Code of Conduct for the Processing of Personal Data by Financial Institutions

VERBOND VAN VERZEKERAARS

November 2nd, 2010

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 Dutch 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.

l. Code of Conduct: the Code of Conduct for the Processing of Personal Data by Financial Institutions.

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.

p. Protocol: the Protocol Incident Warning System Financial Institutions.

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 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 Storage

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 our (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 schems.
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 Medial 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.

6.1.7a. 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 authorized 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 put 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. he 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, this within the context of:

a. the prevention, detection, investigation and prosecution (including the cooperation with (supervisory) authorities) of violations of laws, regulations or the Financial Institutions company rules;
b. 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.

Notes to the Code of Conduct for the Processing of Personal Data by Financial Institutions

1. Preamble

General

Almost every Dutch resident has a relationship with a Financial Institution; be it in the form of a current account, a mortgage loan, a personal loan or insurance. In connection with the relationship that a Financial Institution has or wishes to enter into with a Customer, a Financial Institution will also have to process Personal Data. Various interests play a role in the processing of Personal Data. It is in the Data Subject's interest that his privacy is optimally protected, while the Financial Institution aims to look after its legitimate interests in the best possible manner.

In order to duly reconcile potentially conflicting interests in connection with the processing of Personal Data, a set of rules has been laid down in the form of the Data Protection Act (*Wet bescherming persoonsgegevens)*, hereinafter: WBP [1] Under this act, the Financial Institution processing these Personal Data, i.e. the Controller, has to fulfil a number of obligations. Under the WBP, the individuals whose Personal Data is processed, the Data Subjects, have been granted a number of rights, such as the right of inspection and rectification and the right to object. There is also (independent) supervision of compliance with the WBP by: (i) the Board for the Protection of Personal Data (*College bescherming persoonsgegevens)*, hereinafter: CBP (ii) the officer in charge of data protection, hereinafter: Officer, if such an Officer has been appointed by a Financial Institution or by (iii) special privacy officers or managers who have been appointed as such by a Financial Institution.

The WBP offers organisations and sectors the possibility to lay down rules that are, for example, more tailored to their specific business operations. In view of the close ties between banks and insurers, the Netherlands Bankers' Association (*Nederlandse Vereniging van Banken*), hereinafter: NVB, and the Dutch Association of Insurers *(Verbond van Verzekeraars),* hereinafter: VvV, have decided to draft a single Code of Conduct: the Code of Conduct for the Processing of Personal Data by Financial Institutions (hereinafter: Code of Conduct). The CBP issued a declaration of approval for a period of five years in respect of the first Code of Conduct for the Processing of Personal Data by Financial institutions of 25 January 2003. This Code of Conduct was subsequently updated and the CBP has declared that the updated Code of Conduct constitutes a correct elaboration of the WBP. The approval is valid for a period of five years.

2. Definitions

General

Most of the terms that are defined in the Code of Conduct correspond with terms that are used in the WBP (in order to remain consistent). Four terms that are more or less specific for a Financial Institution and that are not found in the WBP are the terms Customer, Medical Adviser, Security Department and Insured or Insured Party. The terms Customer and Insured / Insured Party will be explained in more detail when discussing the term Data Subject. A

[1] Government Gazette, 2001, 337. The WBP is based on the EU Directive regarding the protection of natural persons in connection with the Processing of Personal Data and concerning the free circulation of these data.

further explanation of the other terms will be provided when discussing the articles in question (article 6.1 and 5.5 of the Code of Conduct, respectively).

For a good understanding of the Code of Conduct, the meanings of three definitions, i.e. that of the Controller, the Data Subject and the Processor should be retained. The WBP imposes certain obligations on the Controller in respect of the Processing of Personal Data and confers certain rights to the Data Subject. In addition, it is important to make a distinction between a Controller and a Processor.

The *Controller* determines the purpose and the means of the Processing. This concerns the legal entity that is formally authorised to take decisions regarding the Processing of Personal Data. In principle, the Financial Institution with which the Data Subject, for example, concludes an agreement will act as the Controller. The WBP does not preclude that, in practice, measures are taken whereby the responsibility within a Group is assigned to another party (for example, the parent company) than the party under whose authority the operational Processing of Personal Data takes place (for example, a subsidiary). In the event that a Financial Institution forms part of a Group, another legal person within the group can be designated as the Controller. In that case, through provisions in the articles of association or by means of an agreement, a specific legal entity within the Group is granted the authority to determine the purpose and the means of the Processing of Personal Data within the Group. In this manner, the parent company can act as the Controller for all the Processing of Personal Data that takes place within the Group, as the legal control lies with the legal entity by virtue of the measures taken. If it cannot be determined who is formally authorised to take decisions regarding the Processing of Personal Data, then the party to whom the Processing of Personal Data must be attributed according to generally accepted standards shall be held responsible. It is difficult to define this more specifically: what generally accepted standards are shall depend on the actual situation.

The *Data Subject* is the individual to whom Personal Data relate. In any case, the individuals who are recorded in the Customer registration system, in whatever manner, belong to the group of Data Subjects. The data of individuals with whom the Financial Institution has a relationship for various reasons are recorded in this system. The term Customer is the generic term used to refer to these individuals. This concerns the following groups of individuals:

(i) individuals with whom an agreement has been concluded;
(ii) individuals with whom an agreement has been concluded in the past and whose Personal Data must still be processed for various reasons;
(iii) individuals who are approached by a Financial Institution for the purpose of entering into an agreement;
(iv) individuals who approach a Financial Institution themselves by requesting information or requesting an offer;
(v) individuals whose Personal Data a Financial Institution is obliged to process by virtue of a legal regulation (for example, the consent of a wife/husband pursuant to Section 88 Book 1 of the Dutch Civil Code) or in view of the applicable time limits; and
(vi) individuals whose Personal Data a Financial Institution is obliged to process in connection with contractual or legal obligations vis-à-vis a Customer, an Insured or a Third Party.

With this latter group, this concerns, for example, individuals who hold an Insured liable for damages that they have suffered due to an event for which the Insured is liable in their opinion. This is the case, for example, in the event of medical liability, whereby a care

provider, such as a hospital, can be held liable for making the wrong diagnosis or providing the wrong treatment. In view of the fact that in the case of this Insured party, this could concern either a natural person or a legal person this has explicitly been expressed in the definition of the term. On the other hand, it can also concern commercial Data Subjects, such as intermediaries and mortgage advisers. Finally: a sole proprietorship without legal personality is also regarded as a Data Subject, as information about the company also contains Personal Data about the director and the owner and as a result, this information must be regarded as Personal Data.

The *Processor* processes Personal Data for the principle, the Controller. The Processor has no control over the Processing, the Processor only acts in accordance with the Controller's instructions. The following is an example of the relationship between the Processor and the Controller: Financial Institutions have largely outsourced the settlement of payment transactions to Equens. The point of departure in this case is that Equens's role consists of the execution of the instructions of the Financial Institutions. Equens does not have any independent authorisation to make use of the Personal Data that has been entrusted to them in connection with payment transactions for other purposes. In this situation, Equens acts as the Processor. This is different insofar as it concerns independent services offered by Equens. In that case, Equens is to be regarded as Controller. In this context, the following example can be provided: Financial Institutions make use of credit card companies to thus be able to offer credit card facilities to Customers through Equens. These credit card companies should be regarded as Controllers, as they offer services independently and, in this context, decide independently about the manner in which Personal Data, which the Financial Institutions provide to the credit card companies, are to be processed. In practice, Financial Institutions often make use of IT service providers to whom Financial Institutions outsource, for example, maintenance and support functions. These IT service providers should be regarded as Processors, as they have no independent control over the processing of the Personal Data that are made available to the IT service provider in this context, while, at the same time, services are provided on behalf of the Financial Institution. Finally, as the last example: Intermediaries that act as intermediaries on behalf of Financial Institutions should be regarded as Controllers, as they offer services independently and decide independently about the Processing of Personal Data.

3. The scope

General

For the applicability of the Code of Conduct to Financial Institutions the strict condition applies that: (i) banks must be members of the NVB; or (ii) banks must be affiliated with Rabobank Netherlands; or (iii) insurers must be a member of the Dutch Association of Insurers (VvV). This means, for example, that when a bank acts as an insurance intermediary on behalf of an insurer, the Code of Conduct shall be applicable. The Code of Conduct does not apply, for example, when it concerns an independent intermediary or the bank is not a member of the NVB or not affiliated with Rabobank Netherlands. The point of departure that the Code of Conduct applies to Financial Institutions, also implies that parts of Financial Institutions, which do not act as a bank or insurer, are not subject to this Code of Conduct, although the Code of Conduct does apply to the Financial Institution. This is, for example, the case for a Financial Institution with a department consisting of legal assistance providers who provide legal assistance to individuals who have concluded a legal assistance insurance policy. In this case, the Code of Conduct does apply to the insurer; however, it does not apply to the legal assistance insurer, which, in this case, is comparable to a lawyer who provides

assistance to an individual in such cases. The above scope does not mean that other natural or legal persons, which do not fall within the definition of Financial Institution, such as independent intermediaries, legal assistance providers and claim adjustment agencies, may not endorse (parts of) the Code of Conduct.

The Processing of the Personal Data of the employees of a Financial Institution does not fall within the scope of the Code of Conduct. The Processing of Personal Data of individuals that are recorded in: (i) incident registers; or (ii) the External Reference Register (hereinafter: EVR), also does not fall within the scope of the Code of Conduct. The Protocol Incident Warning System Financial Institutions (hereinafter: Protocol) applies to the Processing of these Personal Data (Annex I: Document B).

The Code of Conduct for the Processing of Personal Data by Health Insurers shall also apply to health insurers that are members of the Dutch Association of Insurers and of Health Insurers Netherlands (*Zorgverzekeraars Nederland*, ZN) as soon as the Code of Conduct for the Processing of Personal Data by Health Insurers has been approved by the CBP. Although both codes have been aligned to each other with regard to the most important items, concurrence cannot be ruled out completely. This could concern, in particular, the Processing of Personal Data relating to an individual's state of health. In this case, the Code of Conduct for the Processing of Personal Data by Health Insurers shall prevail.

4. Principles Governing the Processing of Personal Data

General
All acts that are performed in respect of Personal Data are included under the Processing of Personal Data. This concerns the collection up to and including the destroying of Personal Data, including all the acts in between. The most important conditions for a lawful Processing of Personal Data are: (i) the determining of the purposes of the Processing; (ii) the determining of the grounds for the Processing; and (iii) the Controller’s obligation to provide information. A further explanation of these conditions is provided below. In connection with the determining of the purpose, the so-called "compatible use" will be discussed in detail in this explanation, as this determines the further Processing of Personal Data, for example, the disclosure.

Purposes of the Processing of Personal Data (article 4.1 and article 4.2)
Personal Data may only be collected for specified, explicit and legitimate purposes. These purposes must be determined or adjusted before the (adjusted) Processing may take place. Specified means that the description of the purpose must be clear. The purposes of the Processing of Personal Data by Financial Institutions are specified in article 5 of the Code of Conduct. The purpose for which the Personal Data are collected is the assessment criterion for a number of other provisions, such as the compatible use, the retention period and the condition that no more Personal Data may be collected than necessary for the purpose. See article 5 of the Code of Conduct for a detailed explanation of the purposes.

Lawful grounds (article 4.3)
The Processing of Personal Data must be based on one of the lawful grounds specified in the WBP. These have therefore been incorporated in the Code of Conduct. If none of the lawful grounds is applicable, the Personal Data may not be processed. It is also possible that several grounds are determined. This will mainly be the case when Personal Data are used for several activities. Financial Institutions base the Processing of Personal Data mainly on

the grounds that the Processing is necessary for the conclusion and execution of an agreement with the Data Subject, in order to comply with legal obligations or because the Processing is necessary in connection with the Financial Institution's legitimate interests. Below an explanation is provided with regard to the grounds that Financial Institutions often use.

The Personal Data are necessary for the execution of the agreement to which the Data Subject is a party or in connection with taking pre-contractual measures.
The first grounds, which are often cited by Financial Institutions, based upon which Personal Data may be processed concern the Processing of Personal Data if this is necessary for the execution of an agreement to which the Data Subject is a party. This is the case, for example, when an individual gives his bank the order to transfer a certain amount of money to the account of a third party. The necessary Processing by the bank of the Personal Data of the Data Subject in connection with this follows from the current account agreement that this individual has concluded with his bank. For that matter, it is not necessary that the Controller is a party to the agreement. It is necessary that the Data Subject is a party to the agreement. The Personal Data may also be processed in the phase before the conclusion of the agreement. An example of this is the Data Subject who requests a bank to open an account or requests an offer for a mortgage loan or insurance.

The Personal Data are necessary in order to comply with a legal obligation to which the Controller is subject.
Increasingly, Financial Institutions are required to Process Personal Data in order to comply with legal obligations. In this context, the Financial Supervision Act (*Wet op het financieel toezicht*, hereinafter: Wft) and the Act for the prevention of money laundering and the financing of terrorism (*Wet ter voorkoming van witwassen en financieren van terrorisme*, hereinafter: Wwft) can be named See the explanatory notes to article 5 of the Code of Conduct for more detailed information about the legal obligations to which Financial Institutions are subject.

The Personal Data is necessary in connection with the legitimate interests of the Controller (or a Third Party to whom the Personal Data are provided), unless the interests or the fundamental rights and freedoms of the Data Subject prevail
In order to assess these grounds, the interests of both the parties concerned shall have to be weighed each time. These latter grounds also apply when Personal Data are processed in connection with marketing activities, the settlement of payment transactions (whereby, for example, Personal Data of a beneficiary, not being the contract party, are processed), risk management and fraud prevention. The providing of Personal Data to a Third Party by a Financial Institution can also be based on these grounds. For instance, providing Personal Data to a supervisory authority, (legal) adviser or other Financial Institution in connection with an investigation or (any) legal proceedings.

For the sake of good order: in addition to the grounds discussed above, Financial Institutions also process Personal Data based on the other grounds referred to in article 4.3 of the Code of Conduct, including, for example, the Data Subject's unambiguous consent. This consent does not have to be obtained in writing. Consent can also be apparent from certain conduct of the Data Subject. Financial Institutions can also request the Data Subject's consent by having the Data Subject check a box on a paper or electronic document, whereby the Financial Institution shall, of course, inform the Data Subject about the purposes of the Processing.

Compatible use (article 4.4)
Financial institutions have substantiated the purpose of the processing of Personal Data in several activities. Compatible use, i.e. whether and to what extent the Personal Data that were obtained in connection with the activities specified in the purposes may also be processed in connection with other activities, depends on the question whether the purpose of the activities in question is compatible with the activity or activities for which the Personal Data were originally obtained.

Before further processing Personal Data, the Financial Institution must ascertain that this is not incompatible with the activity or activities for which the Personal Data were obtained. Various factors play a role when answering the question whether this constitutes compatible use. A number of these factors - not exhaustive - are listed in Section 9, subsection 2 of the WBP, such as the connection with the purpose or the products for which the Personal Data were obtained, the nature of the information, the consequences of the Processing for the Data Subject and the degree in which suitable safeguards are provided in respect of the Data Subject. For instance, Personal Data can be sensitive in the context in which they are used, for example, information about an individual's creditworthiness or prosperity. The more 'sensitive' the Personal Data, the less it can be assumed that it constitutes compatible use if the original purpose is departed from in the Processing. The factors must be assessed and weighed in their totality. None of the factors alone are decisive. If, for example, there is a certain connection between the purpose for which the Personal Data were obtained, but the Personal Data can become sensitive when used in a certain context, while the consequences are far-reaching for the Data Subject, this is not likely to constitute compatible use. In the event that the Data Subject has given permission for the further Processing, the requirement of compatible use is, in any case, satisfied.

Thus, in the case of compatible use, it concerns open norms that have to be assessed and weighed on a case-by-case basis in order to determine whether the exchange of certain data is allowed. As an explanation, a number of examples are provided below.

- In connection with payment orders, the name and address data belonging to a contra account number will be provided to the party issuing the order and the beneficiaries. This information is provided together with the payment. Parties issuing the payment order and beneficiaries can request information regarding the contra account with regard to specific payments. Such requests are submitted to their own bank. The bank handles these requests with due care. If the request clearly has a purpose that lies outside of the settlement of payment transactions, then the request is refused. Prior to payment orders, no address information belonging to current accounts is provided. However, in connection with the settlement of payment transactions, parties can verify in advance whether the name and number combinations are correct. The aim is to minimise the probability of error.

- In the event that irregularities occur in the execution of an agreement, the employees of the Financial Institution may disclose Personal Data about the agreement and the observed irregularities to the Security Department, which can consist of a separate department or of an officer authorised for this. The Security Department/Officer may further process this Personal Data in connection with fraud prevention and have the data recorded, under the conditions specified in the Protocol, in the Incident Register or the EVR.

- A bank can derive information from payment order data regarding the possible interests of a Customer for certain financial services that the bank offers. If the bank uses this information for offering these services, this constitutes compatible use. For instance, a Customer who apparently is a student in view of the fact that the Customer receives student funding on his bank account, he can be approached by the bank for a student account. Payment order data consist only of identifiable data of the party issuing the order and the beneficiary and the information that can be derived from this. These data must be distinguished from the data that the party issuing the order states in the information field of the payment order. Information in the information field may not be used for marketing activities.

- Within the Group, the existence of a claim on a Data Subject can lead to information being exchanged in order to determine whether a payment is payable by another part of the Group by virtue of a non-life insurance policy. In this manner, the amount due and the amount payable can be offset or, if that is not possible, an attachment by garnishment can be imposed on the damage compensation that is payable.

- An example of compatible use is the bank that, upon concluding a mortgage loan, points out the possibility to a non-life insurer within the Group of sending a mailing to the Customer in question regarding household insurance.

- A healthcare costs insurer may also provide the name and address information and date of birth of its insured persons to a pension insurer within the Group, to enable the pension insurer to point out the advantages of supplementary pension insurance to the Data Subjects through a mailing. This cannot be regarded as incompatible with the purpose for which the Personal Data were obtained by the healthcare costs insurer. In addition, the healthcare costs insurer within the Group has a legitimate interest to make use of its Processing of Personal Data in respect of the insured parties in this manner to serve the interests of the other entities within the Group, while the privacy of the insured parties is not unreasonably infringed upon by this course of action. This would be different if the healthcare costs insurer applies selection criteria based on the ‘claim behaviour’ of the insured parties and then provides the results of this selection process to the occupational disability insurer that also belongs to the Group. Such use is ruled out in the Code of Conduct.

Quality of the Personal Data (article 4.5)
The quality of Personal Data comprises two aspects: First, no more Personal Data may be processed than necessary. The purpose of the Processing determines the amount and the type of Personal Data that may be processed. This follows from the words “adequate, relevant and not excessive”. Furthermore, Personal Data must be accurate. This latter condition is based on a best efforts obligation of the Controller. The Controller must take the necessary measures that are reasonably required in order to ensure that the Personal Data are correct and accurate. Therefore, this obligation is not an absolute obligation.

Retention period (article 4.6)
With regard to the retention of Personal Data by a Financial Institution, the following: The Controller must examine whether there are reasons to continue to record the Personal Data. If there are sufficient reasons, then the Controller can determine which periods apply for the retention of these Personal Data. In this case, article 10, first paragraph WBP, serves as the point of departure: Personal Data are not retained for a longer period than necessary for

realising the purposes for which the data are collected or subsequently processed. A Financial Institution shall draw up a policy regarding the retention periods of the Personal Data, the removal of the Personal Data and the possible transfer of these Personal Data to an archive destination. In this last case, the Personal Data shall only be used for archive management, the handling of disputes and carrying out (scientific, statistical or historical) research.

Obligation to provide information (article 4.7 up to and including article 4.9)
The ratio underlying the obligation to provide information is that the Controller can be called to account by the Data Subject. The norm is that the obligation to provide information applies, unless the Data Subject "is already cognizant". Depending on the circumstances, the Controller may assume that the Customer "is already cognizant", for example, because the relevant information has already been provided or sent to the Data Subject or because it is apparent from the conduct of the Data Subject that he is cognizant. When entering into a relationship with a Financial Institution it will usually be clearly indicated on the opening or application form what the purposes are for which the Personal Data are being collected. Financial Institutions can also inform the Data Subject about the Processing of Personal Data by means of terms and conditions, this Code of Conduct, relevant web sites and through a general notification at the CBP. The obligation to provide information also applies when the Financial Institution communicates with a Data Subject and processes Personal Data via the Internet. In this case, the obligation to provide information can be fulfilled by placing a privacy statement. If the Personal Data are collected without the knowledge of the Data Subject, then this obligation to provide information shall apply unless the party providing the information has already informed the Data Subject.

If informing the Data Subject is impossible or demands a disproportionate effort, then the obligation to provide information does not apply provided that the source of the Personal Data is recorded. If the Data Subject can be informed at a later date without this involving a disproportionate effort, the obligation to provide information may be fulfilled at a later date, for example, at the time when the Data Subject is contacted in writing. It is generally accepted that it is unfeasible to send a letter prior to the actual mailing in which it is indicated that the Personal Data of the Data Subject are being recorded with the purpose of sending them a mailing in the near future. It is therefore defendable that the obligation to provide information offers sufficient scope to combine this with the actual mailing.

The consistency principle and the obligation to provide information imposed on Financial Institutions are not absolute. In addition to the exceptions specified in article 4.7 and article 4.8 of the Code of Conduct, the obligation to provide information and the consistency principle do not apply provided that the exceptions referred to in article 9 of the Code of Conduct are satisfied.

Processor (article 4.12)
Financial Institutions may make use of the services of a Processor for the Processing of Personal Data. This Processor can be located both within and outside the Group as well as in countries within the European Economic Area (EEA) and outside the EEA. An agreement must be concluded between the Processor and the Controller, in which in writing, or in an equivalent form, inter alia, the technical and organisational security of the Processing of Personal Data are regulated. For an explanation regarding when it constitutes a Processor see the explanatory notes to article 2 of the Code of Conduct. For the rules that apply when it

concerns a Processor located in countries outside the EEA reference is made to the explanatory notes to article 8 of the Code of Conduct.

5. Purposes of the Processing of Personal Data

General

General (article 5.1)
The purposes for which a Financial Institution processes Personal Data concern the whole range of activities that a Financial Institution carries out in connection with an efficient and effective conduct of business. The Financial Institution has substantiated the purposes in several activities: In the first place, this concerns the assessment and acceptance of Customers and the activities possibly following there from such as entering into and executing agreements and the settlement of payment transactions. In the second place, Personal Data are used to carry out targeted marketing activities, to maintain and expand the relationship with the Customer, or to acquire new Customers. A third activity concerns, in a general sense, the risk management: combating, preventing and detecting behaviour directed against the Financial Institution or the sector in general. In addition, Financial Institutions are increasingly required to process Personal Data in order to comply with legal obligations. In connection with these activities, Customer relationship management is becoming more and more important, not in the least due to the obligations that are imposed by virtue of laws and regulations such as carrying out risk management, for instance, the Customer Due Diligence (CDD). In this context, the Wft and Wwft can be cited in particular.

More in general, it concerns the activities that are of importance for a Financial Institution as a whole in order to manage and maintain the relationship with the Customer. These activities are all interrelated. It concerns the total relationship with the Customer, including the Customer Screening, as required by the Wwft. The business operations can only be carried out effectively and efficiently when the activities are carried out in a coordinated manner. However, coordination of the activities does not automatically imply that all activities are compatible with each other. For instance, Special Categories of Data may not be used as selection criteria for marketing activities, unless the Data Subject has explicitly given his consent for this. This can be the case, for example, for ethnic marketing whereby immigrant population groups are approached for specific products. Use of the Personal Data in connection with various activities must constantly be assessed against the principles governing the Processing of Personal Data.

Entering into and executing an agreement (article 5.2)
Within the framework of efficient and effective business operations, Financial Institutions are increasingly making use of integrated customer information systems. These systems may only be used by employees within the Financial Institution who require the Personal Data for the fulfilment of their task. The fulfilment of tasks differs per employee and therefore also the access to Personal Data. The access to the integrated customer systems is not limited to the separate legal entities; it can apply to all entities within the Group. See also article 5.4 of the Code of Conduct.

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 and/or reconstruction purposes. For instance, this could concern providing name and address information of the (wrong) beneficiary to the party issuing the instructions in connection with an incorrect payment order.

Financial Institutions also make use of the services of other parties such as intermediaries and processing centres in various locations worldwide in connection with the settlement of payment transactions. As a result, Financial Institutions can provide Personal Data to countries outside the EEA. Parties issuing payment orders can be the subject of an investigation by authorised national authorities and authorised national supervisory authorities of the countries where such data is located in connection with the processing of the data both during and after the processing.

Statistical analyses (article 5.3)
Statistical analyses, including credit scoring and data mining, in which Personal Data (not being Special Categories of Personal Data) are processed, are not incompatible with the purpose for which the Personal Data have been collected. Credit scoring is a method to forecast the future payment behaviour of individuals based on a number of indicators. Data mining can be used in many areas, for example, analysing production processes. Data mining can be used to analyse existing information from a database, with the objective of identifying relationships in order to thus be able to steer business processes. To this end, the existing information is stored in a data warehouse. Information within a data warehouse is categorised according to the various subjects that can be of importance to an organisation. This information is then analysed.

In this analysis, distinction should be made between the phase in which profiles are created and the phase whereby, based on this profile, a score or characteristic is attributed to an individual. When creating group profiles at the time of entry, Personal Data may be processed, provided that measures are taken to ensure that the data are only used for statistical purposes when the analysis take place. These measures can consist of laying down in writing that the data shall not be used to take measures or decisions directed at a certain individual. This concerns a form of Processing that can be equated to the Processing for statistical purposes, because the result is a profile that cannot be related to an individual person.

On the other hand, if an individual is linked to that profile or credit score this does constitute the Processing of Personal Data. In that case, the Personal Data of an individual Data Subject are compared to a profile or score and the wider scope of the provisions for compatible use do not apply. It the attributing to an individual takes place in order to approach these individuals for marketing activities then this constitutes Processing in connection with marketing activities and it will have to be assessed whether such use is compatible with the purpose for which the Personal Date were obtained. In that case, the Data Subject can make use of his right to lodge an objection.

If Special Categories of Personal Data are required for statistical analysis, then the explicit consent of the Data Subject is required, unless requesting the Data Subject’s consent is impossible or involves a disproportionate effort. However, in that case, it must be examined whether the additional conditions have been satisfied, namely that the analysis must serve a general interest, that the Processing for the analysis in question is necessary and that in

performing the analysis the necessary safeguards are provided that the privacy of the Data Subject is not infringed upon disproportionately.

Marketing activities (article 5.4)
The use of Personal Data for marketing activities is governed by the general principle that such data must be fairly and duly processed. An elaboration of this is that preferably use is made of Personal Data originating form the Data Subject himself. If the Personal Data do not originate from the Data Subject himself, article 4.8 of the Code of Conduct applies with regard to the obligation to provide information. This means, for example, that in the event of the external purchase of Personal Data with the aim of approaching the Data Subject more efficiently through, for example, enrichment or mailing, the Data Subject shall be notified of the marketing purpose or, if this involves a disproportionate effort, that the source of the Personal Data shall be recorded. In addition, a processor agreement must be concluded with companies that act as Processors, such as mailing agencies. It must also be verified constantly whether the Data Subject has not invoked his right to demand exclusion from this type of Processing.

Various means of communication can be employed when carrying out marketing activities, such as mail, telephone and electronic means. Separate rules and conditions apply for each of these means of communication. As these mainly concern the rights conferred to the Data Subject in each case, these rules and conditions are further elaborated in the relevant sections (article 7.2 of the Code of Conduct).

Customers who purchase products from a company belonging to a Group may be approached by that particular company as well as the other companies belonging to the Group in connection with the marketing of products. Of course, in both cases, all conditions as specified in the Code of Conduct continue to apply. If the activity does not follow from the purpose of the activity for which the Personal Data have originally been collected, it should be examined whether the proposed Processing is incompatible with this. The extent to which the Customer has been informed about the composition of the Group also plays a role when weighing this. Such information can be provided, for instance, by means of an advertisement or a statement detailing the composition of the Group in communications aimed at the Customer. If it had been made sufficiently clear to a Customer, in one way or another, that the Financial Institution is part of a Group, the Customer may be approached by all entities of the Group for the purpose of marketing activities. The marketing of products and services that are offered by the members of a Group can therefore be deemed to be related. The Customer may always invoke his right of objection.

In connection with the settlement of payment transactions, distinction can be made between information that is processed in connection with the execution of the payment order, the so-called payment order data, and the information that a Customers provides in the information field. The payment order data may be used for marketing purposes, information in the information field may not be used for marketing purposes.

If a Financial Institution makes use of telemarketing, the Financial Institution must first check in the so-called 'do not call me' register whether the Data Subject has invoked his right to demand exclusion from telemarketing.

Security and integrity (article 5.5)
Within Financial Institutions, the department in charge of fraud and crime control is often a separate unit. This department also records events that could be of importance for the security and integrity of the Financial Sector and that therefore require special attention. This can concern various events ranging from the report of a stolen laptop to the suspicion that a certain individual is involved in a form of fraud or crime. These Personal Data are recorded in a so-called Incident Register. The Personal Data recorded in the Incident Register may, in principle, only be used within the Financial Institution or the Group to which the Financial Institution belongs. In order to prevent an uncontrollable use of these Personal Data, a limited set of data (name, address and date of birth) are recorded in an Internal Reference Register (IVR) that can be inspected by the departments in question in connection with, inter alia, Customer acceptance and claim adjustment. If it appears that a Data Subject is recorded in this Internal Reference Register, the Security Department must be contacted, which will then advise on the decision that should be taken. The Code of Conduct applies to this form of Processing of Personal Data and a separate report must be made to the CBP.

It is unavoidable that employees of the *customer business* of the Financial Institution also play a role in fraud and crime control. Employees of the *customer business* of the Financial Institution can, in this context, for example, report relevant events to the Security Department or, if necessary, request advice on the course of action with regard to a certain Customer. The Code of Conduct also applies in these cases.

If, after further investigation, it appears that the event is of such a nature that it satisfies the conditions stipulated in the Protocol, the information is recorded in the Incident Register and, when additional conditions are satisfied, in the External Reference Register. The Protocol and not the Code of Conduct applies to such a form of Processing.

In certain cases, the Personal Data in connection with credit applications, debts and events are also recorded in registers that are maintained by a legal person that is independent of the Financial Institution. Examples are the Credit Registration Agency Foundation BKR and the CIS Foundation, that act as Controllers for the Central Credit Information System (hereinafter: CKI) and for the Special Reports and the Confidential Notifications System (SVM). This Code of Conduct applies to recording Personal Data in and removing Personal Data from these systems. The Processing of the Personal Data in the systems themselves does not fall within the Code of Conduct.

A special form of Processing of Personal Data concerns Personal Investigation by insurers. A Personal Investigation can be necessary, for example, in order to ensure that no compensation is paid for fraudulent loss claims. The legitimacy of a claim will then, for instance, be verified through door-to-door enquiry or video recording. The Code of Conduct "Personal Investigation" also applies to these forms of investigation (Annex I: Document C).

Processing of Personal Data in connection with legal regulations (article 5.6)
In recent years, the number of obligations to collect and disclose Personal Data by virtue of legal regulations have increased. In addition to regulations that follow more or less logically from the legislation in respect of Financial Institutions, such as insurance laws, in particular, the obligation of the Customer Due Diligence has been added to this. For instance, in connection with the implementation of the EC Directives 2005/60/EC and 2006/70/EC, the Act for the Prevention of Money Laundering and Financing of Terrorism (*Wet ter voorkoming van witwassen en financieren terrorisme*, Wwft) was implemented. The act is a combination

of the Identification Provision of Services Act (*Wet ter identificatie bij dienstverlening*, Wid) and the Disclosure of Unusual Transactions Act (*Wet Melding ongebruikelijke transacties*, MOT).

The Wwft requires that the data of the document with which the identity was determined must be recorded. The recording of the data is in line with the obligation to carry out a Customer Due Diligence as specified in the Wwft. In view of the fact that the Wwft is risk based, this means that the Financial Institution has the possibility to gear the Customer Due Diligence to the risk sensitivity for money laundering or the financing of terrorism or to the type of Customer, the commercial relationship, the product or the transaction. This gives the institution the freedom to make its own choices, taking into account the risks and existing control measures. As is the case for the Wid and the MOT Act, an important role is reserved for the supervisory authorities in the Wwft. As proof of identification and verification – two requirements specified in the Wwft – Financial Institutions may – as under the WID – record a 'copy of the passport' in their records. The Wwft prescribes (summarised) two activities in the field of Customer Due Diligence and the Disclosure of Unusual Transactions. For the sake of good order, it should be observed that, in addition, there are many other legal regulations by virtue of which Financial Institutions are required to process certain Personal Data.

In many cases, Financial Institutions are required to record the Citizen's Service Number (*burgerservicenummer,* BSN) in their records. In addition, background information of Customers must be collected and checked. An example of this is the Financial Supervision Act (*Wet op het financieel toezicht*, Wft) that prescribes that when providing a loan a system of credit registrations must be consulted, such as, for example, the Central Credit Information System (*Centraal Krediet Informatiesysteem*, CKI), which is maintained by the BKR Foundation. This act also prescribes that information must be obtained about the financial position of the lender. The elaboration of the Decree prudential rules (*Besluit prudentiële regels*) takes this a step further and specifies that the Financial Institution must provide for a systematic analysis of integrity risks. Furthermore, this policy must also be implemented in procedures and measures that can be verified in an independent manner. It is also the case for insurers that the Wft prescribes that in some cases information must be obtained about the financial position, knowledge, experience, objectives and risk appetite of a customer, for example, when they advise on complex products (inter alia certain life insurance policies).

The obligation to make data available when this is demanded by investigating officers or supervisors is a totally different matter. In the case of a request to make information available this sometimes only concerns identifying data such as name, address or date of birth belonging to a bank account or insurance policy number. In other cases, the Public Prosecutor can demand additional information such as the period, the nature of the services provided, information about accounts and payment transactions. It can also occur that Special Categories of Personal Data are requested.

6. Processing of Special Categories of Personal Data

General

Personal data relating to an individual's state of health (article 6.1)
The Processing of Personal Data by a Financial Institution relating to an individual's state of health is subject to a number of supplementary regulations.

Subject to certain conditions, a Financial Institution may process Personal Data relating to an individual's health. The conditions under which this may take place our specified in article 6.1 of the Code of Conduct. For example, a Financial Institution can process Personal Data relating to an individual's state of health if this is necessary for the assessment of a Customer, the acceptance of a Customer or the execution of an agreement with a Customer. This is also the case when a Customer wishes to enter into an agreement with a Financial Institution in respect of a mortgage or life insurance.

When assessing the individual's state of health and the risks connected to this in connection with acceptance or an entitlement to insurance of a (prospective) insured party the Medical Adviser plays a central role. He carries out a medical investigation, whereby under strict conditions a medical examiner can be called in, and reports the results and conclusions to the insurer as part of his substantiated advice. The Medical Adviser is responsible for all Processing of Personal Data relating to an individual's state of health carried out by him and the persons who work on the investigation under his responsibility. The group of individuals who work under his responsibility are referred to as the medical staff or medical agency. When entering into an insurance agreement, the Data Subject has the right to be the first one to be informed of the results and conclusions of the investigation as referred to in Section 7:464, second subsection, under b of the WBGO and may decide, based thereon, whether the results and conclusions may be disclosed to others. In order to be able to exercise these rights, that Data Subject must submit a written request to the insurer.

The insurer takes a decision regarding the acceptance of the Customer or claim adjustment based on the advice provided by the Medical Adviser. Health statements must be sent to the Medical Advisor or his medical agency or staff. It is unavoidable that persons who are responsible for decision-making regarding acceptance or claim adjustment obtain insight into Personal Data relating to an individual's state of health, other than the Health Statement. They can obtain these Personal Data directly from a (potential) insured party, but also from the Medical Adviser. For instance, when a claim is submitted in the event of, for example, personal injury the injured person often indicates the nature of the injury unrequested. It is the Medical Advisers responsibility to determine which Personal Data relating to an individual's state of health are strictly necessary and may be disclosed in connection with taking a decision. The person taking the decision on the acceptance and the claim adjuster may only make use of this information in connection with the acceptance or claim adjustment. In this manner, a separation is created between the assessment of an individual's state of health in the form of an advice provided by the Medical Adviser and the decision that is taken by the insurer also based on this advice. The person taking the decision on the acceptance and the claim adjuster have a confidentiality obligation in this context under Section 21, second subsection of the WBP by virtue of their office, profession or legal regulations or by virtue of an agreement. It is also the responsibility of the Medical Adviser to determine which information relating to an individual's state of health may be disclosed to others working within the medical agency / on the medical staff in connection with providing the advice.

A Financial Institution also processes information relating to an individual's state of health in connection with the settlement of payment transactions. This is also the case when the information field in connection with a payment order contains information relating to an individual's state of health.

A Financial Institution may (further) process Personal Data relating to an individual's state of health when the Financial Institution has obtained the explicit permission of the Data Subject.

Personal Data relating to an individual's state of health that have been processed in connection with the assessment of a Customer, the acceptance of a Customer and the execution of an agreement with a Customer in connection with a specific product may not be used for the assessment of a Customer, the acceptance of a Customer or the execution of an agreement with a Customer in connection with another product without the consent of the Data Subject. If, for example, information relating to an individual's state of health is processed by a Financial Institution in connection with a life insurance policy that the Data Subject wishes to conclude with the Financial Institution, the Financial Institution may not use this information in connection with occupational disability insurance. This is permitted if the Data Subject has explicitly given his permission for this.

The Processing of Personal Data that are necessary in connection with the execution of the agreement does not fall under the responsibility of the Medical Adviser. For instance, the Processing of Personal Data relating to an individual's state of health does not fall under the responsibility of the Medical Adviser when this concerns drafting expense claims or legal proceedings or the handling of complaints. Processing of data whereby certain information relating to an individual's state of health, which was provide by or on behalf of the Data Subject in connection with the management of the relationship with the Customer, which is recorded in the administration, also does not fall under the responsibility of the Medical Adviser. This can concern specific situations, whereby, based on information regarding an individual's state of health, measures have to be taken in connection with the duty of due care with regard to investments or asset management. A serious illness or dementia are examples of this.

If an additional investigation takes place or Personal Data are collected from parties other than the Data Subject, the explicit consent of the Data Subject shall be requested.

Special rules of conduct have been drawn up for the processing of very specific Personal Data relating to an individual's health, such as Personal Data relating to heredity and HIV These rules have been laid down in the 'Genetic Research Moratorium' and the 'HIV Code of Conduct'.

Personal Data relating to criminal offences (article 6.2)
The Processing of Personal Data by a Financial Institution relating to criminal offences is subject to a number of supplementary regulations.

Subject to certain conditions, a Financial Institution may process Personal Data relating to criminal offences. The conditions under which this may take place our specified in article 6.2 of the Code of Conduct. For example, a Financial Institution may process Personal Data relating to criminal offences if this is necessary for the assessment of a Customer, the acceptance of a Customer or the execution of an agreement with a Customer. For instance,

in an insurance application, questions are asked regarding the criminal record of the applicant and of others insofar as this is necessary for concluding an insurance agreement. This concerns criminal offences in the last eight years. A Financial Institution may also process data relating to criminal offences if this is necessary in connection with the security and integrity of, inter alia, the Financial Sector. For instance, the Security Department of a Financial Institution may process Personal Data relating to fraud and crime. If this is necessary in connection with safeguarding the security and integrity, Special Categories of Personal Data may be processed in addition to information relating to criminal offences. A Financial Institution may always process data relating to criminal offences if the Financial Institution has obtained the Data Subject's consent.

The Financial Institution may make Personal Data relating to criminal offences, which have been perpetrated or which are expected to be perpetrated based on facts and circumstances against one of the Financial Institutions belonging to the Group, available within the Group. This also applies with regard to Personal Data that serve to detect possible criminal conduct directed against one of the Financial Institutions belonging to the Group. This is subject to the condition that the data are only made available to officers who require the data in connection with carrying out their task, as well as to the police and the Judicial authorities.

These Personal Data may only be made available to officers outside the Group if the Protocol is endorsed and complied with.

Other Special Categories of Personal Data (article 6.3)
In addition to Personal Data relating to an individual's state of health and data relating to criminal offences, Financial Institutions may also process other Special Categories of Personal Data in, inter alia, the following situations. In the first place, this concerns information that is provided together with other information, for example, the information field of a payment order. It can concern the information that it concerns the payment of the membership of a political party or church. The Processing of Personal Data also takes place through the storage of the original documents or (digital) copies of these documents. Furthermore, in some cases, the Citizen's Service Number (BSN) is recorded in the records of the Financial Institution. As specified in article 5.6 of the Code of Conduct, this only take place when legal grounds exist for this. In this case, the Personal Data may only be used for the purpose specified. It can also concern Personal Data regarding the ethnic background, which may only be used for marketing activities with the explicit consent of a Data Subject.

7. Rights of the Data Subjects

7.1 Inspection and rectification

General
The WBP confers rights on the Data Subjects: the right to inspect his own Personal Data and the right to rectify, supplement, remove or block these Personal Data. In addition, the Data Subject has the right to object and the right to be exempted from a decision taken solely on the basis of the automated processing of Personal Data.

The right to inspect the data and to rectify the data if necessary (article 7.1)
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. This overview must contain a description of the purpose of the Processing, the categories of Personal Data being Processed, the recipients or categories of recipients and the available information on the source of the Personal Data. The Controller must provide this overview to the Data Subject within four weeks of the date of receipt of the request.

A Financial Institution does not have to respond to an inspection request if the provisions stipulated in article 9 of the Code of Conduct have been fulfilled. For instance, an inspection request can be refused if it concerns matters such as the security of the Financial Institution and the prevention, detection and prosecution of criminal offences. Another example is the situation that, besides the Personal Data of the Data Subject, Personal Data of a Third Party are also being processed and this Third Party can have objections to the disclosure of his or her Personal Data as well. In this case, it must be assessed whether the information cannot be provided or whether it is possible to omit or erase the information regarding which the objection was raised.

Depending on the circumstances, it can be necessary that copies are provided of documents or excerpts of the data carriers on which Personal Data have been recorded. Exceptions can be made for: (i) documents, which the Data Subject already possesses (because, for example, he already received a copy) and of which he has been able to form an opinion and (ii) the recording of personal considerations of the employees which are also intended for internal consultations. Moreover, the request for copies may also be refused, in addition to the provisions stipulated in article 9 of the Code of Conduct, when it concerns misuse by the Data Subject himself or the requests constitutes a disproportionate burdening of the Financial Institution and leads to the infringement of the rights and interests of Third Parties.

In the interpretation of the right of inspection, jurisprudence is taken into account, such as, for example, the Dexia decision.

As part of the right of inspection, the Data Subject has the right to receive information regarding the logic of the automated Processing if use is made of special computer software. Examples include data mining programmes and the preparation of credit scores. The disclosure of the logic may not compromise the business secret or the intellectual property right, particularly the copyright protection of the software. However, this should not result in denial of access to all information.

An additional provision applies to the right of inspection. The Controller must see to it that the applicant is duly identified to ensure that the correct person is given access to the Personal Data. Therefore, in the event of a written inspection request, additional measures must be taken, such as the obligation to enclose a copy of a passport or driving licence, in order to be able to compare the signatures, possibly with signatures that are already on record.

Where appropriate, the Data Subject can request the Controller to rectify, supplement, remove or block the Personal Data if the data are incorrect, incomplete or irrelevant for the purpose or purposes of the Processing or are otherwise being processed in contravention of a legal regulation. When data are blocked this concerns situations whereby the Personal Data cannot be removed because the data could possibly be required to be used in

proceedings. In this case, technical or organisational measures must be taken to prevent other use.

Where a Controller has met a request to rectify, supplement, remove or block data, he is obliged to notify any Third Party, to whom he has provided the Personal Data in question, of the changes, unless this is impossible or would involve a disproportionate effort.

Right of objection and consent (article 7.2)
The WBP specifies the system of objection in further detail, distinguishing between relative and absolute objections. Relative objections may be lodged if the legal ground for Processing lies in the protection of the legitimate interests of the Controller. On the basis of his special personal circumstances, the Data Subject can request that the Processing of his Personal Data be terminated. In this case, the Controller must reconsider the Processing and weigh his interest against the (special) interest of the Data Subject.

This relative objection must clearly be distinguished from the objection that is possible when Personal Data are used for commercial, charitable or idealistic purposes. In this case, a variegated regulation applies, depending on the means of communication used.

The use of automatic calling systems without human intercession or a fax for Direct Marketing are only permitted when the Data Subject has given his prior permission for this ("opt-in").

The less stringent "opt-out" rules apply to making use of contact information for offering products and services by phone or mail. Use is permitted as long as the Data Subject has not indicated that he wishes to have this use blocked. Although, the possibility of "opt-out" must be pointed out to the Data Subject each time his Personal Data are used for marketing purposes. In that case, the use must be terminated immediately.

When the telephone is used, the existence of the 'do not call me' register, in which all requests for a block are recorded, must be pointed out to the Data Subject. In addition, before approaching a Data Subject by telephone for Direct Marketing purposes with regard to investment products, the Financial Institution must have obtained the prior permission of the Data Subject (“opt-in”).

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"). In that case, the absolute right of objection to have this use terminated immediately ("opt-out") must be pointed out to the Data Subject each time.

Obtaining and making use of Personal Data from the computer of a Data Subject (cookies) is only allowed when the Personal Data are necessary to assess the functioning of the system or in order to fulfil a request of the Data Subject. Any other use is only allowed if the Data Subject has openly been informed and he has not indicated that he does not consent to such a use.

Compensation of costs (article 7.3)
The Controller may demand a compensation for the costs of inspection of the Data Subject's own data or for exercising the relative right of objection, this charge may not exceed an amount laid down by order in council. The amount has been fixed at € 0.23 per page with a maximum of € 4.50. This maximum amount or even a higher amount, up to a maximum of € 22.50, may also be asked when it concerns a form of processing that is difficult to access or when it concerns many copies.[2]

Decisions based on automated processing (article 7.4)
The Controller must ensure that the Data Subject is not made subject to a decision that is solely based on automated processing if such decision could have legal consequences or could effect the Data Subject to a substantial degree. This involves, in particular, decisions taken on the basis of automated Processing that are intended to evaluate certain aspects of an individual's personality.

This regulation is not absolute and states that there are situations in which such a decision is permissible, for instance, where a decision is taken in connection with the conclusion or execution of an agreement and adequate measures have been taken, or where the decision is taken on legal grounds, in which measures have been laid down that serve to protect the legitimate interest of the Data Subject. Examples of this are the conclusion of an insurance or financing agreement and the Sections 4:32 and 4:34 of the Wft. Adequate measures include providing the Data Subject with an opportunity to express his view. In the event of a negative decision, the Data Subject must be informed of the logic on which the automated Processing of Personal Data is based.

8. Special subjects

General

Data Protection Officer (article 8.1)
The WBP provides for the possibility to appoint a Data Protection Officer. The Officer can act as an (internal) supervisor. The appointment of such an Officer is optional. The notification of the Processing of Personal Data can only be made to this Officer, who has been appointed by the Controller, if this Officer is registered with the CBP. Requests for a prior investigation may only be submitted to the CBP. In order to actually be able to carry out his supervisory task, the Officer must have access to all systems where Personal Data are possibly processed.

The exchange of information with countries outside the EEA (article 8.2)
The international exchange of information is of importance for Financial Institutions. For a Financial Institution, this often follows from the tasks that must be carried out such as the settlement of payment transactions and the execution of insurance agreements. When carrying out such tasks, it is necessary to make use of the services of other parties such as intermediaries and/or processing centres in various locations worldwide. Data Subjects can be the subject of an investigation by authorised national authorities of the countries where such data is located in connection with the Processing both during and after the processing.

[2] Decision on cost compensations rights of Data Subjects WBP (Government Gazette 2001, 305). See also decision of the CBP, z200-00052.

Disclosure of Personal Data to countries within the EEA is always permitted. The complexity of the regulations in the field of the disclosure of Personal Data to countries outside of the EEA is different for Financial Institutions than for other Controllers, because the emphasis lies primarily on the provisions stipulated in article 8.2.3 of the Code of Conduct. This article explicitly states that the exchange and disclosure of Personal Data are permitted when this is necessary for, inter alia, the execution of an agreement between a Data Subject and the Controller or when this is necessary for the conclusion and execution of an agreement to be concluded in the interest of the Data Subject. For example, this could concern international payment transactions at the request of Data Subjects, re-insurance agreements or the exchange of information in connection with damages or an accident in a foreign country. Disclosure can also take place if unambiguous permission has been obtained from the Data Subject, for example, through Customer Terms and Conditions or when it is necessary in connection with a compelling general interest. This interest can include the circumstance that a Financial Institution is subject to (foreign) laws and/or regulations of (foreign) supervisors as a result of which Personal Data must be disclosed based on (foreign) writs. If the Financial Institution is obliged, in this specific case, to disclose Personal Data, the Financial Institution shall take additional adequate measures to protect the interests of the Data Subject and, if necessary, consult with the CBP.

In the event one of the provisions of article 8.2.3 of the Code of Conduct cannot be invoked, then disclosure to countries outside the EEA is permitted provided that there is an adequate level of protection. It is also considered an adequate level of protection when the European Commission has decided that a given country offers adequate guarantees for the protection of Personal Data. Adequate guarantees for the protection of Personal Data can be offered, for example, through the implementation of approved Binding Corporate Rules within a Group. Binding Corporate Rules are rules that prescribe worldwide within a Group how Personal Data must be processed. If Binding Corporate Rules have been implemented within the Group, the Personal Data can be exchanged within the Group in accordance with the provisions in the Binding Corporate Rules. In the event of disclosure of Personal Data to a Processor or Controller in the United States, the regulations can be made use of as laid down in the Safe Harbour Principles, provided that the receiving party has endorsed these principles.

Disclosure to a Financial Institution is always allowed if permission has been granted for this based on article 77 subsection two of the WBP.

Protection of Personal Data (article 8.3)
Financial Institutions attach great importance to the protection of Personal Data and therefore, they take adequate measures in connection with the electronic exchange of Personal Data. A protection policy is almost always developed in which it is described concretely which organisational and technical measures must be taken to protect Personal Data from theft and unauthorised access. When determining the adequate level of protection, the state of technology, the costs of implementation, the risks entailed in the Processing and the nature of the to be protected Personal Data are taken into account.

Camera surveillance (article 8.4)
A Financial Institution may make use of camera surveillance subject to the conditions specified in article 8.4 of the Code of Conduct. For example, camera surveillance is permitted when this is necessary for the security of a Financial Institution or its Customers and employees, for the detection of criminal offences or establishing the violation of (company)

rules and as support in legal proceedings. Furthermore, the recording must take place selectively, that the data may not be stored longer than necessary and the necessary organisational and technical measures must be taken to protect the Personal Data. If the Customer request this, further information shall always be provided. Where appropriate, inspection can also mean the request for inspection of the images referred to here. In that case, the Financial Institution can ask the person submitting the request to provide the day and time of the contact.

Recording telephone conversations (article 8.5)
The Financial Institution may record telephone conversations subject to the conditions stipulated in article 8.5 of the Code of Conduct. For example, recording telephone conversations is permitted when complying with a legal obligation, for providing evidence, for (fraud) investigation and detection, for evaluation of the quality of the service and for training, coaching and appraisal purposes. Furthermore, the data may not be stored longer than necessary and the necessary organisational and technical measures must be taken to protect the Personal Data. The reason for recording the telephone conversations is, inter alia, that afterwards the contents of the order can be verified, if this is necessary, for example, in connection with a dispute with a Customer. An example of this could be an order to buy or sell securities. Another reason to record a telephone conversation is, for example, recording the exact time at which the loss of theft of a bankcard was reported or if it concerns threats directed against the Financial Institution or its employees. Financial Institutions will inform their Customers in general about the recording of this communication, for example, through the product terms and conditions and this Code of Conduct. The Financial Institution shall also instruct its personnel with regard to this. If the Customer request this, further information shall always be provided. Where appropriate, inspection can also mean the request for inspection of the communication referred to here. In that case, the Financial Institution can ask the person submitting the request to provide the day and time of the conversation or the contact.

Recording communication (article 8.6)
Communication information is recorded within Financial Institutions at various occasions. This mainly occurs because orders are submitted increasingly using other than the traditional written and verbal means of communication. Electronic means of communication play an increasingly larger role. 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

General
The consistency principle, transparency principle and the rights of the Data Subject are specified in the articles 4.4, 4.7, 4.8, 4.9, 7.1.1, 8.4.5 and 8.5.4 of the Code of Conduct can be set aside in special situations if there are urgent reasons for this, which necessity is more compelling that the rights and freedoms of the Data Subject. This could be the case, for example, if a Financial Institution is subject to an investigation carried out by a supervisor or the tax and customs administration. Also in the case of fraud investigation that is carried out by the Financial Institution or in connection with possible legal proceedings, it can be of importance not to inform Data Subjects of this if this could harm the investigation.

10. Compliance with the Code of Conduct

General

Financial Institutions attach great importance to the correct compliance with the rules of the WBP and the Code of Conduct. The principle of responsibility for the Processing of Personal Data implies that the Financial Institution has sufficient insight into the various forms of Processing of Personal Data. In this context, Financial Institutions have implemented a system of self-evaluation in order to also ensure compliance with the WBP and this Code of Conduct. The (i) audit department appointed by a Financial Institution contributes to the control by periodically, preferably annually, verifying through a form of self evaluation in which manner the Processing of Personal Data is carried out. Within the Financial Institution, the (ii) management of the institution is also responsible for the compliance with laws and regulations. In addition, (iii) Compliance or another department charged with supervision must ensure that the Processing of Personal Data takes place within the legal framework.

The abovementioned departments of Financial Institutions can also draft reports regarding the compliance with the WBP. Depending on the outcomes of these reports and the nature and extent of the individual Processing of Personal Data, it shall be specified with regard to which activities additional investigation should take place. In order to ensure the compliance with the rules of the WBP and the Code of Conduct, a Financial Institution is also required to draw up and implement internal instructions, which specify in which manner the Personal Data are to be processed within the Financial Institution. The instructions concern, in any case, those items of which the Financial Institution is of the opinion that further clarification is desirable. This concerns many subjects such as security manuals and documents in which it is described which technical and organisational measures have to be taken. In addition, this could concern, for example, a regulation regarding recording telephone conversations.

11. Disputes

General

The Netherlands Bankers' Association (NVB) and the Dutch Association of Insurers (VvV) are members of the Arbitration Institute for Financial Services (*Klachteninstituut Financiële Dienstverlening*, KiFiD). The aim of this independent institute is to offer one counter for resolving disputes with Financial Institutions. The Ombudsman and the Arbitration Committee that work within the KiFiD offer an alternative for court proceedings. In a relatively short period of time, an attempt is made to find a solution in consultation with the service provider in question or an opinion is expressed regarding the issue.

The procedures that are possible are the following: Each Financial Institution has an internal complaints handling or arbitration procedure. If the complaint is not handled or not handled to the satisfaction of the Data Subject, the Data Subject can submit the dispute to the KiFiD within three months after following this internal complaints procedure. The decision based on the internal arbitration procedure of the Financial Institution constitutes a decision in the sense of Section 46 of the WBP. If the dispute pertains to the right of inspection / rectification and is submitted to the KiFiD within six weeks after the decision of the internal arbitration procedure of the Financial Institution, based on Section 47 of the WBP the period of six weeks within which the Data Subject has the right to submit the case to the CBP or - by means of an appeal procedure – to the court will be suspended, to be counted as from the time of submission up to the end of the procedure at the KiFiD. If the Data Subject only

submits the dispute to the KiFiD after the end of the period of six weeks, it is, of course, no longer possible to make use of the procedure of Section 46/47 of the WBP.

The Data Subject also has the right, at his own option, to disregard the internal arbitration procedure of the Financial Institution in question and submit a dispute directly to the CBP or the court. As a result, he forfeits his right to make use of the internal arbitration procedure of the Financial Institution as well as, subsequently, his right to make use of the arbitration procedure of the KiFiD.

For more information about the KiFiD, we refer to the following web site: www.kifid.nl or the Arbitration Institute for Financial Services (*Klachteninstituut Financiële Dienstverlening*, Kifid), PO Box 93257, 2509 AG The Hague, telephone 0900-klacht or 0900-35552248 (€ 0.10 per minute).

For questions regarding the Code of Conduct, you can also contact the NVB, PO Box 3543, 1001 AH Amsterdam, telephone 020 55 02 888 or by e-mail info@nvb.nl or you can contact the Dutch Association of Insurers (VvV), PO Box 93450, 2509 AL The Hague, telephone 070 333 8500 or by e-mail: Gedragscode_Privacy@verzekeraars.nl.

Annex I: Information

The following documents have been included as information with this Code of Conduct.

A. Regulation Information Tax and Customs Administration / Banks
B. Protocol Incident Warning System Financial Institutions
C. Code of Conduct Personal Investigation
D. Genetic Research Moratorium Dutch Association of Insurers
E. HIV Code of Conduct
F. Protocol Insurance Examinations