



**Tucht recht**  
**Banken**

**Privacy Statement**  
**Foundation for Banking Ethics Enforcement**

1 July 2019

**Contents**

**Article 1: Definitions..... 3**

**Article 3: Party responsible for processing and Processor ..... 5**

**Article 4: Purposes and grounds ..... 5**

**Article 5: Categories of Relevant Individuals..... 5**

**Article 6: Categories of Personal Data ..... 6**

**Article 7: Quality ..... 7**

**Article 8: Security ..... 7**

**Article 9: Storage period ..... 8**

**Article 10: Confidentiality and awareness..... 8**

**Article 11: Inclusion and consulting the Disciplinary Register ..... 8**

**Article 12: Publishing anonymous data..... 8**

**Article 13: Information and provision ..... 8**

**Article 14: Right of review ..... 9**

**Article 15: Right to correction, addition, and deletion ..... 9**

**Article 16: Objection ..... 10**

**Article 17: Complaints..... 10**

**Article 18: Approval and amendments ..... 10**

**Article 19: Final provision ..... 11**

## Article 1: Definitions

- 1.1 **General Director:** the General Director appointed by the Foundation;
- 1.2 **AP:** the Personal Data Authority;
- 1.3 **Bank:** a Bank whereby the employees of said Bank are subject to the scope of the Banking Sector Code of Conduct in accordance with the Financial Supervision Act, and which is subject to ethics enforcement;
- 1.4 **Certified Individual:** a natural person who has signed an agreement as defined in the Code of Conduct for the banking sector;
- 1.5 **Board:** the Board of Managers of the Foundation for Banking Ethics Enforcement;
- 1.6 **Relevant Individual:** the person to whom the personal data pertain;
- 1.7 **Relevant Bank:** the Bank at which the Defendant worked or was present when the behaviour to which the Complaint or Report refers took place;
- 1.8 **Special personal data:** Personal data from which can be derived an individual's race or ethnic background, political opinions, religious or philosophical convictions, or membership in a labour union, as well as data pertaining to an individual's health or sexual orientation (in accordance with Art. 9 section 1 AVG);
- 1.9 **Appeals Committee:** the Appeals Committee as referred to in the Banking Sector Ethics Regulations;
- 1.10 **Data leak:** any incident in which Personal Data are unintentionally destroyed or lost, changed, provided or made available.
- 1.11 **Third party:** a natural person or legal entity, which is not the Relevant Individual, the party responsible for processing the data, the Processor, or the persons authorised to process the Personal Data under the direct authority of the party responsible for processing the data or the Processor;
- 1.12 **Expert:** an individual who has extensive experience in the banking sector;
- 1.13 **DSI:** The Dutch Securities Institute Foundation;
- 1.14 **Complaint:** a written complaint submitted by the General Director in accordance with section 2.1.2 of the Banking Sector Ethics Regulations;
- 1.15 **Reporter:** the person who makes a report;
- 1.16 **Report:** a written report in accordance with Article 2.1 of the Ethics Regulations;
- 1.17 **Personal Data:** any data pertaining to an identified or identifiable natural person, including but not limited to: name, address, date of birth, gender, telephone number, e-mail address, and position;
- 1.18 **Publication:** a published statement and/or verdict as referred to in the Ethics Regulations;
- 1.19 **Privacy Statement:** this Privacy Statement issued by the Foundation for Banking Ethics Enforcement;
- 1.20 **Protocol:** the Foundation for Banking Ethics Enforcement Disciplinary Register Protocol;
- 1.21 **Disciplinary Measure:** a (conditional) irrevocable Measure implemented in accordance with the Ethics Regulations, which is also understood to include an amicable settlement as referred to in the Ethics Regulations;
- 1.22 **Foundation:** Foundation for Banking Ethics Enforcement, founded by the *Nederlandse Vereniging van Banken* (Dutch Banking Association);

- 1.23 **Enforcement Committee:** the Enforcement Committee as referred to in the Ethics Regulations;
- 1.24 **Disciplinary Register:** the register in which irrevocable disciplinary measures are administered and made available to the banking sector for a specified time period;
- 1.25 **Ethics Regulations:** The Banking Sector Ethics Regulations;
- 1.26 **Defendant:** a Certified Individual against whom a complaint has been filed;
- 1.27 **Processor:** the natural person or legal entity that processes Personal Data on behalf of the Foundation for Banking Ethics Enforcement. The Processor has an executive responsibility with regard to the activities of the Foundation for Banking Ethics Enforcement;
- 1.28 **Party responsible for processing data:** the entity which determines the purpose and resources for the processing of the Personal Data. In the context of this Privacy Statement, this is the Foundation for Banking Ethics Enforcement;
- 1.29 **Processing of Personal Data:** an activity or set of activities pertaining to Personal Data or a collection of Personal Data, such as collection, recording, organising, structuring, storing, editing or changing, requesting, consulting, using, providing by means of sending, publishing, or making available by other means, aligning or combining, protecting, deleting, or destroying data.

## **Article 2: Scope of this Privacy Statement**

- 2.1 This Privacy Statement applies to all processing of personal data by the Foundation.
- 2.2 The exception to this is the Processing of Personal Data in the context of the Disciplinary Register. This form of data processing is subject to the provisions of the Disciplinary Register Protocol.

## **Article 3: Party responsible for processing and Processor**

- 3.1 The party responsible for processing such data is the Foundation, with its statutory address at Beursplein 5, 1012 JW Amsterdam.
- 3.2 The Foundation has created the position of Data Protection Specialist in order to monitor the guidelines for processing and protecting personal data. This initiative was reported to the Personal Data Authority. The Data Protection Specialist can be contacted via [info@tuchtrechtbanken.nl](mailto:info@tuchtrechtbanken.nl) (attn.: Data Protection Specialist) or via the post at: Tuchtrecht Banken, attn.: Data Protection Specialist, Postbus 3861, 1001 AR Amsterdam.
- 3.3 DSI is the Processor of Personal Data in the implementation of the Foundation's duties. The Foundation and DSI have signed a processing agreement to that end.

## **Article 4: Purposes and grounds**

- 4.1 The Foundation processes Personal Data for the following purposes:
  - to maintain an independent disciplinary body to process Complaints regarding a Certified Individual.
  - the application and implementation of ethics law, as stipulated in the Ethics Regulations;  
This is understood to include: the reporting procedure, the complaint procedure, the Enforcement Committee procedure, the revision procedure, and the Appeals Committee procedure.
  - maintaining the Disciplinary Register in order to guarantee the effectiveness of banking supervision;
  - performing all activities pertaining to or in support of the above.
- 4.2 The Foundation processes Personal Data exclusively:
  - when such processing is necessary to comply with the legal obligation expressed in Art. 3:17 of the Financial Supervision Act (Wft). In accordance with Art. 3:17 Wft, banks in the Netherlands are legally required to have an ethics enforcement regulation. The enforcement of this provision is delegated to the Foundation;
  - when such processing is necessary to perform the task of the general interest, specifically providing an ethics enforcement regulation within the banking sector;
  - when such processing is necessary due to a justified interest of the Foundation or a Third Party, unless such interest is in conflict with the interest of the individual whose data is being processed, and their interest takes priority;

## **Article 5: Categories of Relevant Individuals**

- 5.1 The Foundation processes Personal Data regarding the following categories of Relevant Individuals:

- General Director and his/her employees;
- Certified Individual / Defendant;
- Contact person at the Relevant Bank;
- Expert or witness;
- Members of the Enforcement Committee and the Appeals Committee;
- Members of the Board;
- Reporter;
- Persons involved in the Report and/or Complaint, and/or the processing of such, including clients of a Bank;
- The Secretary of the Enforcement Committee and the Appeals Committee;

## **Article 6: Categories of Personal Data**

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

- Report data: These are Personal Data pertaining to a Report, including the Reporter's first- and last name, initials, gender, telephone number, e-mail address, and country; the Certified Individual's first- and last name, initials, gender, telephone number, e-mail address, bank, position, department, and office location; a description of the Certified Individual's behaviour, when it occurred, and which norm is alleged to have been violated. Sensitive Personal Data such as financial data may also be processed.

In exceptional circumstances, Special personal data regarding the Reporter may also be included in the report data. These special personal data will only be processed if such processing is necessary for the investigation and the disciplinary procedure, and for the execution of the legally required banking ethics law (Article 3.17 WFT), as stipulated in the Ethics Regulations. The report data are provided by the Reporter.

- Complaint data: These are Personal Data pertaining to the Complaint, the investigation, the revision procedure, the handling of the Complaint, the evidence, the verdict, the Measure, the challenge, the defence and the higher appeal, and communications pertaining to the above. The Personal Data processed in relation to a complaint include, but are not limited to, the following: personal details, contact information, employment information, information provided to the Relevant Individual and additional Personal Data necessary to investigate the Report or Complaint. Sensitive Personal Data such as financial data may also be processed. In exceptional circumstances, Special personal data or criminal records pertaining to the Certified Individual / Defendant may be included in the complaint data. Special personal data are only processed by the Foundation if necessary for the execution of the legally required banking ethics law. The Foundation has received permission from the Personal Data Authority to process criminal records pertaining to the disciplinary procedure. The complaint data are provided by the Reporter, the Relevant Individual, or the Relevant Bank.
- Data pertaining to the members of the Board, the Enforcement Committee and the Appeals Committee, the Secretary of the Enforcement Committee and the Secretary of the Appeals Committee: these include, but are not limited to: first-

and last name, initials, gender, titles, date of birth, home- and/or work address, postcode, city, telephone number, e-mail address, bank account number.

These data are provided by the Relevant Individuals.

- Other contacts: when a Relevant Individual contacts the Foundation via telephone, e-mail, or post, then personal data such as their name, (e-mail) address, telephone number, and other data shared by the Relevant Individual may be processed, depending on the nature of the contact.

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

## **Article 7: Quality**

7.1 Personal data are processed in a proper and accurate manner, in accordance with the Ethics Regulations and this Privacy Statement. Personal data are only processed inasmuch as such processing is sufficient, pertinent, and not excessive in relation to the purposes described in Article 4 of this Privacy Statement. In the event that data provided are excessive or not pertinent, then the Foundation will not process these data, or the data will be included in the Report or Complaint in an anonymous or pseudonym form. The Foundation takes suitable organisational and technical measures to achieve this goal.

7.2 Personal data are only processed inasmuch as the data are correct and accurate in relation to the purposes described in Article 4 of this Privacy Statement. If the data are found to be incorrect, then the Foundation will not process them, if the data are irrelevant to the verdict to be reached.

## **Article 8: Security**

8.1 The Foundation will implement suitable technical and organisational measures to secure the personal data against loss, damage, any form of violation of the integrity of data, or any form of unauthorised use. These measures guarantee a suitable security level with regard to the risks of use and the nature of the data to be protected, taking the state of the technology and the costs of implementation into consideration. The measures are intended in part to prevent the unnecessary collection and further processing of the personal data.

8.2 The Foundation ensures that processors offer sufficient guarantees with regard to the technical and organisational security measures for the processing activities. The Foundation monitors compliance with these measures. The Foundation shall sign a processing agreement with its processors.

8.3 The Foundation conducts regular data protection impact assessments (DPIA). A DPIA involves identifying any potential privacy risks and the implementation of any necessary corrective measures. When the Foundation changes its work methods, the Foundation also conducts a DPIA before implementing the proposed changes.

8.4 Employees of the Foundation who process Personal Data are required to report a Data Leak immediately in accordance with the Foundation's Data Leak Reporting Duty Protocol. The Foundation is required to report Data Leaks to the Personal Data Authority if a Data Leak can result in a significant chance of negative consequences for the protection of Personal Data. In some cases, the Foundation is also obliged to

inform the Relevant Individual. In the Processing Agreement, the Foundation requires the Processor (DSI) to report any Data Leaks.

### **Article 9: Storage period**

- 9.1 With the exception of the situation described in Art. 9.2, Personal Data will not be stored in a form that makes it possible to identify the Relevant Individual for a period longer than necessary to achieve the purpose for which the data were collected or processed.
- 9.2 The case file will be stored for seven (7) years after the ethics enforcement procedure is complete, after which the file will be definitively destroyed. Measures are recorded in the Disciplinary Register for the period specified in the Ethics Regulations and the Disciplinary Register Protocol.

### **Article 10: Confidentiality and awareness**

- 10.1 Any person who has access to personal data in the context of his/her work for the Foundation is required to maintain confidentiality and/or to sign a confidentiality statement to that end. This includes the General Director, the Secretary and the members of the Board, the Enforcement Committee and the Appeals Committee, the Expert and any person involved in handling a Report or Complaint. A person who has access to Personal Data in the conduct of his/her work shall only process the data to the extent necessary for the performance of the relevant position, activities, or task.
- 10.2 The Foundation guarantees that any person who has access to Personal Data in the context of his/her work for the Foundation is required to treat them with the utmost care and to have sufficient knowledge to achieve to that end.

### **Article 11: Inclusion and consulting the Disciplinary Register**

- 11.1 Inclusion in and consultation of the Disciplinary Register may only take place in accordance with the provisions of the Protocol.

### **Article 12: Publishing anonymous data**

- 12.1 As stipulated in the Ethics Regulations, the Foundation may publish a verdict with any identifying data in a manner of its own choosing.

### **Article 13: Information and provision**

- 13.1 In accordance with the Ethics Regulations, the Foundation must inform the Certified Individual and the Relevant Bank if any Personal Data are processed for the purpose of a process or argumentation in writing within a period of four weeks. The notification must contain a description of the purpose of the processing, and information about the rights of the Relevant Parties and the right of complaint. The Certified Individual shall be informed of the contents of the report, unless there are serious grounds for not sharing certain information.
- 13.2 In the event that the Personal Data of any third parties are processed by the Foundation, then the Foundation shall only inform the third party that Personal Data



pertaining to that party are being processed if such is permissible to protect the interests of the Relevant Persons (including the Reporter and the Certified Individual/Defendant). The Foundation will then only inform the third party if doing so is possible and/or does not involve a disproportionate amount of effort. The notification must contain a description of the purpose of the processing.

- 13.3 Report and complaint information may be provided to the members of the Enforcement Committee and its Secretary and the Appeals Committee and its Secretary. These individuals are also subject to the provisions of this Privacy Statement.
- 13.4 The Foundation shall only provide Personal Data to Third Parties if there are grounds to do so as described in Article 4 of this Privacy Statement, or if legally obliged to do so. In all other situations, data will not be shared with Third Parties.

#### **Article 14: Right of review**

- 14.1 A Relevant Person may submit a request to the Foundation to view his/her own Personal Data.
- 14.2 The Foundation shall process the Relevant Person's request if it is submitted in writing or electronically, and is accompanied by initials, last name, (e-mail) address, and a secure copy of a valid proof of identification.<sup>1</sup> In order to confirm the Relevant Person's e-mail address, a verification e-mail will be sent to the Relevant Person's e-mail address known to the Foundation. If the Foundation cannot determine that the individual making the request is actually the Relevant Person, or if there is a suspicion that the request may be fraudulent, then the Foundation may ask the Relevant Person to identify him/herself in person. If the identity of the Relevant Person cannot be confirmed, then the request of review will not be processed.
- 14.3 The Foundation will inform the Relevant Person in writing whether or not the Personal Data pertaining to him/her are being processed within four weeks of receipt of the request. If a request is too complex or burdensome, then the Foundation may extend this period by a maximum of two months. If the Relevant Person's Personal Data are processed, then the Foundation shall provide a complete overview of the Personal Data pertaining to the Relevant Person processed by the Foundation, unless there are grounds on which such a review request cannot be honoured. In the event that the Foundation refuses to honour the request, the reasons for such a refusal shall be provided to the applicant. In the event that this right of review also involves the rights and freedoms of other individuals, for example if the documents also include the Personal Data of persons other than the Relevant Person, then the Foundation may limit the right of review.

#### **Article 15: Right to correction, addition, and deletion**

- 15.1 A Relevant Person may request that the Foundation change, improve, supplement, delete, or screen his/her Personal Data if these data are incorrect, insufficient for the

---

<sup>1</sup> For instructions on making a secure copy, see: <https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/fraude-voorkomen-met-kopie-id-bewijs>.

- purpose for which they are processed, impertinent, or processed in violation of a legal regulation.
- 15.2 The Foundation shall process the request in accordance with Article 14.2 of this Privacy Statement.
  - 15.3 The Foundation shall inform the Relevant Person whether and to what extent it will honour the request in writing within four weeks of receipt of the request. If a request is too complex or burdensome, then the Foundation may extend this period by a maximum of two months. In the event that the Foundation refuses to honour the request, the reasons for such a refusal shall be provided to the applicant.
  - 15.4 The Foundation shall ensure that a decision to change, improve, supplement, delete, or screen the data is carried out as quickly as possible.
  - 15.5 In the event that the Foundation honours the Relevant Party's request to change, improve, supplement, delete, or screen his/her data, then the Foundation will also inform the third parties, such as Banks, to which these data have been provided, unless doing so is impossible or involves a disproportionate amount of effort.

### **Article 16: Objection**

- 16.1 The Relevant Person may object to the processing of his/her Personal Data by the Foundation. The Foundation shall then cease the processing of the Personal Data to which the person objects as quickly as possible, unless there are urgent and justifiable grounds to override this objection that outweigh the interests of the Relevant Person. In the event that DSI refuses to honour the request, the reasons for such a refusal shall be provided to the applicant.

### **Article 17: Complaints**

- 17.1 In the event that the Relevant Person is of the opinion that the Foundation is acting in conflict with the Privacy Statement, the Ethics Regulations, the Protocol, the law, and/or has treated him/her incorrectly, then the Relevant Person may submit a complaint in accordance with the [Foundation for Banking Ethics Enforcement Complaint Regulations](#).
- 17.1 If the Relevant Person is of the opinion that the complaint has not been processed properly by the Foundation, then he/she may appeal to the court or to the Personal Data Authority.

### **Article 18: Approval and amendments**

- 18.1 The privacy statement was approved by the Foundation and can be amended by the Foundation at its discretion.
- 18.2 The Foundation shall regularly evaluate whether the Privacy Statement fulfils its objectives. Any amendments must be accompanied with a revision date.
- 18.3 Once every two years, the Foundation shall conduct a review of this Privacy Statement.
- 18.4 If a situation arises that is not described in this Privacy Statement, then the Foundation shall take the necessary corrective measures and evaluate whether this Privacy Statement must be amended or supplemented.

**Article 19: Final provision**

19.1 This document may be referred to as the Foundation for Banking Ethics Enforcement Privacy Statement, and shall go into effect as of 1 July 2019.