Code of Conduct for the Processing of Personal Data

by Financial Institutions

1. Preamble

2. Definitions

3. The scope of the Code of Conduct

3.1 The sector

3.2 Application

4. Principles governing the Processing of Personal Data

5. Purposes of the Processing of Personal Data

5.1 General

5.2 Processing of Personal Data in connection with the assessment and acceptance of Customers, the conclusion and execution of agreements with a Customer and the settlement of payment transactions

5.3 Processing of Personal Data in connection with analyses for historical, statistical and scientific purposes

5.4 Processing of Personal Data in connection with marketing activities

5.5 Processing of Personal Data in connection with the security and integrity of the Financial Sector as well as the use of warning systems

5.6 Processing of Personal Data in connection with legal regulations

6. Processing of Special Categories of Personal Data

6.1 Personal Data relating to a person’s state of health

6.2 Personal Data relating to criminal offences

6.3 Other Special Categories of Personal Data

7. Rights of the Data Subjects

7.1 Inspection and rectification

7.2 Objection and consent

7.3 Compensation of costs

7.4 Decisions based on the automated Processing of Personal Data
8. Special subjects .................................................................................................................................................. 14
  8.1 Officer ......................................................................................................................................................... 14
  8.2 Data exchange with countries outside the European Economic Area (EEA) ........................................ 14
  8.3 Protection of Personal Data....................................................................................................................... 15
  8.4 Camera surveillance .................................................................................................................................. 15
  8.5 Recording of telephone conversations ..................................................................................................... 16
  8.6 Recording of electronic communication .................................................................................................. 16

9. Urgent reasons .................................................................................................................................................. 16

10. Compliance with the Code of Conduct ..................................................................................................... 17

11. Disputes ......................................................................................................................................................... 18

Notes to the Code of Conduct for the Processing of Personal Data by Financial Institutions .................. 19
1. **Preamble**

1.1 Banks and insurers (hereinafter: Financial Institutions) process Personal Data in connection with their business operations and consider it important that these Personal Data are handled with due care and are treated as confidential information.

1.2 The Data Protection Act (*Wet bescherming persoonsgegevens*), hereinafter: WBP) aims to provide guarantees for the protection of the privacy of natural persons in respect of the processing of Personal Data.

1.3 The Netherlands Bankers’ Association (*Nederlandse Vereniging van Banken*), hereinafter: the NVB, and the Association of Insurers (*Verbond van Verzekeraars*), hereinafter: the Association, have drawn up a Code of Conduct for the Processing of Personal Data by Financial Institutions (hereinafter: Code of Conduct) in accordance with the provisions of the WBP, which Code of Conduct has been approved by the Board for the Protection of Personal Data (*College Bescherming Persoonsgegevens*), hereinafter CBP on 13 April 2010. This declaration of approval was published in the Netherlands Government Gazette 2010 nr. 6360 on 26 April 2010. The CBP has declared that, in view of the specific characteristics of the sector, the Code of Conduct forms a correct elaboration of the WBP and other legal regulations governing the Processing of Personal Data. The approval is valid for a period of five years. This Code of Conduct replaces the previous Code of Conduct for the Processing of Personal Data by Financial Institutions.

1.4 The Code of Conduct aims:
- a. to lay down rules for Financial Institutions for the Processing of Personal Data;
- b. to provide information to individuals whose Personal Data are (or will be) processed by Financial Institutions; and
- c. to contribute to the transparency of the rules applied by Financial Institutions in respect of the Processing of Personal Data.

2. **Definitions**

For the purpose of this Code of Conduct, the following terms are defined as:

- a. **File**: any structured set of Personal Data, which is accessible according to specific criteria and relates to different subjects.

- b. **Data Subject**: the individual to whom Personal Data relate.

- c. **Processor**: the individual processing the Personal Data on behalf of the Controller, without being subject to his direct control.

- d. **Special Categories of Personal Data**: Personal Data concerning a subject’s religion or beliefs, race, political opinions, health, sexual preferences, trade union membership, as well as Personal Data relating to criminal offences and Personal Data relating to unlawful or objectionable conduct in connection with a ban imposed in respect of such conduct.

- e. **CBP**: the Data Protection Board (*College bescherming persoonsgegevens*), as referred to in section 51 of the WBP.

- f. **Customer**: the Data Subject with whom a Financial Institution: (i) maintains a legal relationship; or (ii) has maintained a legal relationship, (iii) considers entering into a legal relationship; or (iv) who has indicated that he is considering entering into a legal relationship with a Financial Institution or (v) individuals of whom a Financial Institution is obliged to process the Personal Data by virtue of statutory regulations or in view of the applicable time limit or (vi) individuals of whom a Financial
Institution is obliged to process Personal Data in connection with contractual or legal obligations vis-à-vis a Customer, Insured Party or Third Party.

g. Third Party: any individual other than a Data Subject, the Controller, the Processor, or any other individual who is authorised to process Personal Data under the direct control of the Controller or the Processor.

h. Direct Marketing: the transmission of information by a Financial Institution to a Data Subject with the aim of promoting the conclusion of an agreement.

i. Financial Institution: a bank and/or an insurer.

j. Officer: the officer in charge of data protection as referred to in section 62 of the WBP.

k. Incident Register / Incident Registration: The Processing of Personal Data that could be of importance for the security and integrity of the Financial Institution and that therefore requires special attention.


m. Group: the economic entity in which legal persons and companies are linked organisationally and to which a Financial Institution belongs.

n. Medical adviser: the doctor who acts as the person responsible for the Processing of Personal Data regarding a person's state of health, who is required in order to provide an independent expert advice in connection with the assessment of the state of health (i) of the Insured, (ii) of persons who have submitted a claim to the Insured or (iii) of the to be insured persons or (iv) in connection with the assessment of the medical actions of an Insured, to the departments of the insurance company that are responsible for taking the decision on an application or claim.

o. Personal Data: any information regarding an identified or identifiable natural person.


q. Security Department: the department(s) or the individual(s) within a Financial Institution that is (are) responsible for the Processing of Personal Data in connection with safeguarding the security and integrity.

r. Controller: the legal person, which alone or jointly with others, determines the purposes of and the means for the Processing of Personal Data or the legal person designated for this purpose within the Group.

s. The Insured / Insured Party: a natural or legal person who has concluded an insurance policy with a Financial Institution and any other persons who are entitled to compensation for damages and/or payment in accordance with the terms and conditions of the insurance policy.

t. Processing Personal Data: any operation or set of operations which is performed on Personal Data, such as collection, recording, organisation, storage, alteration, consultation, use, disclosure and destruction.

u. WBP: Data Protection Act (Wet bescherming persoonsgegevens).

3. The scope of the Code of Conduct
3.1 **The sector**

3.1.1 The Code of Conduct applies to Financial Institutions (i) that are members of the Netherlands Bankers’ Association; (ii) that are affiliated with Rabobank Netherlands; or (iii) that are members of the Dutch Association of Insurers.

3.2 **Application**

3.2.1 In the first place, this Code of Conduct shall apply to the (partially) automated Processing of Personal Data by a Financial Institution as part of its business operations. The Code of Conduct shall also apply to the manual Processing of Personal Data by a Financial Institution as part of its business operations, provided that the Personal Data are recorded in a File or are destined to be recorded in a File.

3.2.2 Processing of Personal Data in connection with: (i) incident registration by the Security Department; (ii) the External Reference Register (hereinafter: EVR); or (iii) in the capacity of the Financial Institution as an employer fall outside the scope of this Code of Conduct.

3.2.3 If the Code of Conduct for the Processing of Personal Data by Health Insurers is approved, then, in the event of a discrepancy, the Code of Conduct for the Processing of Personal Data by Health Insurers shall prevail for health insurers that are also members of Health Insurers Netherlands (Zorgverzekeraars Nederland).

4. **Principles Governing the Processing of Personal Data**

4.1 Personal Data shall be processed in accordance with the law and in a correct and careful manner.

4.2 Personal Data shall be collected for specified, explicit and legitimate purposes. This is further specified in article 5 of the Code of Conduct.

4.3 Personal Data shall only be processed if and insofar as such is consistent with at least one of the following legal grounds:
   a. the Data Subject has given his unambiguous consent for the Processing of the Personal Data;
   b. the Processing of Personal Data is necessary for the execution of an agreement to which the Customer is a party or in connection with taking pre-contractual measures at the request of the Customer, which are necessary for entering into an agreement;
   c. the Processing of Personal Data is necessary for compliance with a legal obligation to which the Financial Institution is subject;
   d. the Processing of Personal Data is necessary in order to protect the vital interests of the Data Subject;
   e. the Processing of Personal Data is necessary for the proper performance of a public law duty by the administrative body in question or by the administrative body to which the data are provided; or
   f. the Processing of Personal Data is necessary for the promotion of the legitimate interests of the Financial Institution or of a Third Party to whom the Personal Data are made available, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject, in particular the right to privacy.

4.4 Personal Data shall not be processed further in a manner that is inconsistent with the purposes for which the data have been obtained.
4.5 A Financial Institution shall take measures to ensure that Personal Data, taking into account the purposes for which the data are processed, are accurate, sufficient, relevant and not excessive.

4.6.1 Personal Data shall be removed at the end of the retention period, which shall be determined by the Financial Institution, and may be transferred to an archive destination for the archive administration, the settlement of disputes and carrying out (scientific, statistical or historical) research.

4.6.2 Personal Data may be stored for a longer period than stipulated in article 4.6.1 of the Code of Conduct insofar as this data is stored for historical, statistical or scientific purposes and the responsible party has taken the necessary measures to ensure that the data in question are only used for these specific purposes.

4.7 If Personal Data are obtained from the Data Subject, the Controller shall inform the Data Subject about his identity and the purposes of the Processing of Personal Data, unless the Controller may reasonably assume that the Data Subject is already cognizant of this. This obligation to provide information shall be fulfilled before the data are obtained.

4.8 If the Personal Data are obtained in another manner, the Controller shall inform the Data Subject about his identity and the purposes of the Processing of the Personal Data at the time of the recording of the data or, when the Personal Data are destined to be provided to a Third Party, at the time the data are first provided to a Third Party. This obligation does not apply when the Data Subject is already aware of this or when the provision of such information to the Data Subject proves impossible or could involve a disproportionate effort. In that case, the origin of the Personal Data shall be recorded. This obligation also does not apply when the recording or provision of the data is prescribed by or under the law.

4.9 If, in view of the nature of the data, the circumstances in which the data are obtained or the use that is made of the data, it should be necessary, in order to ensure the fair and careful Processing of Personal Data, further information shall be provided to the Data Subject in addition to the information as referred to in article 4.7 and 4.8 of the Code of Conduct.

4.10 Within the framework of its on-line business operations, a Financial Institution may record and further process Personal Data of a Data Subject who approaches a Financial Institution through the Internet. Financial Institutions shall make information available on their policy regarding Personal Data obtained through the Internet by means of a Privacy Statement on the web site in question. The Privacy Statement shall at least contain the information as referred to in article 4.7 of the Code of Conduct.

4.11 A Financial Institution can opt to not apply the purpose consistency principle (article 4.4 of the Code of Conduct) and the obligation to provide information (article 4.7, 4.8 and 4.9 of the Code of Conduct) if the Financial Institution satisfies the provisions stipulated in article 9 of the Code of Conduct.

4.12 Financial Institutions can make use of the services of a Processor for the Processing of Personal Data. If the Financial Institution makes use of the services of a Processor, an agreement shall be concluded with this Processor, in which it will be laid down in writing or in another equivalent form, inter alia, that technical and organisational measures must be taken for the protection of this data.

5. Purposes of the Processing of Personal Data

5.1 General

5.1.1 The Processing of Personal Data by Financial Institutions shall take place in accordance with the
principles governing the Processing of Personal Data for the purpose of an efficient and effective conduct of business, in particular, within the context of carrying out the following activities:

a. the assessment and approval of a Customer, the conclusion and execution of agreements with a Customer and the settlement of payment transactions;
b. performing analyses of Personal Data for statistical and scientific purposes;
c. carrying out (targeted) marketing activities in order to establish a relationship with a Data Subject and/or maintain or expand a relationship with a Customer;
d. the safeguarding of the security and integrity of the financial sector, including detecting, preventing, investigating and combating (attempted) (criminal or objectionable) conduct directed against the sector which the Financial Institution is part of, the Group to which a Financial Institution belongs, the Financial Institution itself or its Customers and employees, as well as the use of and the participation in warning systems;
e. complying with legal obligations;
f. Customer relationship management.

5.1.2 A Financial Institution shall not process more Personal Data than strictly necessary. Financial Institutions shall only make these Personal Data available within the Group to authorised employees.

5.1.3 Where necessary, Financial Institutions shall report their specific activities to the CPB or, insofar applicable, to their own Officer.

5.2 Processing of Personal Data in connection with the assessment and approval of Customers, the conclusion and execution of agreements with a Customer and the settlement of payment transactions.

5.2.1 Personal Data are (collected and) processed in connection with the assessment and acceptance of Customers and the conclusion and execution of agreements. Insofar as this concerns Personal Data regarding a person’s state of health and regarding criminal offences, the provisions referred to in article 6 of the Code of Conduct shall apply.

5.2.2 In connection with the assessment and acceptance of a Customer and the conclusion and execution of an agreement with a Customer, Financial Institutions may record Personal Data in and remove Personal Data from warning systems as referred to in article 5.5.2 of the Code of Conduct.

5.2.3 In connection with the normal settlement of payment transactions, Financial Institutions may provide Personal Data to the counterparty. In addition, unless agreed otherwise in advance, additional Personal Data are provided to the parties involved in the further Processing of Personal Data, insofar as this may be reasonably necessary for verification purposes or reconstruction purposes.

5.3 Processing of Personal Data in connection with analyses for historical, statistical and scientific purposes

5.3.1 The Processing of Personal Data for historical, statistical or scientific purposes shall not be regarded as inconsistent with the purposes for which the Personal Data were collected earlier. The Financial Institution shall take the necessary measures to ensure that the further Processing of the Personal Data shall only take place for these specific purposes.

5.3.2 Analyses of Personal Data in order to draw up group profiles are regarded as Processing for statistical or scientific purposes.

5.4 Processing of Personal Data in connection with marketing activities
5.4.1 If it has been made sufficiently clear to the Customer that the Financial Institution, with which the Customer has contact, is part of a Group, the Customer may then be approached by all entities of the Group for the purpose of marketing activities provided that the other provisions of the WBP are satisfied.

5.4.2 For marketing activities, use shall primarily be made of the Personal Data provided by the Data Subject himself. In the event that use is made of Personal Data that were not obtained from the Data Subject himself, article 4.8 of the Code of Conduct shall apply and the Financial Institution shall have to ensure that it acts in accordance with the WBP.

5.4.3 For marketing activities, Financial Institutions may make use of the services of companies specialised in this field. Financial Institutions shall ensure that a processor agreement is concluded with these companies in which, in writing or in a comparable form, obligations are laid down which the Processor must adhere to in respect of the WBP. Financial Institutions shall supervise the correct compliance with the agreements made between the parties.

5.4.4 Subject to the provisions stipulated in article 6.3.1 of the Code of Conduct, Financial Institutions may make use of Personal Data recorded in payment orders to bring financial products of the Group, to which the Financial Institution belongs, to the attention of the Customer. The Financial Institution shall refrain from bringing financial products to the attention of the Customer at the request of the Customer.

5.4.5 When carrying out marketing activities, the Financial Institution shall verify, each time, whether the Data Subject has made use of the right of objection, as referred to in article 7.2 of the Code of Conduct, in relation to the Processing of Personal Data for this purpose. The Financial Institution shall also check whether the Data Subject has registered with the register referred to in section 11.7 subsection 6 of the Telecommunications Act.

5.4.6 Special Categories of Personal Data shall only be used for marketing purposes with the explicit approval of the Data Subject.

5.5 Processing of Personal Data in connection with the security and integrity of the Financial Sector as well as the use of warning systems

5.5.1 For the security and integrity of the Financial Sector, data, including Personal Data, relating to (i) incidents that in view of the specific nature of the Financial Sector require the care and attention of the Financial Institution; (ii) (potential) changes, inter alia, in respect of the agreement concluded with the Financial Institution; (iii) noncompliance with a contractual obligation or other (attributable) breach; or (iv) actions of Financial Institutions, including investigations as referred to in article 5.6.1 of the Code of Conduct, are recorded in an Incident Register, which is maintained by the Security Department or another department of the Financial Institution in question that has been allocated this task. The Code of Conduct applies to this Incident Register.

5.5.2 If an incident as referred to in the first paragraph satisfies the criteria specified in the Protocol, the data relating to this incident shall be registered in the incident register. Registration in the EVR is also possible (Annex I: Document B).

5.6 Processing of Personal Data in connection with legal regulations

5.6.1 By virtue of, inter alia, the legal regulations set out below, Financial Institutions are obliged, in certain cases, to collect, process and provide the Personal Data of a Data Subject to certain Institutions (including government Institutions and supervisors). A number of these legal obligations are set out below (non-exhaustive).
a. Under the Act for the prevention of money laundering and the financing of terrorism (Wet ter voorkoming van witwassen en financieren van terrorisme; Wwft), a customer screening must be carried out when it concerns a business relationship in order to prevent money laundering and the financing of terrorism.

b. Financial Supervision Act (Wet op het financieel toezicht; Wft): under the Wft, Financial Institutions that provide loans to natural persons who are subject to the Wft, are obliged to participate in a ‘system of credit registration’. The Credit Registration Agency in Tiel (Bureau Krediet Registratie; BKR) manages such a system of credit registrations. Financial Institutions provide Personal Data about the origin and repayment of loans to the BKR and also have access to Personal Data that have been made available by other Financial Institutions. The nature of the recorded Personal Data, the conditions for recording, use and disclosure and the rules for the removal of the Personal Data have been laid down in the BKR regulations, which also contain a specific disputes settlement procedure.

c. Pursuant to the Wft, a party offering a financial services agreement is obliged to obtain information about the financial position of the Customer. In addition, the Decree prudential rules stipulates that Financial Institutions must provide for a systematic analysis of integrity risks and must implement a policy with regard to measures and procedures for the ethical conduct of business.

d. Income Tax Act 2001 (Wet inkomstenbelasting 2001) and the Income Tax Implementation Act 2001 (Invoeringswet inkomstenbelasting 2001): under these acts, Financial Institutions are required to state the citizen service number (burgerservicenummer), hereinafter BSN, as a mandatory identifier on the information to be submitted for tax purposes.

e. General provisions citizen service number Act (Wet algemene bepalingen burgerservicenummer, Wabb): under this act, insurers as referred to in section 23, subsection 1, under c, of the Pension Act are obliged to use the citizen service number for the administration of pension schemes.

f. State Taxes Act (Algemene wet inzake de rijksbelastingen, AWR): under this act, Financial Institutions - with an administration obligation – are obliged to record the BSN of the identity document in their administration.

g. Various laws, including the Code of Criminal Procedure, oblige Financial Institutions, if this is demanded, to make information about their Customer’s transactions available to investigation officers and supervisory bodies.

6. Processing of Special Categories of Personal Data

6.1 Personal data relating to a person’s state of health

6.1.1 A Financial Institution may process Personal Data relating to a person’s state of health insofar as this is necessary for: the assessment of a Customer, the approval of a Customer, the execution of an agreement with a Customer and the settlement of payment transactions.

6.1.2 Without prejudice to the provision specified in article 6.1.1 of the Code of Conduct, a Financial Institution may process Personal Data relating to a person’s state of health if: (i) the Customer’s explicit consent has been obtained; (ii) the information has clearly been disclosed by the Data Subject; (iii) this is necessary for determining, exercising or defending a right in legal proceedings; (iv) this is necessary to comply with an obligation by virtue of international law; (v) this is
necessary in view of a compelling general interest and adequate guarantees are provided for the protection of privacy and this is stipulated by law or the CBP has granted an exemption.

6.1.3 Personal Data regarding a person's state of health that are processed in order to make an assessment of a Customer, in connection with the acceptance of a Customer, the execution of an agreement with a Customer with regard to a specific product or the settlement of a claim for damages of a Customer shall not be used without the Customer's explicit consent for the assessment of a Customer, the acceptance of a Customer, the execution of an agreement with a Customer for another product or the settlement of another claim for damages.

6.1.4 The Processing of Personal Data regarding a person's state of health by a Financial Institution in order to be able to issue an advice regarding the medical assessment of a Customer as well as of the medical actions of an Insured is reserved for a Medical Adviser and the persons who are involved in this advice under his responsibility. Additional information regarding a Customer's state of health may only be requested by a Medical Adviser or by personnel belonging to his medical service or staff.

6.1.5 The collection of Personal Data regarding a person's state of health by a Medical Adviser of a Financial Institution from other parties than the Customer shall only take place after the Customer has given his permission and issued an authorisation for this. This authorisation may not be of a general nature, but must concern the Processing in connection with a concrete issue. The Customer must be informed about the nature of the to be requested information as well as about the purpose thereof. This must be apparent from the authorisation.

6.1.6 Reports by a medical expert, the Working Conditions Service (Arbodienst), as well as information from the practitioner providing the treatment shall be entered in a medical file that is kept under the responsibility of the Medical Adviser. The Customer has the right - preferably through a confidential doctor appointed by him or her – to fully inspect a medical file regarding the Customer, except for the notes of the Medical Adviser, and to receive copies thereof, unless this would violate the privacy of the Third Parties discussed in the report.

6.1.7 a. If, in connection with the acceptance and/or the handling of claims, a customer is requested to undergo a medical examination or an additional examination, the Financial Institution shall point out in the medical examiner's documents and forms the importance of identification in order to prevent mistaken identity.

b. The Customer shall then be informed that he has the right to make it known in writing that he wishes to be informed of the results and conclusion of the examination. Unless it concerns an insurance policy concluded under civil law, the Customer has the right to demand that he shall be the first to be informed of this information in order that he may decide that the results and conclusions are not to be communicated to others.

6.1.8 The Processing of Personal Data regarding a person's state of health does not fall under the responsibility of the Medical Adviser insofar as this is necessary for:

a. taking a decision regarding the risk that is to be insured by the insurer;

b. the settlement of claims in order to determine the size of the reported claim or determine the damage, in order to be able to decide whether additional information is required or whether payment can be made directly. The above without prejudice to the provision stipulated in article 6.1.4 that the additional information shall be requested and assessed by the Medical Adviser and that for the direct settlement of the claim only the necessary Personal Data regarding the person's state of health shall be processed;

c. the execution of the insurance or financing agreement, including also the Processing of Personal Data in connection with receiving and processing expense claims and financing agreements or if the Customer requests this in connection with his state of health.
6.1.9 The information regarding a person’s state of health shall only be processed by persons who are bound to secrecy by virtue of their office, profession or legal regulations or by virtue of an agreement, except insofar as they are obliged to disclose this information by law or their task requires that this information be disclosed to others who are authorised to Process this information pursuant to article 6.1 of the Code of Conduct.

6.1.10 The Processing of Personal Data relating to hereditary traits is subject to the genetic research moratorium (moratorium erfelijkheidsonderzoek). (Annex I: Document D).

6.1.11 The Processing of Personal Data regarding a person’s state of health that can be derived form a blood test is subject to the code of conduct for HIV (HIV gedragscode). (Annex I: Document E).

6.2 Personal data relating to criminal offences

6.2.1 Financial Institutions may process Personal Data relating to criminal offences insofar as this is necessary for: (i) the assessment of a Customer, the acceptance of a Customer, the execution of an agreement with a Customer and the settlement of payment transactions; (ii) safeguarding the security and integrity of the financial sector, including also detecting, preventing, investigating and combating (attempted) (criminal or objectionable) conduct directed at the sector which a Financial Institution is part of, at the Group to which the Financial Institution belongs, at the Financial Institution itself, at its Customers and employees, as well as the use of and the participation in warning systems; or (iii) to comply with legal obligations.

6.2.2 Without prejudice to the provisions stipulated in article 6.2.1, the Financial Institution may process Personal Data relating to criminal offences if: (i) the Customer’s explicit consent has been obtained; (ii) the information has clearly been disclosed by the Data Subject; (iii) this is necessary for determining, exercising or defending a right in legal proceedings; (iv) this is necessary to comply with an obligation by virtue of international law; (v) this is necessary in view of a compelling general interest and adequate guarantees are provided for the protection of privacy and this is stipulated by law or the CBP has granted an exemption; (vi) in the event that adequate and specific safeguarding measures have been taken and the procedure is followed pursuant to section 31 of the WBP.

6.2.3 In view of a sound acceptance policy, Financial Institutions may enquire about facts relating to a possible criminal record of persons to be insured and others whose interests are also insured in the applied for insurance policy (including directors and shareholders of legal entities), insofar as these facts relate to a period of eight years prior to the date of the insurance application. In this regard, the disclosed criminal record may only be used for the assessment of the insurance application and legally obtained data relating to a criminal record may be used in connection with invoking non-compliance with the disclosure obligation.

6.2.4 The prohibition on processing other Special Categories of Personal Data does not apply insofar as this is necessary in addition to the processing of Personal Data relating to a criminal offence for purposes for which this information is being processed.

6.2.5 Personal Data that: (i) relate to criminal offences that were perpetrated, or that, based on facts and circumstances, are expected to be perpetrated, against one of the Financial Institutions within a Group; or (ii) serve to detect possible criminal conduct towards one of the Financial Institutions of the Group, can be disclosed by the Financial Institution within the Group, provided that the information is only disclosed to officers who require this information in connection with the performance of their duties as well as to the police and the judicial authorities.

6.3 Other Special Categories of Personal Data
6.3.1 The information field of a payment order can contain Special Categories of Personal Data. The execution of payment orders also entails the Processing of such Personal Data. The Processing of Personal Data also takes place through the storage of the original documents or (digital) copies of these documents.

6.3.2 A Financial Institution may process (other) Special Categories of Personal Data if: (i) the Customer’s explicit consent has been obtained; (ii) the information has clearly been disclosed by the Data Subject; (iii) this is necessary for determining, exercising or defending a right in legal proceedings; (iv) this is necessary to comply with an obligation by virtue of international law; (v) this is necessary in view of a compelling general interest and adequate guarantees are provided for the protection of privacy and this is stipulated by law or the CBP has granted an exemption.

7. Rights of the Data Subject

7.1 Inspection and rectification

7.1.1 A Data Subject is entitled – with reasonable intervals – to request an overview in writing of the Personal Data of the Data Subject that are being processed by that Financial Institution. With the exception of the exceptional cases specified in article 9 of the Code of Conduct, the Financial Institution shall send a complete overview of the Personal Data to the Data Subject within four weeks of receiving the request. If the Financial Institution is not processing any Personal Data of the Data Subject, the Financial Institution shall also inform the Data Subject of this within four weeks after receiving the request.

7.1.2 The overview referred to in article 7.1.1 of the Code of Conduct contains, in a comprehensible form: (i) a description of the purpose or the purposes of the Processing; (ii) the categories of Personal Data which the Processing pertains to; (iii) the recipients or categories of recipients, as well as; (iv) the available information regarding the origin of the Personal Data.

7.1.3 If it should become apparent from the overview that the Personal Data are incorrect or, for the purpose of the Processing, incomplete or irrelevant or are being processed in another manner that is inconsistent with this Code of Conduct or with legal regulations, the Data Subject can request, in writing, the rectification, addition, removal or protection of the Personal Data in question. The Financial Institution shall inform the Data Subject within four weeks of the receipt of the aforementioned request in writing whether and to what extent the request can be granted. In the event that the request of the Data Subject cannot be granted or cannot be fully granted, this shall be substantiated.

7.1.4 The request referred to in article 7.1.1 of the Code of Conduct must be submitted to the Financial Institution that is responsible for the Processing of the Personal Data in question. The rectification request must contain a specification of the to be corrected Personal Data. The Financial Institution is responsible for adequately determining the identity of the party submitting the request.

7.1.5 If it is not clear for the Data Subject who is to be regarded as the Controller for the Processing of the Personal Data in question, for example because the Financial Institution forms part of a Group, the Data Subject can address his request to the management of the Financial Institution that he suspects is processing his Personal Data. The management of the Financial Institution in question must ensure that the request is handled in the correct manner.

7.2 Objection and consent

7.2.1 If the grounds for the Processing of Personal Data lie in the legitimate interest of the Controller or of a Third Party to whom the Personal Data have been provided, the Data Subject has the right to
lodge an objection against the Processing of Personal Data in connection with special personal circumstances. The Controller shall assess whether the objection is justified within four weeks of receiving the notice of objection. If this is the case, then the Processing of the Personal Data of the Data Subject will be terminated immediately.

7.2.2 If a Financial Institution processes Personal Data in connection with fundraising for commercial or charitable purposes, the Data Subject can always lodge an objection free of costs. In the event of an objection, the Financial Institution shall immediately take measures to terminate this form of Processing of Personal Data. The Controller shall ensure that the possibility to lodge an objection is always pointed out to the Data Subject in the event that, for the purposes mentioned above, a message is sent directly to the Data Subject.

7.2.3 The use of automatic calling systems without human intercession, of a fax or of electronic messages for Direct Marketing purposes is only permitted when the sender can demonstrate that the Data Subject has given his prior permission for this ("opt-in"). Granting this consent shall be free of charge for the Data Subject.

7.2.4 The use of other techniques than the techniques specified in article 7.2.3 of the Code of Conduct including telephone calls and ‘regular’ mail for Direct Marketing is permitted unless the Data Subject has indicated that he does not wish to receive information or notifications whereby these techniques are used ("opt-out"). Facilities preventing the Data Subject from receiving unsolicited information shall be free of charge for the Data Subject.

7.2.5 A Financial Institution that has received electronic contact information for electronic messages (such as e-mail, SMS messages and MMS messages) in connection with the sale of a financial product or the providing of a financial service may use this information for the Direct Marketing of comparable financial products or financial services of its own ("soft opt-in"). This, subject to the condition that: (i) when the contact information was obtained from the Data Subject the possibility was explicitly offered to lodge an objection free of charge against the use of this electronic contact information; and, (ii) if the Data Subject has not made any use of this, at the time of each communication, he shall explicitly be offered the possibility to lodge an objection free of charge against the further use of his electronic contact information. Section 41, second subsection, of the WBP shall apply mutatis mutandis.

7.2.6 The Financial Institution must comply with the information obligation referred to in Section 3:15 of the Dutch Civil Code when making use of electronic messages for Direct Marketing purposes.

7.2.7 A Financial Institution shall only make use of an electronic means of communication to gain access to Personal Data that are stored in the computer of a user of a public communication network if that is necessary to enable or facilitate sending the communication over a public network or to provide the service requested by the user and the storage of or access to information is strictly necessary for this.

7.2.8 In all other cases, a Financial Institution may only obtain access in the event that the user has been informed in a clear and precise manner about the purposes for which access to computers or Personal Data is required and in a sufficiently clear manner the opportunity has been offered to refuse this access.

7.3 Compensation of costs

7.3.1 A Financial Institution may demand a compensation to offset the costs of a request of a Data Subject as referred to in the articles 7.1.1 and 7.2.1 of the Code of Conduct. Such a charge shall not exceed the amount laid down by order in council.
7.3.2 In the event that Personal Data are adapted, altered or deleted as referred to in article 7.1.3 of the Code of Conduct or in the event that the objection referred to in article 7.2.1 of the Code of Conduct is upheld, the compensation referred to in article 7.3.1 of the Code of Conduct shall be refunded.

7.4 Decisions based on the automated Processing of Personal Data

7.4.1 The taking of a decision by a Financial Institution solely based on the automated Processing of Personal Data intended to evaluate certain aspects relating to an individual's personality shall only be allowed if: (i) such a decision is taken in the course of entering into or executing an agreement, or (ii) such a decision is authorised by law which also lays down measures to safeguard the Data Subject’s legitimate interests.

7.4.2 If the decision does not satisfy the Data Subject's request, he shall be given the opportunity to forward his point of view. In this case, the Financial Institution shall inform the Data Subject of the logic on which the automated individual decision was founded.

8. Special subjects

8.1 Officer

8.1.1 A Financial Institution may appoint an Officer. Only a natural person possessing adequate knowledge for the discharge of his task and who may be deemed sufficiently reliable may be appointed as an Officer. For the discharge of his task, the Officer shall be independent of the Financial Institution that has appointed him and shall not receive any instructions regarding the exercise of his duties. The Financial Institution appointing him shall enable the Officer to discharge his task adequately and shall ensure that he shall not suffer any negative consequences from carrying out his task. In connection with this, the Officer shall be protected against dismissal.

8.1.2 The Officer shall ensure that the Financial Institution complies with the regulations governing the processing of Personal Data by or under any law, as well as with the provisions of this Code of Conduct. He shall prepare an annual report of his activities and findings. The Officer shall have the powers vested in him by virtue of article 63 and 64 of the WBP. The General Administrative Law Act shall be applied in a similar manner.

8.2 Data exchange with countries outside the European Economic Area (EEA)

8.2.1 In connection with their services, Financial Institutions exchange Personal Data within the Group with Processors and Third Parties whose services the Financial Institution makes use of. As a result, Personal Data can be disclosed to countries located outside of the EEA, now that entities that form part of the Group, Processors and Third Parties can be located in countries outside of the EEA.

8.2.2 Subject to the principles governing the Processing of Personal Data, a Financial Institution may transfer Personal Data to countries outside of the EEA, if the country in question ensures an adequate level of protection in respect of the Personal Data being transferred. It is also considered an adequate level of protection when the European Commission has decided that a given country offers an adequate level of protection. In addition, an adequate protection level can be created by implementing approved Binding Corporate Rules within a Group worldwide.

8.2.3 The transfer of Personal Data by a Financial Institution is always allowed if:
   a. the Data Subject has given his unambiguous consent for this; or
   b. the transfer of Personal Data is necessary for the execution of an agreement between the Customer and the Controller or in connection with taking steps at the request of the
Customer prior to entering into an agreement, which are necessary for entering into an agreement; or
c. the transfer is necessary for the conclusion or execution of an agreement concluded or to be concluded between the Controller and a Third Party in the interest of the Customer; or
d. the transfer is necessary in connection with an important general interest or for the purpose of establishing, implementing or defending any right at law; or
e. the transfer is necessary for the protection of the vital interests of the Data Subject; or
f. the Minister of Justice has granted permission for the transfer or categories of transfer.

8.3 Protection of Personal Data

8.3.1 The Financial Institution that processes Personal Data shall, taking into account: (i) the latest state of technology; (ii) the costs of implementation; (iii) the risks entailed in the Processing; (iv) and the nature of the Personal Data, take appropriate technical and organisational measures to protect Personal Data against, inter alia, (intentional) destruction, loss, falsification, unauthorised disclosure or access and any other from of unlawful Processing of Personal Data.

8.3.2 In the event that the Processing of Personal Data is carried out by a Processor, the Controller shall ensure that it is laid down in an agreement with the Processor in question in writing or in another equivalent form, that the Processor shall provide sufficient guarantees in respect of the technical and organisational security measures regarding the to be carried out Processing of Personal Data.

8.4 Camera surveillance

8.4.1 Subject to certain conditions, financial Institutions may make use of surveillance cameras. Camera surveillance, the images obtained through camera surveillance and the processing thereof have the following purpose:
a. the security and protection of buildings and premises, which the Financial Institution uses or which are owned by the Financial Institution;
b. to guard goods in these buildings;
c. to safeguard the interests of the Financial Institution and the safety and interests of the employees, Customers or Third Parties;
d. to prevent, detect or investigate criminal offences or violations of the Financial Institution’s (company) rules;
e. to support legal proceedings.

8.4.2 Camera surveillance by Financial Institutions is only allowed, if:
a. camera surveillance can be carried out selectively, i.e. that no more locations or persons may be recorded than is necessary for the abovementioned purposes. Insurers must also comply with the Code of Conduct for Personal Investigations (Gedragscode Persoonlijk Onderzoek) (Annex I: Document C).
b. the Personal Data obtained through camera surveillance are not stored longer than is necessary for the purposes described in article 8.4.1 of the Code of Conduct. The storage period can vary for each camera application;
c. the images obtained through camera surveillance are stored and protected in such a manner as to ensure that these images are not accessible to unauthorised individuals and the necessary measures are taken to prevent manipulation and to ensure that the images can be traced and reconstructed.
d. camera surveillance has been clearly indicated. As and when necessary, a hidden camera can be used to record or investigate criminal offences or violations of company rules or in connection with providing evidence in legal proceedings.

8.4.3 Insofar as Personal Data regarding a person’s race is processed during camera surveillance, then
this may only occur in order to identify the Data Subject and only insofar as this is inevitable for this purpose.

8.4.4 Financial Institutions may provide the images obtained through camera surveillance to the police and the Judicial authorities, the Security Department and officers within the Group who are responsible for the supervision of compliance with the company rules.

8.4.5 A Data Subject shall have the right to view the camera recording and/or obtain a copy of the camera recording subject to the condition that the Data Subject provides sufficient information to the Financial Institution so that the Financial Institution shall be able to trace the specific camera recording. The Data Subject must at least inform the Financial Institution about the location, date and time of the recording, or provide another indication in order to facilitate the search. The Financial Institution shall not be required to enable inspection if the conditions stipulated in article 9 of the Code of Conduct are satisfied.

8.5 Recording of telephone conversations

8.5.1 The recording of telephone conversations by a Financial Institution, the resulting tape recording and the Processing thereof have the following purpose: (i) being able to provide evidence, inter alia, regarding interpretation differences or disagreements regarding the contents of a telephone conversation; (ii) (fraud) investigation and detection; (iii) evaluating the quality of the services provided; (iv) training, coaching and appraisal purposes.

8.5.2 The tape recordings shall be stored and protected in such a manner that they are not accessible to unauthorised individuals and the necessary measures shall be taken to prevent manipulation.

8.5.3 The Financial Institution shall not store tape recordings any longer than necessary for the purposes set out in article 8.5.1 of the Code of Conduct.

8.5.4 A Data Subject has the right to listen to the tape recording, receive a copy of the tape recording or receive a transcript of the recorded telephone conversation depending on the contents of the tape, subject to the condition that the Data Subject provides sufficient information to the Financial Institution so that the Financial Institution shall be able to trace the specific tape recording. The Data Subject must at least inform the Financial Institution about the date and time of the conversation, the telephone number used by the Data Subject and provide an indication of the telephone number that the Data Subject called or provide another indication to facilitate the search. The Financial Institution shall not be required to enable inspection if the conditions stipulated in article 9 of the Code of Conduct are satisfied.

8.5.5 Financial Institutions may provide the tape recordings to the police and the Judicial authorities, the Security Department and officers within the Group who are responsible for the supervision of compliance with the company rules.

8.6 Recording of electronic communication

8.6.1 In as far as possible, article 8.5 of the Code of Conduct shall be applied in a similar manner to the recording of Personal Data obtained through electronic communication with a Data Subject.

9. Urgent reasons

9.1 The purpose consistency principle, the transparency principle and the rights of the Data Subject as referred to in articles 4.4, 4.7, 4.8, 4.9, 7.1.1, 8.4.5 and 8.5.4 of the Code of Conduct may be set aside in special circumstances, whereby all facts and circumstances are of importance, if
there is an urgent reason for this, which is more compelling than the rights and freedoms of the Data Subject, within the context of:

- the prevention, detection, investigation and prosecution (including the cooperation with (supervisory) authorities) of violations of laws, regulations or the Financial Institutions company rules;
- protecting and defending the rights and freedoms of the Financial Institution / Financial Sector, the personnel or other persons (including the Data Subject or a Third Party) including: (i) the safety (of employees and Customers) of the Financial Institution / Financial Sector; (ii) the company secrets and reputation of the Financial Institution; (iii) the continuity of the Financial Institution/Financial Sector; (iv) confidentiality in connection with, for example, a (proposed) merger or acquisition; (v) involvement of advisers in, inter alia, the fields of law, tax matters and insurance.

10. **Compliance with the Code of Conduct**

10.1 Financial Institutions attach great importance to the correct compliance with the rules of the WBP and the Code of Conduct. In this context, Financial Institutions have implemented a system of self-evaluations in order to carry out periodical risk analyses regarding the compliance with the WBP and this Code of Conduct. As part of this process, a Financial Institution shall determine the manner and the frequency in which the various business units of the Financial Institution shall be audited with regard to the correct compliance with the WBP and the Code of Conduct, as well as the preparation of reports.

10.2 In order to ensure the compliance with the rules of the WBP and the Code of Conduct, a Financial Institution is required to draw up and issue internal instructions which specify in which manner the Personal Data are to be processed by the Financial Institution. The internal instructions concern, in any case, those items of which the Financial Institution is of the opinion that further explanation is desirable.

11. **Disputes**

11.1 Data Subjects who are of the opinion that a Financial Institution is violating the Code of Conduct or the WBP, may address themselves to the Complaints Institute Financial Services Foundation (*Stichting Klachteninstituut Financiële Dienstverlening, KiFiD*), PO Box 93257, 2509 AG The Hague. Subject to the condition that the internal complaints procedure of the Financial Institution has been followed first. Depending on the complaint in question, the Data Subject may also apply directly to the CBP or the competent court. In all cases, the Data Subject must take into account the terms specified in article 46 and 47 of the WBP.