

Privacy regulations Foundation for Banking Ethics Enforcement

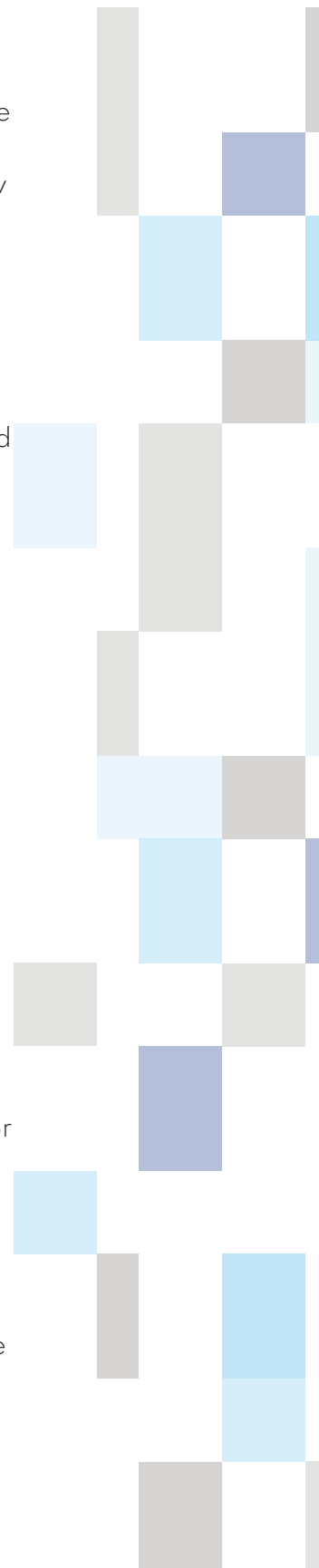
Content


1	Definitions	2
2	Scope of these Privacy Regulations	3
3	Controller	3
4	Purposes and basis	4
5	Categories of Data Subjects	4
6	Categories of Personal Data	5
7	Quality	6
8	Security	6
9	Retention periods	7
10	Secrecy and awareness	7
11	Inclusion in and consultation of the Disciplinary Register	7
12	Anonymising Publications	8
13	Informing and providing	8
14	Right of inspection	9
15	Right to rectification and supplementation	9
16	Right to restriction of processing	10
17	Right to data portability	10
18	Right to oblivion/deletion	11
19	Right to human intervention	11
20	Right of objection	11
21	PG Complaints	11
22	Adoption and amendments	12
23	Final provision	12



1 Definitions

- 1.1 **Managing Director:** the Managing Director to be appointed by the Foundation;
- 1.2 **AP:** the Data Protection Authority;
- 1.3 **Bank:** a Dutch or European bank whose employees fall within the scope of the Rules of Conduct under the Financial Supervision Act (Wft) and/or under agreements with the Foundation and to which disciplinary law applies;
- 1.4 **Sworn Person:** a natural person who has taken the banking oath as referred to in the Financial Sector Oath or Solemn Declaration Regulations 2015 (associated with the Financial Supervision Act);
- 1.5 **Board:** the board of the Foundation for Banking Ethics Enforcement;
- 1.6 **Data Subject:** the person to whom Personal Data relates;
- 1.7 **Affected Bank:** the bank with which the Respondent is or was employed at the time of the conduct to which the Report or Complaint relates;
- 1.8 **Special Personal Data:** Personal Data revealing, for example, racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and, for example, data regarding health, or someone's sexual orientation (in accordance with Article 9(1) GDPR);
- 1.9 **Appeals Committee:** the Appeals Committee referred to in the Disciplinary Regulations for the Banking Sector;
- 1.10 **Data Breach:** a breach relating to Personal Data. Security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to data transmitted, stored or processed otherwise (Article 4(12) GDPR);
- 1.11 **Third Party:** a natural or legal person other than the Data Subject, the Controller, the Processor, or the persons authorised under the direct authority of the Controller or the Processor to process Personal Data;
- 1.12 **Expert:** any person with extensive experience in the banking sector;
- 1.13 **Data Protection Officer (DPO):** the independent supervisor of the Foundation's compliance with privacy legislation;
- 1.14 **Complaint:** a complaint substantiated in writing by the Managing Director in accordance with article 2.1.2 the Disciplinary Regulations for the Banking Sector;
- 1.15 **Measure:** the (conditional) measure that has become irrevocable under the Disciplinary Regulations, which also includes an amicable settlement as referred to in the Disciplinary Regulations;
- 1.16 **Notifier:** the person filing a Report;
- 1.17 **Report:** a written, reasoned report in accordance with Article 2.1 of the Disciplinary Regulations for the Banking Sector;
- 1.18 **Personal data:** any data relating to an identified or identifiable natural person (Article 4(1) GDPR);



- 
- 1.19 **Publication:** a published ruling and/or decision as referred to in the Disciplinary Regulations;
 - 1.20 **PG Complaint** a complaint by a Data Subject regarding the Foundation's handling of his/her Personal Data or a complaint about the Foundation's conduct; a PG Complaint is subject to the Complaints Regulations of the Foundation for Banking Ethics Enforcement;
 - 1.21 **Privacy Regulations:** these Privacy Regulations of the Foundation for Banking Ethics Enforcement;
 - 1.22 **Protocol: Protocol of the** Disciplinary Register of the Foundation for Banking Ethics Enforcement;
 - 1.23 **Foundation:** Foundation for Banking Ethics Enforcement;
 - 1.24 **Disciplinary Committee:** the Disciplinary Committee referred to in the Disciplinary Regulations;
 - 1.25 **Disciplinary Register:** the register in which disciplinary measures that have become irrevocable for a definite period are recorded and kept accessible to the Dutch Banking Sector;
 - 1.26 **Disciplinary Regulations** disciplinary regulations of the banking sector;
 - 1.27 **Respondent:** a Sworn Person against whom a Complaint has been filed;
 - 1.28 **Processor:** a natural or legal person, organisation, or body which processes Personal Data on behalf of the Controller (Article 4(8) GDPR);
 - 1.29 **Controller:** a natural or legal person, an organisation or a body which, individually or together with others, determines the purpose of and the means for processing Personal Data (Article 4(7) GDPR);
 - 1.30 **Processing of Personal Data:** any operation or set of operations involving Personal Data (Article 4(2) GDPR).

2 Scope of these Privacy Regulations

- 2.1 These Privacy Regulations apply to all processing of Personal Data within the Foundation.
- 2.2 An exception is the processing of Personal Data in the context of the Disciplinary Register. Such processing is subject to the Protocol of the Disciplinary Register.

3 Controller

- 3.1 The controller of the data processing is the Foundation, with offices at Beursplein 5, 1012 JW Amsterdam
- 3.2 The Foundation has established the position of a Data Protection Officer to monitor the guidelines regarding the processing and protection of Personal Data. This has been reported to the Data Protection Authority.



4 Purposes and basis

- 4.1** The Foundation processes Personal Data for the following purposes:
- maintaining an independent disciplinary tribunal to handle complaints against a Sworn Person;
 - the application and implementation of disciplinary proceedings as laid down in the Disciplinary Regulations; this means: the reporting procedure, the complaint procedure, the procedure before the Disciplinary Committee, the review procedure and the procedure before the Appeals Committee;
 - maintaining the Disciplinary Register to ensure the effectiveness of disciplinary law in banking;
 - doing everything related or conducive to the foregoing.
- 4.2** The Foundation processes Personal Data exclusively:
- where such processing is necessary to comply with the legal obligation under Section 3:17c of the Financial Supervision Act (Wft). Pursuant to Section 3:17c Wft, there is a legal obligation to provide disciplinary regulations. Their implementation is entrusted to the Foundation;
 - where such processing is necessary for the performance of the task carried out in the public interest of providing disciplinary regulations within the banking sector;
 - when such processing is necessary because of a legitimate interest of the Foundation or of a third party, unless that interest conflicts with the interest of the person whose data is being processed and the latter interest takes precedence.

5 Categories of Data Subjects

- 5.1** The Foundation at any rate processes Personal Data of the following categories of Data Subjects:
- Managing Director and their staff;
 - Sworn Person / respondent;
 - Contact at the Relevant Bank;
 - Expert or witness;
 - Members of the Disciplinary and Appeals Committees;
 - Members of the Board;
 - Notifier
 - Persons involved in the Report and/or Complaint and/or its handling;
 - Secretary of the Disciplinary and Appeals Committees.



6 Categories of Personal Data

6.1 The following categories of Personal Data can be processed by the Foundation:

- Report data: This is Personal Data relating to the Report, including the first and last name, initials, gender, telephone number, email address and country of the Notifier; first and last name, initials, gender, telephone number, email address, bank, position, department, office location of the Sworn Person; a description of the Sworn Person's conduct, when it took place and what standard is alleged to have been breached. Sensitive Personal Data such as financial data may also be processed.

In exceptional cases, special Personal Data regarding the Notifier may form part of the reporting data. This special data will only be processed if the processing thereof is necessary for the investigation and disciplinary proceedings.

The report data is provided by the Notifier.

- Complaint data: This is Personal Data relating to the Complaint, investigation, review procedure, handling of the Complaint, evidence, decision, Measure, challenge, defence and appeal and communication related thereto.
- Personal Data processed for a Complaint includes, but is not limited to, the following Personal Data: personal details, contact details, work details and information of Data Subjects and additional Personal Data to the extent necessary to investigate the Report or Complaint. Sensitive Personal Data such as financial data may be processed. In exceptional cases, special Personal Data or criminal data regarding the Sworn Person/Respondent may form part of the complaint data. The Foundation has obtained permission from the Data Protection Authority for the processing of criminal data for the purpose of disciplinary proceedings. The Complaint details are provided by the Notifier, Data Subjects or the Relevant Bank.
- Details of members of the Board, the Disciplinary Committee and the Appeals Committee, the secretary of the Disciplinary Committee and the secretary of the Appeals Committee: these include but are not limited to first and surname, initials, gender, titles, date of birth, place of residence and/or work address, postal code, place of residence, telephone number, e-mail address, bank account number. These details are obtained from the Data Subjects.
- Other contacts: when a Data Subject contacts the Foundation by telephone, email or post, Personal Data may be processed such as name, (email) address, phone number, and other data shared by the Data Subject, depending on the content of the contact.



6.2 The Categories of Personal Data processed within the Foundation are recorded in a processing register.

7 Quality

7.1 Personal Data is processed in a proper and careful manner in accordance with the law, the Disciplinary Regulations and these Privacy Regulations. Personal Data is only processed insofar as it is adequate, relevant and not excessive in relation to the purposes referred to in Article 4 of the Privacy Regulations. If data that is provided are not relevant or excessive, the Foundation will refrain from processing such data or include it in the Report or Complaint in anonymous form. The Foundation will take organisational and technical measures to achieve this.

7.2 Personal Data is processed only insofar as it is true and accurate in view of the purposes referred to in Article 4 Privacy Regulations. If the data appears to be incorrect, an amendment will be included in the file.

7.3 In regard to documents that still contain incorrect Personal Data, however, such data can be retained if this is necessary for making a decision. This is for the sake of due process during disciplinary proceedings.

8 Security

8.1 The Foundation implements appropriate technical and organisational measures to secure Personal Data against loss or against any form of unlawful processing. Taking into account the state of the art and the costs of implementation, these measures shall ensure an appropriate level of security in view of the risks presented by the processing and the nature of data to be protected.

8.2 The Foundation shall ensure that Processors provide sufficient guarantees in respect of technical and organisational security measures relating to the processing operations. The Foundation will monitor compliance with those measures. The Foundation will enter into a processing agreement with its Processors.

8.3 The Foundation regularly conducts a 'Data Protection Impact Assessment' (DPIA). A DPIA involves identifying privacy risks and taking measures where necessary. The Foundation also conducts a DPIA when it changes its working methods, before implementing the proposed change.

8.4 Employees who process Personal Data are required to report a data breach immediately in accordance with the Data Breach Notification Protocol of the Foundation. The Foundation is required to report data breaches to the Data Protection Authority if there is a data breach that leads to a significant likelihood of adverse consequences for the protection of Personal Data.

9 Retention periods

9.1 Except in the situation described in Article 9.2, Personal Data shall not be retained longer than necessary for the fulfilment of the purposes for which it is collected or subsequently processed. Where applicable, Personal Data shall be converted into a form that renders identification of the data subject impossible.

9.2 Following completion of the disciplinary proceedings, the case file will be kept for another seven (7) years, after which the case file will be permanently destroyed. Measures are recorded in the Disciplinary Register for the period specified in the Disciplinary Regulations and in the Disciplinary Register Protocol.

10 Secrecy and awareness

10.1 Anyone who has access to Personal Data as part of their work for the Foundation must sign a confidentiality agreement. This includes the General Director, the Secretary and the members of the Board, the Disciplinary Committee and the Appeals Committee, the Expert and anyone involved in the handling of a Report and Complaint. Anyone who has access to Personal Data in the context of their work shall only process Personal Data to the extent necessary for the performance of the relevant job, work or task.

10.2 The Foundation shall ensure that anyone who has access to Personal Data in the course of their work for the Foundation treats it with care and has sufficient knowledge to do so.

11 Inclusion in and consultation of the Disciplinary Register

11.1 Inclusion in and consultation of the Disciplinary Register shall take place solely in accordance with the provisions of the Protocol.



12 Anonymising Publications

12.1 As provided in the Disciplinary Regulations, the Foundation may publish a ruling, redacting identifying information as it deems fit.

13 Informing and providing

13.1 In accordance with the Disciplinary Regulations, the Foundation shall inform the Sworn Person and the Relevant Bank during the proceedings or arguments in writing within four weeks that Personal Data concerning him or her is being processed. The notice shall include an indication of the purpose of the processing and information regarding the rights of data subjects and the right of complaint.

The Sworn Person shall be informed of the content of the reported data, unless there are compelling interests based on which certain data cannot be shared.

13.2 If Personal Data of any third Data Subject is processed by the Foundation, the Foundation will only inform the Data Subject that Personal Data relating to him or her is being processed if this is permissible in view of the interests of the Data Subject (including the Notifier and the Sworn Person/Respondent). In addition, the Foundation will only inform the third Data Subject if this does not prove impossible and/or does not require a disproportionate effort. The notice shall contain an indication of the purpose of the processing.

13.3 Reported data and Complaint data may be provided to members of the Disciplinary Committee and its secretary and to the Appeals Committee and its secretary. These persons are also bound by these Privacy Regulations.

13.4 The Foundation shall only provide Personal Data to Third Parties if there is a basis for doing so as referred to in Article 4 of these Privacy Regulations or if there is a legal obligation to do so. In all other situations, data will not be shared with Third Parties.





14 Right of inspection

14.1 A Data Subject may ask the Foundation for access to their Personal Data.

14.2 The Foundation will process the Data Subject's request if the Data Subject's identity can be established with sufficient certainty. The Foundation will do this first on the basis of the data already known. In order to confirm the Complainant's email address, a verification email will be sent to the Complainant's email address known to the Foundation. Only in extreme cases will a secure copy of a legal identity document be requested. If the Foundation cannot establish that the person making the request is actually the Data Subject, the Foundation may request the Data Subject to identify themselves in person. If the identity of the Data Subject cannot be established or if abuse is suspected, a request for inspection will not be processed.

14.3 Within four weeks of receiving the request, the Foundation shall inform the Data Subject in writing whether Personal Data concerning him or her is being processed. Where a request is highly complex or very extensive, the Foundation may extend this period by up to two months. If Personal Data of a Data Subject is processed, the Foundation will provide a full overview of the Personal Data processed by the Foundation processed Personal Data about Data Subject, unless there are grounds on the basis of which a request for inspection cannot be honoured.

14.4 If the Foundation refuses the request, it will give reasons for such refusal. If and to the extent that this right to access also affects the rights and freedoms of others, for example if the documents also include Personal Data of others than the Data Subject, the Foundation may restrict the right of access.

15 Right to rectification and supplementation

15.1 A Data Subject may request the Foundation to amend, correct, supplement or block their Personal Data if such data is factually inaccurate, incomplete or irrelevant for the purpose of processing, or is processed in breach of a legal requirement.

15.2 The Foundation shall consider the request in accordance with Article 14.2 of these Privacy Regulations.

15.3 Within four weeks of receipt, the Foundation shall inform the Data Subject in writing whether, or to what extent, it will comply with the request. If a request is highly complex or very extensive, the Foundation may extend this period by a maximum of two months. If the Foundation refuses the request, it will give reasons for its refusal.

15.4 The Foundation shall ensure that a decision to amend, correct, supplement or block Personal Data is implemented as soon as possible

15.5 If the Foundation complies with the Data Subject's request and modifies, corrects, completes or shields their data, the Foundation will also inform the third parties, e.g. Banks, to whom this data was provided prior thereto, unless this is impossible or requires disproportionate effort.

16 Right to restriction of processing

16.1 A Data Subject has the right to submit a request to the Foundation to restrict the processing of Personal Data if it may be inaccurate, unlawfully processed, no longer necessary for the purposes of processing or an objection has been raised against the processing of Personal Data of a Data Subject.

16.2 The Foundation shall consider the request in accordance with Article 14.2 of these Privacy Regulations.

16.3 The Foundation shall inform the Data Subject in writing whether, or to what extent, it will comply with the request within four weeks of receipt. If a request is highly complex or very extensive, the Foundation may extend this period by a maximum of two months. If the Foundation refuses the request, it will give reasons for its refusal.

16.4 The Foundation will ensure that a decision to restrict processing is implemented as soon as possible.

17 Right to data portability

17.1 Under the GDPR, a Data Subject may submit a request to transfer Personal Data; the right to data portability. Data Subject may ask the Foundation to disclose Personal Data to the Data Subject or to a third party. This right only applies if Personal Data is processed on the basis of consent or performance of an agreement. Personal Data is mainly processed by the Foundation on the basis of a legal obligation, the right to transfer Personal Data does not apply to this.

18 Right to oblivion/deletion

18.1 If a Data Subject believes that the Processing of Personal Data is no longer necessary, if consent to the Processing is withdrawn, if an objection is made to the Processing, if the Personal Data is processed unlawfully or if the retention period has expired, the Data Subject may request the Foundation to delete the Personal Data. As the Foundation mostly processes Personal Data on the basis of a legal obligation, the right to oblivion can often not be invoked.

19 Right to human intervention

19.1 When an organisation makes a decision based on automatically processed data, the GDPR gives the Data Subject the right to human intervention. The decision-making at the Foundation is not automated, and therefore this right does not apply to the Processing carried out by the Foundation.

20 Right of objection

20.1 A Data Subject may object to the processing of Personal Data by the Foundation. The Foundation will cease the processing of Personal Data against which the objection is lodged as soon as possible, unless there are compelling legitimate grounds which oppose this and which outweigh the interests of the Data Subject. If the Foundation refuses the Data Subject's request, it will give reasons for such refusal.

21 PG Complaints

21.1 If a Data Subject believes that the Foundation has acted in breach of the Privacy Regulations, the Data Subject may file a complaint with the Data Protection Officer. This can be done by e-mail at privacy@disciplinary-law-banks.nl or by postal address: Tucht recht Banken, attn. the Data Protection Officer, Postbus 3861, 1001 AR Amsterdam.

21.2 If a Data Subject believes that the Foundation has acted in breach of the Disciplinary Regulations, the Protocol, the law and/or has treated him incorrectly, the Data Subject may also file a complaint in accordance with the Complaints Procedure of the Foundation for Banking Ethics Enforcement.

21.3 If, in the Data Subject's opinion, a complaint has not been dealt with properly, the Data Subject may turn to the Data Protection Authority or the courts.



22 Adoption and amendments

- 22.1 These Privacy Regulations have been adopted by the Foundation and may be amended by the Foundation
- 22.2 The Foundation regularly reviews whether the Privacy Regulations are still adequate. Each amendment is provided with a date.
- 22.3 Once a year, the Foundation conducts an internal review of these Privacy Regulations.
- 22.4 If a situation arises that is not described in these Privacy Regulations, the Foundation will take the necessary measures, and it will assess whether these Privacy Regulations need to be supplemented or amended.

23 Final provision

- 23.1 This document is cited as the Privacy Regulations of the Foundation for Banking Ethics Enforcement and shall come into effect on 1 August 2024.