FSMA Privacy Policy for banking service providers

This Privacy Policy sets out how the Financial Services and Markets Authority, located at 12-14 rue du Congrès/Congresstraat, 1000 Brussels and registered with the Crossroads Bank for Enterprises under number 0544.279.965 (hereafter "the FSMA" or "we"), as data controller, processes personal data of banking service providers as part of its supervision of compliance with the Law of 22 April 2019 introducing a banker's oath and a disciplinary regime for the banking sector, and its implementing royal decrees and regulations (hereafter referred to jointly as "the legislation on the banker's oath").

For more information about the legislation on the banker's oath, about the obligations arising specifically therefrom for banking service providers and for more detailed explanations of certain concepts used in this Privacy Policy, please see the various Frequently Asked Questions (FAQs) about the banker's oath and the disciplinary regime for banking service providers that are grouped by theme on the FSMA website.

With regard to other data processing activities or general information on the processing of personal data by the FSMA, please see the FSMA's general Privacy Policy or, where applicable, another specific privacy policy available on the website. As regards the use of cookies on the FSMA websites, please see the FSMA's Cookie Policy.

1. To whom does this Privacy Policy apply?

This Privacy Policy is addressed to banking service providers, as defined in the legislation on the banker's oath. For a list of the various categories of banking service providers, see the question "Who is subject to the banker's oath?" under the section "Scope" in the Frequently Asked Questions (FAQs) on the banker's oath and the disciplinary regime for banking service providers.

The concept of "banking service providers" also includes, where applicable, former banking service providers who either recently left their positions and are included on the lists of banking service providers drawn up by credit institutions, as described in this Privacy Policy, or who were banking service providers at the time of the actions that are the subject of a complaint, disciplinary proceedings or disciplinary sanctions as described in this Privacy Policy.

Lastly, with regard to the issuance by the FSMA of the certificate of "the absence of professional ban" (see below), this Privacy Policy also applies to candidate banking service providers who may request such a certificate in the context of their application to work at a credit institution or banking agent in order to be able to carry out one or more activities of a banking service provider.

2. What kind of personal data of banking service providers does the FSMA process, for what purposes and on what legal basis?

The FSMA processes personal data of banking service providers in order to fulfil its legal task to contribute to ensuring compliance with the legislation on the banker's oath. This data processing is consequently necessary for the performance of tasks carried out in the public interest and entrusted to the FSMA. These tasks and the associated processing of personal data are set out in greater detail below for each category.

The FSMA may (further) use these data for other supervisory purposes as well, where the processing of such data is required for the performance of other tasks carried out in the public interest as assigned to it by national or European laws or regulations. This is the case, for example, as regards its

assessments in connection with the fit and proper requirements in view of regulated functions (see also the specific FSMA Privacy Policy for its fit and proper assessments for regulated functions).

1. ***Lists of banking service providers***

Credit institutions are required to draw up lists of banking service providers who work for them or act on their account, and these lists must be submitted every six months to the FSMA. In principle, credit institutions should already have informed banking service providers of this legal obligation and the requirement to communicate the relevant data to the FSMA (as recipient of these data).

The FSMA processes the personal data it receives about banking service providers while collecting and managing these lists.

The following categories of personal data are processed:

- **Identification information**:
  - surname, first name and (where applicable) middle name;
  - date of birth;
  - the identification number (identifier) issued by the credit institution;

- **Professional information**:
  - name of the credit institution where the banking service provider works or for whose account he or she is acting;
  - (where applicable) name of the banking agent(s) where the banking service provider is active;
  - category(ies) of banking service providers to which the banking service provider belongs, as from which date and (where applicable) until which date;
  - (where applicable) date the oath was taken;
  - company number (only for banking service providers who are themselves banking agents registered with the FSMA as a natural person).

As indicated above, the FSMA receives these personal data from the credit institutions.

2. ***The oath-taking at the FSMA***

In addition, the FSMA also processes the personal data of banking service providers who are required to take the oath at the FSMA. It processes these data in order to manage the registrations for the oath-taking, to organise the oath-taking sessions and to issue a certificate of the oath having been taken.

The following categories of personal data are processed:

- **Identification information**:
  - surname and first name;
  - date of birth;
  - internal reference number for the taking of the oath.

  At the beginning of the oath-taking session, the banking service provider will be asked to provide a proof of identity (e.g. the eID) in order to be able to verify that the person present is in fact the registered banking service provider. At the end of the oath-taking session, the banking service provider will be asked for a signature, to confirm his or her presence.

- **Professional information**:

- (professional) contact information (optional phone number solely to be used in case of emergency and optional email address for communications relating (i) to the registration for the oath-taking and (ii) to the digital delivery of the certificate of the oath having been taken);
- name of the credit institution or banking agent (possibly multiple entities) where the banking service provider is active at that time;
- company number (only for banking service providers who are themselves banking agents registered with the FSMA as a natural person).

With the exception of the internal reference number issued by the FSMA for the oath-taking, the FSMA receives these personal data mainly from the banking service providers themselves upon registering for the oath-taking. Registration takes place in principle online via eID/itsme by using an application provided by the FSMA.

The oath is normally taken on the premises of the FSMA. General information about the processing of personal data gathered when visiting the FSMA (e.g. via the images recorded by the security cameras in the building and the parking garage, when using the WiFi network, etc.) can be found in the general Privacy Policy of the FSMA.

3. The complaints channel, disciplinary proceedings and the disciplinary register

a) The complaints channel

In accordance with the legislation on the banker's oath, the FSMA has made available a complaints channel (available in French and Dutch only) that allows anyone to lodge a complaint regarding compliance by banking service providers (i) with the obligation to take the oath and (ii) with the individual rules of conduct.

If the FSMA receives a complaint via this channel, it will process the personal data of the banking service provider in question as entered on the complaint form. The FSMA processes these data for the purposes of receiving, investigating and following up on the complaint. For cases where a complaint gives rise to the opening of a disciplinary investigation, please see point b) below. Not all complaints, however, necessarily lead to the opening of a disciplinary investigation, and not every such investigation is initiated in response to a complaint (but it may also take place where the FSMA identifies serious indications of infringements in the course of carrying out its other legal duties).

Where complaints are received via the complaints channel, the following categories of personal data of the banking service provider concerned are processed:

- **Identification information**: surname and first name;

- **Professional information**:
  - name of the credit institution or banking agent where the banking service provider was active at the time of the actions that are the subject of the complaint;
  - position of the banking service provider at the above-mentioned entity;

- **Other information** on the banking service provider that is provided in the description of the complaint, in the additional relevant information provided or in the appended evidentiary material.

The FSMA receives these personal data from the person who lodged the complaint. As regards the processing of personal data of a person lodging a complaint, please see the question "How does the FSMA process personal data collected in the context of a complaint relating to the banker's oath?" under the section "Complaints channel" in the Frequently Asked Questions (FAQs) on the banker's oath and the disciplinary regime for banking service providers.

b) Disciplinary proceedings

If there are serious indications of infringements relating to the oath-taking and/or to compliance with the individual rules of conduct, the (Deputy) Investigations Officer of the FSMA will investigate the relevant actions. As explained above, this investigation may be carried out in response to a complaint (see above) or if such indications are identified by the FSMA in the course of carrying out its other legal duties. After completing the investigation, the FSMA may decide to impose a disciplinary sanction.

The FSMA processes personal data of the banking service provider in order to (i) conduct the investigation (in accordance with the rules of procedure laid down in the applicable legislation and taking into account the rights of defence), and (ii) impose a disciplinary sanction where applicable.

The following categories of personal data are processed:

- **Identification information**:
  - surname, first name and (where applicable) middle name;
  - date of birth;
  - contact details;

- **Professional information**:
  - name of the credit institution or banking agent where the banking service provider was active at the time of the actions being investigated;
  - company number (only for banking service providers who at the time of the actions being investigated were themselves banking agents registered with the FSMA as a natural person);
  - position and/or category(ies) of the banking service provider;

- **Other information** on the banking service provider that appears in the disciplinary dossier, such as
  - additional information gained from the facts identified, the investigations conducted or remarks by the banking service provider;
  - information on the follow-up to the investigation (including, where applicable, on the (nature of the) disciplinary sanction imposed by the FSMA).

The FSMA receives this information in the first instance from third parties, such as a person lodging a complaint, another supervisory authority, persons who are being questioned in the course of a disciplinary investigation or the entity where the banking service provider is or was working. The FSMA also receives personal data from the banking service provider him/herself (for example, in a defence put up against any charges) or from its own enquiries.

The disciplinary sanctions that the FSMA may impose will be published on its website, albeit without the identification information of the banking service provider in question.

c) Keeping a disciplinary register

The FSMA also processes personal data of banking service providers on whom it imposed a disciplinary sanction for purposes of keeping a register of such sanctions, as required under the legislation on the banker's oath.

The register contains the following categories of personal data:

- **Identification information**:
  - surname, first name and (where applicable) middle name;
  - date of birth;

- **Information on the disciplinary sanction imposed:**
  - type of disciplinary sanction (including, where applicable, the nature and duration of the professional ban or the description of the mandatory training to be taken);
  - date when the disciplinary sanction was imposed.

The register itself is not made public, nor is it made available to the credit institutions/banking agents. It is a source of information used by the FSMA to issue a certificate attesting that no professional ban had been imposed (see point 4 below: "Obtaining a certificate that no professional ban has been imposed").

4. Obtaining a certificate that no professional ban has been imposed

Each person who seeks to carry out the activities of a banking service provider may, in accordance with the legislation on the banker's oath, ask the FSMA for a certificate that no professional ban has been imposed on him or her. In this case, the FSMA serves as a "one-stop shop" where information is centralised regarding cases where, in the Belgian banking sector, a professional ban has been imposed.

In order to be able to issue such certificates correctly, the FSMA processes personal data of the candidate banking service providers who request a certificate, as well as of the persons (including banking service providers) on whom a professional ban has been imposed, in order to check whether an ongoing professional ban has been imposed on the person requesting the certificate.

The following categories of personal data are processed:

a) ON CANDIDATE BANKING SERVICE PROVIDERS WHO REQUEST A CERTIFICATE:

Identification data: surname, first name and date of birth

The FSMA receives these data from the candidate banking service provider him- or herself. The certificate is issued automatically, in principle, via an online request after identification via eID/itsme by using an application provided by the FSMA.

b) ON THE PERSONS (INCLUDING BANKING SERVICE PROVIDERS) ON WHOM A PROFESSIONAL BAN HAS BEEN IMPOSED:

- **Identification information:**
  - surname, first name and (where applicable) middle name;
  - date of birth;

- **Professional information:**
  - name of the entity where the person was active at the time of the actions that gave rise to the professional ban;

- company number (only if the professional ban was imposed on a person who at the time of the actions in question was him- or herself a banking agent registered with the FSMA as a natural person);

- **Information on the professional ban imposed:**
  - the authority that imposed the ban (i.e. the FSMA, the NBB or the ECB);
  - date of the professional ban;
  - nature of the prohibited activities;
  - duration of the professional ban.

  If the ban was not imposed by the FSMA, the latter shall obtain these data from the NBB.

3. How long does the FSMA store your personal data?

As regards the handling of complaints, the personal data relating to a banking service provider against whom a complaint was lodged but that did not give rise to a disciplinary proceeding, will be stored for 5 years (as from the date the complaint was received).

If disciplinary proceedings were initiated against the banking service provider, the personal data may be stored for longer, taking into account the period for appeal against the disciplinary decisions taken by the FSMA or the statute of limitations for liability claims.

In addition, the data of persons who intend to carry out the activities of a banking service provider and have therefore asked the FSMA for a certificate indicating that they are not under any professional ban, will – after the issue of this certificate – be stored as long as necessary to prevent any fraud with such certificates (and, where applicable, to be able to impose an administrative sanction if it should appear that a person does not comply with the professional ban imposed by the FSMA).

In each of the other cases delineated in question 2 (see above), the personal data will in any case be stored as long as the person continues to work as a banking service provider. Thereafter, these data may continue to be stored as long as is necessary for the FSMA to fulfil its tasks carried out in the public interest, taking into account, among other things:

- the fact that a banking service provider may once again be active in the sector in the near future (whether or not in a different regulated function), in which case it is important to know the history of his or her dossier;
- the fact that even after a person is no longer working as a banking service provider, complaints may be lodged or actions brought to the FSMA's attention. In such a case, the FSMA must be able to check whether the person concerned was on the list of banking service providers at the time of the actions, and for example, has fulfilled the obligation to take the banker's oath.

Finally, the FSMA, as a federal authority, is subject to the Law of 24 June 1955 on the National Archives and is thus not at liberty to simply destroy documents in its possession. Consequently, some personal information is kept longer in documents that the FSMA must preserve for archiving purposes in the public interest, albeit with the appropriate guarantees.

4. With whom does the FSMA share your personal data?

Within the limits of its obligation of professional secrecy and, where necessary and applicable, the FSMA may, as part of its supervision of compliance with the legislation on the banker's oath, share the personal data of banking service providers with:

- the NBB or the prudential supervisor in another member state, for persons to whom a fit and proper requirement at the credit institution applies, in particular where the definitive investigation report by the (Deputy) Investigations Officer of the FSMA concludes that there has been an infringement and the FSMA is required, under the legislation on the banker's oath, to inform the competent prudential authority;
- the credit institution or banking agent where the banking service provider is or was active, for instance where the (Deputy) Investigations Officer obtains advice from the entity in question;
- other third parties that are asked for information or that are heard in the context of a disciplinary investigation;
- the competent judicial authorities, for example if the FSMA takes a disciplinary decision that gives rise to court proceedings (such as an appeal against a disciplinary decision lodged with the Council of State).

More general information about the cases where the FSMA shares personal data with third parties and information about the sharing of personal data with (third party) service providers whose services are used by the FSMA (such as ICT service providers), is available in the general Privacy Policy of the FSMA (under the questions "With whom do we share your data?" and "Does the FSMA process your data outside the European Economic Area?").

5. What are your privacy rights and how can you exercise them?

Under the General Data Protection Regulation (GDPR), you have a set of rights as regards your personal data. In this connection, you may request the FSMA to access, rectify or delete your personal data. In addition, you have the right to object to the processing of your data for certain specific and legitimate reasons, and in certain cases you may request that the processing of your personal data be restricted.

However, the FSMA is not required to take action on such requests in all cases. Some of these rights have a very specific scope or are subject, in the GDPR, to special conditions or exceptions (such as exceptions to your rights in cases of public interest). Moreover, because of the FSMA's obligation of professional secrecy, you will not be able to exercise certain rights (such as the right of access, rectification and objection) if your personal data were not submitted to the FSMA by yourself (Article 46*bis* of the Law of 2 August 2002 on the supervision of the financial sector and on financial services).

If you wish to exercise your privacy rights, please send your request by email to dataprotection@fsma.be or by post to the FSMA's Data Protection Officer. For more information about the procedure to follow and about your privacy rights in general, please see the FSMA's general Privacy Policy.

Finally, if you consider that your rights have not been respected, you may at any time lodge a complaint with the Data Protection Authority, Rue de la Presse/Drukpersstraat 35, 1000 Brussels, email: contact@apd-gba.be (see also https://www.dataprotectionauthority.be).

6. How can you be updated as to any amendments to this Privacy Policy?

This Policy may be amended. You can consult the most recent version of the Privacy Policy at any time on our website.

This Privacy Policy was last amended on 4 June 2025.

7. How can you contact us?

The FSMA has a Data Protection Officer (DPO), who is your contact person for any questions or requests you may have regarding the processing of your personal data.

If you have questions about this Privacy Policy or want to exercise your rights regarding the processing of your personal data, you can contact us:

- via email to dataprotection@fsma.be; or
- by letter to:

Financial Services and Markets Authority (FSMA)
Attn: Data Protection Officer
Rue du Congrès / Congresstraat 12-14
1000 Brussels (Belgium)