true, complete, accurate, up to date and adjusted to the particular service you provide or intend to provide.

The information requested for each section concerns:

1. A concise description of the measures and procedures already in place within your institution that ensure compliance with PSD2 requirements already in force at the date of this circular (e.g. incident reporting);
2. A concise description of the action plan and measures that will be taken by your institution, including a timeframe, to comply with PSD2 requirements that will enter into force in the near future (e.g. RTS SCA/CSC);
3. In case of new payment services, a concise description of the action plan and measures that will be taken by your institution, including a timeframe, to comply with PSD2 requirements.

Any expected difficulties and hurdles should be clearly highlighted.

Each section includes a list of subjects that should be treated in the response. Should you deem it useful, additional subjects may be mentioned albeit this should be done in a concise manner.

The information should preferably be compiled in one *.pdf document and is to be submitted by e-mail to Psd@nbb.be or via postal service addressed to the Governor of the NBB.

The information should be submitted by 30 September 2019 for the first time and thereafter whenever a change in the programme of activities is decided upon.

Contents

| | | |
|-----|---|----|
| 1 | PREFACE | 2 |
| 2 | GENERAL INFORMATION | 4 |
| 3 | PAYMENT SERVICES | 5 |
| 4 | NEW REQUIREMENTS STEMMING FROM PSD2..... | 6 |
| 4.1 | Process to file, monitor, track and restrict access to sensitive payment data | 6 |
| 4.2 | Authentication and secure communication..... | 6 |
| 4.3 | Security policy..... | 7 |
| 4.4 | Incidents..... | 8 |
| 4.5 | The principles and definitions applicable to the collection of statistical data on performance, transactions and fraud..... | 8 |
| 4.6 | Card-based issued payment instruments | 8 |
| 5 | Extension of the Programme of Activities | 9 |
| 5.1 | General | 9 |
| 5.2 | Business plan & functionalities | 9 |
| 5.3 | Organisation..... | 9 |
| 5.4 | Governance arrangements and internal control mechanisms..... | 9 |
| 5.5 | AML/CFT arrangements | 10 |
| 6 | OTHER GENERAL REMARKS | 11 |
| 7 | DECLARATION BY THE INSTITUTION..... | 12 |

2 GENERAL INFORMATION

NAME OF THE CREDIT INSTITUTION:

ADDRESS¹:

¹ In case of a branch of a credit institution from a third country, please mention both the address of the head office as well as the address of the Belgian branch

3 PAYMENT SERVICES

This information file concerns:

- the information file relating to already offered payment services ²

Please indicate the payment services (to the exclusion of PIS and AIS) already offered by your institution on the date of entry into force of the Law of 11 March 2018 by clicking the corresponding box(es) in the table below.

- a change in the programme of activities³

Only indicate the new payment services you contemplate by clicking the appropriate box in the table below. PIS and AIS offered prior to the date of entry into force of the law of 11 March 2018 or prior to the publication of this document should also be mentioned here. Please also indicate the expected start date.

| Payment services as defined in Annex I of PSD ⁴ | Current | Contem- plated | Start date |
|--|--------------------------|--------------------------|---------------|
| a. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account. | <input type="checkbox"/> | <input type="checkbox"/> | |
| b. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account. | <input type="checkbox"/> | <input type="checkbox"/> | |
| c. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider: | <input type="checkbox"/> | <input type="checkbox"/> | |
| (i) execution of direct debits, including one-off direct debits; | <input type="checkbox"/> | <input type="checkbox"/> | |
| (ii) execution of payment transactions through a payment card or a similar device; | <input type="checkbox"/> | <input type="checkbox"/> | |
| (iii) execution of credit transfers, including standing orders. | <input type="checkbox"/> | <input type="checkbox"/> | |
| d. Execution of payment transactions where the funds are covered by a credit line for a payment service user: | <input type="checkbox"/> | <input type="checkbox"/> | |
| (i) execution of direct debits, including one-off direct debits; | <input type="checkbox"/> | <input type="checkbox"/> | |
| (ii) execution of payment transactions through a payment card or a similar device; | <input type="checkbox"/> | <input type="checkbox"/> | |
| (iii) execution of credit transfers, including standing orders. | <input type="checkbox"/> | <input type="checkbox"/> | |
| e. Issuing of payment instruments and/or acquiring of payment transactions. | <input type="checkbox"/> | <input type="checkbox"/> | |
| f. Money remittance. | <input type="checkbox"/> | <input type="checkbox"/> | |
| g. Payment initiation services. | <input type="checkbox"/> | <input type="checkbox"/> | |
| h. Account information services. | <input type="checkbox"/> | <input type="checkbox"/> | |

² This file is to be submitted following the entry into force of the law of 11 March 2018.

³ In accordance with article 76 of the law of 25 April 2014 (the Belgian banking law), a change in the programme of activities of a credit institution should be notified in advance to the National Bank of Belgium.

⁴ For reasons of convenience, the numbering follows the numbering as it would already be included in the list of activities mentioned in Annex I to PSD II.

4 NEW REQUIREMENTS STEMMING FROM PSD2

Please compile the requested information in a single document respecting as much as possible the template.

In order to allow manageable responses that can be processed and afterwards can be compared sector-wide, the size of the answers to the questions should be limited. For your convenience, some items will indicate the desired maximum number of pages or words.

Unless otherwise stated, annexes such as procedures and policies should not be included or added. However, brief and concise diagrams and flowcharts may be inserted in the document.

Belgian credit institutions should provide, when applicable, the same information for their passported branches and services in accordance with Articles 35 to 39 of Directive 2013/36/EU of 26 June 2013.

4.1 Process to file, monitor, track and restrict access to sensitive payment data⁵

The institution should provide a description of the process in place to file, monitor, track, and restrict access to sensitive payment data consisting of:

- a. description of the flows of data classified as sensitive payment;
- b. the procedures in place to authorise access to the sensitive payment data;
- c. a description of the monitoring tool;
- d. the access right policy, detailing access to all relevant infrastructure components and systems, including data bases and back-up infrastructures;
- e. a description of how the collected data is filed;
- f. the expected internal and/or external use of the collected data, including by counterparties;
- g. the IT system and technical security measures that have been implanted, including encryption and/or tokenisation;
- h. identification of the individual(s), bodies and/or committees with access to the sensitive payment data;
- i. an explanation of how breaches will be detected and addressed; and
- j. an annual internal control program in relation to the safety of the IT systems

The description under this section should not be longer than 15 pages.

4.2 Authentication and secure communication⁶

- i. Payment services offered by the institution

The institution should describe the measures, processes and protocols that demonstrate compliance with the authentication and secure communication requirements regarding strong customer authentication (SCA) and common and secure communication (CSC) applied by the institution for the payment services it offers (maximum 2000 words for respectively SCA and CSC).

- ii. The institution as account servicing payment service provider

If you are an account servicing payment service provider that offers payment accounts that are accessible online, please indicate if you will opt for a customer facing interface or for a dedicated interface.

⁵ Article 145 items 1° (a) *juncto* article 46 of the law of 11 March 2018

⁶ Article 145 items 1° (a) and (b) *juncto* articles 47 to 49 of the law of 11 March 2018; For this item, explicit reference is made to the regulatory technical standards (“RTS”) on strong customer authentication (“SCA”) and common and secure communication (“CSC”) published on 13 March 2018 as EU Regulation 2018/389 in the Official Journal of the EU (hereinafter referred to as the “RTS SCA/CSC”)

Should you have opted for the dedicated interface and if you will seek to obtain or have obtained an exemption for the contingency mechanism (fall back) under Article 33(6) of RTS SCA/CSC interface(s) in accordance with Circular NBB_2019_04, a reference thereto suffices, and the information requested in this item needs not to be provided.

If not, the measures, processes and protocols should be described that demonstrate compliance with the authentication and secure communication requirements regarding strong customer authentication (SCA) and common and secure communication (CSC) between an account holder and an AISP/PISP and for card-based issued payment instruments. (maximum 2000 words)

As part of this explanation, a visual representation of the customer journey when a PSU accesses its payment account via a PISP or an AISP (including any authentication steps that take place in your institution's domain) is to be included. This representation should include a step-by-step customer journey of obtaining account information and initiating a payment through the dedicated interface (if any) compared to the customer journey when the payment service user (PSU) does so through your institution's directly offered PSU interface(s).

iii. secure corporate payment processes or protocols

Please elaborate, as the case may be, which secure corporate payment processes or protocols are used within your institution and how PSUs are authenticated.

Should you have already introduced an exemption file in accordance with Circular NBB_2019_06, a reference thereto suffices for the relevant secure corporate payment processes or protocols, and the information requested in this item needs not to be provided

4.3 Security policy⁷

The institution should provide a detailed and substantiated security risk assessment of its payment services, including the new services envisioned to be available within a year. For each risk, the assessment should include

- a description of the risk, including its impact on the institution and its customers, should the risk materialise,
- the inherent risk levels, with an estimation of their likelihood and their impact on the institution,
- the mitigating controls already in place with a description of their effect on the risk level,
- the residual risk level once the mitigating controls are implemented,
- the still to be implemented actions identified to improve the effectiveness of the controls, if any, and the planning for their implementation.

The institution should provide an assessment of its compliance with the « *EBA Guidelines on security measures for operational and security risks under the PSD2* » introduced in Circular NBB_2018_13. The document should present a description of the non-compliance areas and an assessment of their impact on the risk level of the institution.

If the institution offers or wishes to offer AIS and/or PIS, the institution should describe how those new services are/will be implemented. The document should include:

- a description of the IT systems used to implement those services,
- a description of how those systems are integrated within the existing systems of the institution,
- the list of the third-party suppliers involved in the provision of those services, if any, and a description of their respective contribution.

⁷ Article 145 item 1° (c) *juncto* articles 50 to 52 of the law of 11 March 2018

4.4 Incidents⁸

The institution should provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints, which should contain:

- organisational measures and tools for the prevention of fraud
- the individual(s) and bodies responsible for assisting customers in case of fraud, technical issues, and/or claim management;
- reporting lines in case of fraud;
- the contact point for customers, including name and email address;
- the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including notification of mayor incidents to NCAs under Article 96 of PSD2 and in line with the EBA Guidelines on incident reporting (EBA/GL/2017/10)⁹; and
- the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

4.5 The principles and definitions applicable to the collection of statistical data on performance, transactions and fraud¹⁰

The institution should provide a description of the principles and definitions applicable to the collection of the statistical data on performance, transaction and fraud consisting of the following information:

- the type of data that is collected, in relation to customers, type of payment service, channel, instrument, jurisdictions and currencies;
- scope of the collection, in terms of activities and entities concerned, including branches, and agents;
- the means of collection;
- the purpose of collection;
- the frequency of collection; and
- supporting documents such as a manual, that describe how the system works.

4.6 Card-based payment instruments¹¹

The institution should provide a description on the procedures and measures in place for confirming the availability of funds on the payer's account with the institution to the payment service provider issuing card-based payment instruments for the execution of a card-based payment transaction.

⁸ Article 145 item 1° (d) *juncto* article 53 of the law of 11 March 2018

⁹ See Circular NBB_2018_14 of 29 March 2018

¹⁰ Article 145 item 1° (e) *juncto* article 54 of the law of 11 March 2018; See also Circular NBB_2018_30 of 27 November 2018

¹¹ Article 145 items 2° (a) and (c) *juncto* articles 55 and 58 of the law of 11 March 2018

5 EXTENSION OF THE PROGRAMME OF ACTIVITIES

In case you plan to extend your programme of activities by offering new payment services, specifically PIS and AIS, please provide the information mentioned below. Institutions that already offer PIS and/or AIS prior to the publication of this document, should also provide the information mentioned below.

Please note, that this information file does not replace the notification(s) to be made under articles 86 to 89 (branch) respectively articles 90 and 91 (free provision of services) of the Belgian banking law.

5.1 General

In addition to the information to be provided for under section 4 above, the institution should provide the information set out below.

5.2 Business plan & functionalities

The institution should provide

- (i) the rationale to develop the new payment services;
- (ii) a description of the new payment services consisting of at least;
 - a. a visual representation of the customer journey when a PSU accesses its payment account via your PIS and/or an AIS (including any authentication steps that take place in your institution's domain);
 - b. an overview of the various PIS and/or AIS functionalities offered to the PSU specifying the type of information/accounts/products (both within the scope of PSD II and outside of the scope of PSD II) the PSU will have access to;
 - c. A brief overview of the technique(s) used to obtain access to the information/accounts/products (both within the scope of PSD II and outside of the scope of PSD II) from the ASPSP
 - d. A description of the implemented measures and procedures that demonstrate the institution's compliance with the obligations set out in article 48 of the Law 11 March 2018 when offering PIS, respectively article 98 of the Law of 11 March 2018 when offering AIS
- (iii) a general description of the impact on its business plan of the development and the carrying out of the new activities demonstrating the employment of appropriate and proportionate systems, resources and procedures to operate soundly; and
- (iv) the impact on its own funds requirements.

5.3 Organisation

The institution should provide a description of

- (i) the organisational changes following the new payment services (e.g. changes in departments, persons responsible etc...);
- (ii) the distribution channels that will be used for the new payment services; and
- (iii) a description of the relevant outsourcing agreements, if any.

5.4 Governance arrangements and internal control mechanisms

The institution should provide a description of the initial approval process and subsequent changes in its governance arrangements and internal control mechanisms following the developments of the new payment services.

The following items may be included in this description:

- risk & compliance mapping and subsequent risk management and follow up by the compliance function
- the procedures put in place to carry out controls (frequency, with the branches, if any, etc...)
- the measures taken to comply with art. 48 and/or art. 98 of the Belgian law of 11 March 2018

5.5 AML/CFT arrangements¹²

The institution should provide a description of its assessment of the money laundering and terrorist financing risk associated with the new payment services and the measures it will put in place to mitigate the risks and comply with the applicable AML/CFT obligations (including those put in place with its branches).

¹² This section is not applicable if the newly carried out activity is limited to AIS only.

6 OTHER GENERAL REMARKS

Please indicate any other concerns, issues or hurdles you may have identified or encountered or will encounter with respect to the implementation of the PSD2 requirements that are not covered above.

7 DECLARATION BY THE INSTITUTION

ACTING IN MY CAPACITY:

- AS CHIEF EXECUTIVE OFFICER
- AS AN EXECUTIVE DIRECTOR
- AS CHAIRMAN OF THE BOARD OF DIRECTORS
- AS A SENIOR MANAGER (CEO -1 LEVEL)

OF

I, THE UNDERSIGNED,

AFTER HAVING MADE THE USUAL VERIFICATIONS, HEREBY DECLARE THAT THE INFORMATION PROVIDED IN THIS FORM AND ITS ATTACHMENTS IS TRUE, COMPLETE, ACCURATE AND UP TO DATE

DATE, TITLE AND SIGNATURE

.....