

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

1. Preamble
2. Definitions
3. Description of the sector, scope and data subjects
  - 3.1 The sector
  - 3.2 Scope
  - 3.3 Data subjects
4. Principles governing the processing of personal data
5. Processing of personal data
  - 5.1 General
  - 5.2 Processing of personal data relating to the assessment and acceptance of (potential) customers, the conclusion and performance of contracts with a data subject and the settlement of payment transactions
  - 5.3 Processing of personal data relating to analyses for statistical and scientific purposes
  - 5.4 Processing of personal data relating to marketing activities
  - 5.5 Processing of personal data relating to security and integrity, as well as the use of warning systems
  - 5.6 Processing of personal data in connection with legal regulations
6. Processing of special categories of personal data
  - 6.1 Personal data relating to a data subject's state of health
  - 6.2 Personal data relating to criminal offences
  - 6.3 Other special categories of personal data
7. Rights of the data subjects
  - 7.1 Notice and rectification
  - 7.2 Objection
  - 7.3 Compensation
  - 7.4 Decisions based on the automated processing of personal data
8. Special subjects
  - 8.1 Officer
  - 8.2 Data exchange with countries outside the European Union
  - 8.3 Protection of personal data
  - 8.4 Camera surveillance
  - 8.5 Recording of telephone conversations

9. Auditing and supervision

10. Disputes

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

1. General

2. Notes to a number of articles

2.1 Introduction

2.2 Definitions

2.3 Description of the sector, scope and data subjects

2.4 Principles governing the processing of personal data

2.5 Processing of personal data

2.6 Rights of data subjects

ANNEX 1: Information

## 1. Preamble

- 1.1 As part of their business operations, banks and insurers (hereafter: ‘financial institutions’) process personal data and find it important that these personal data are handled with due care and that they are treated as confidential.
- 1.2 The Data Protection Act (*Wet bescherming persoonsgegevens*), hereafter: 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*), hereafter: NVB, and the Association of Insurers (*Verbond van Verzekeraars*), hereafter: VvV, have drawn up earlier codes of conduct relating to the Data Protection Act (Privacy Code of Conduct for the Banking Industry (Netherlands Government Gazette 207, 25 October 1995), and the Code of Conduct for the Processing of Personal Data in the Insurance Industry (Netherlands Government Gazette 44, 5 March 1998), in which legal regulations are worked out in further detail.
- 1.4 NVB and VvV wish to make their respective codes of conduct consistent with the WBP and integrate them into the Code of Conduct for the Processing of Personal Data by Financial Institutions (hereafter: Code of Conduct).
- 1.5 The Code of Conduct aims:
  - a. to provide financial institutions with guidelines on the treatment 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 in respect of the personal data processed and to be processed by financial institutions.
- 1.6 Based on section 25 of the WBP, NVB and VvV have asked the Board for the Protection of Personal Data (*College bescherming persoonsgegevens*), hereafter: CBP, to assess whether this Code of Conduct is a correct elaboration of the WBP and/or any other legal regulation governing the processing of personal data.
- 1.7 CBP has assessed this Code of Conduct and subsequently declared that [...].

## 2. Definitions

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

- a. Filing system: 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 a personal data relates as detailed in 3.3.
- c. Processor: the individual processing personal data on behalf of the controller without being subject to his direct control.

- d. Special categories of personal data: personal data relating to a subject's religion or philosophy of life, race, political persuasion, health, sex life, membership of a trade union, as well as criminal offences and personal data relating to unlawful or objectionable conduct in connection with a ban imposed in respect of such conduct.
- e. Special risk: the situation in which an individual is denied compensation as a result of the deliberate provision of incorrect information, or if an insurance policy has been cancelled or otherwise terminated as a result of the provision of incorrect information on the loss experience.
- f. CBP: the Data Protection Board (*College bescherming persoonsgegevens*), as referred to in section 51 of the WBP.
- g. Customer: the natural individual with whom a financial institution maintains or has maintained a legal relationship, or the natural person who has indicated that he is considering to enter into a relationship with a financial institution.
- h. Third party: any individual other than the data subject, the controller, the processor, or any other individual, who, under the direct control of the controller or the processor, is authorised to process personal data.
- i. Financial institution: a bank and/or insurer.
- j. Officer: the individual in charge of data protection as referred to in section 62 of the WBP.
- k. Functional unit: the group of individuals involved in a direct or similar fashion in the purpose for which medical data have been requested or provided.
- i. Code of conduct; the Code of Conduct for the Processing of Personal Data by Financial Institutions.
- m. Group: the economic unit in which legal entities and companies are connected organisationally and to which a financial institution belongs.
- n. Personal data: any information relating to an identified or identifiable natural person.
- o. Controller: the legal person, which alone or jointly with others, determines the purposes and means of the processing of personal data, or the legal person designated for this purpose within a Group.
- p. Processing of personal data: any operation or set of operations which is performed upon personal data, such as collection, recording, organisation, storage, alteration, consultation, use, disclosure and destruction.
- q. WBP: Data Protection Act (*Wet bescherming persoonsgegevens*).

### **3. Description of the sector, scope and data subjects**

### **3.1 The sector**

The code of conduct applies to credit institutions that are members of the Netherlands Bankers' Association (*Nederlandse Vereniging van Banken, NVB*), as well as to any banks associated with Rabobank Nederland and to insurers that are members of the Association of Insurers (*Verbond van Verzekeraars*).

### **3.2 Scope**

This code of conduct shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system where such is effected by a financial institution as part of normal business operations. The processing of personal data in connection with incident registers by the security departments of financial institutions and the processing of personal data in the capacity of employer fall outside the scope of this code of conduct.

### **3.3 Data subjects**

Within the framework of the activities set out in article 5, the personal data of the following data subjects are processed:

- a. customers;
- b. individuals whom a financial institution aims to approach in order to persuade them to enter into a legal relationship;
- c. individuals approaching a financial institution;
- d. individuals whose personal data a financial institution is obliged to process under a legal regulation (for instance permission from the spouse under section 88, book 1 of the Dutch Civil Code) or in view of prevailing terms of prescription;
- e. individuals whose personal data a financial institution is obliged to process in connection with contractual or legal obligations vis-à-vis a customer or a third party.

## **4. Principles governing the processing of personal data**

- 4.1 Personal data shall be processed fairly and lawfully.
- 4.2 Personal data shall be collected for specified, explicit and legitimate purposes.
- 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 explicit consent for the processing of personal data;
  - b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - c. processing of personal data is necessary for compliance with a legal obligation to which the controller is subject;
  - d. processing of personal data is necessary in order to protect the vital interests of the data subject; or

- e. processing of personal data is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the personal data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject, particularly the right to privacy.

4.4 Personal data shall not be processed in a way that is inconsistent with the purposes for which they have been collected.

4.5 The controller shall take measures to ensure that personal data, taking into account the purposes for which they are processed, are accurate, sufficient, relevant and not excessive.

4.6 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 the personal data of the data subject, unless the controller may assume on reasonable grounds that the data subject is already cognizant of this. This obligation to provide information shall be fulfilled before the data are obtained.

4.7 If the personal data are obtained in any other way, the controller shall inform the data subject of this at the time of undertaking the recording of the data, or, if the personal data are destined to be provided to a third party, at the time when the data are first disclosed. The obligation does not apply if the data subject is already aware of this or if 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. Nor does the obligation apply if the recording or provision of the data is prescribed by or under the law.

4.8 If, in view of the nature of the data, the circumstances in which they are obtained or the use that is made of them, such is vital to the safeguarding of the fair and careful processing of personal data, additional information shall be provided to the data subject besides the information referred to in 4.6 and 4.7.

4.9 Within the framework of their on-line business operations, financial institutions may record and further process personal data of data subjects approaching a financial institution through the Internet. By means of a Privacy Statement on their web sites, financial institutions shall make information available on the policy concerning personal data obtained through the Internet. The statement shall contain at least the information as referred to in article 4.6.

## **5. Processing of personal data**

### **5.1 General**

5.1.1 Subject to the principles governing the processing of personal data, the processing of personal data by financial institutions is effected within the framework of an efficient and effective business management, with a particular focus on the following activities:

- a. the assessment and acceptance of (potential ) customers, the conclusion and performance of contracts with a data subject and the settlement of payment transactions;
- b. the performance of analyses of personal data for statistical and scientific purposes;
- c. the performance of (targeted) marketing activities designed to establish a relationship with a data subject and/or maintain or extend a relationship with an existing customer;
- d. the safeguarding of the security and integrity of the sector, including the fight against and the prevention and investigation of (attempts at) (punishable) conduct directed against the industry to which a financial institution belongs, the group to which a financial institution belongs, the financial institution itself, its customer base and staff, as well as the use of and participation in warning systems;
- e. the fulfilment of legal obligations.

5.1.2 Financial institutions shall not process more personal data than is strictly necessary. They shall make these personal data only available to employees within the group, who, subject to the principles governing the processing of personal details, are authorised to handle these data.

5.1.3 Where necessary, financial institutions shall state their specific activities in the registration with the CBP, or, where applicable, with their own officer.

## **5.2 Processing of personal data relating to the assessment and acceptance of (potential) customers, the conclusion and performance of contracts with a data subject and the settlement of payment transactions.**

5.2.1 Personal data are collected relating to the assessment and acceptance of (potential) customers and the conclusion and performance of a contract. Insofar as this involves personal data relating to health and criminal convictions, the provisions of paragraph 6 shall apply.

5.2.2 Factual data relating to claims submitted under the contracts or a certain well-defined category thereof, concluded with the financial institutions, may be forwarded to a central disclosure office set up by or for the participating financial institutions relating to activities aimed at preventing and combating fraud. For the assessment and acceptance of (potential) customers, financial institutions may provide data to and remove them from warning systems. This code of conduct does not apply to such warning systems.

5.2.3 Within the framework of the normal settlement of payment transactions, a financial institution forwards personal data to the other party. Also, unless otherwise agreed, additional data are provided to the parties involved in the further processing of personal data insofar as these are, in reason, needed for verification and reconstruction purposes.

5.2.4 Within the framework of the implementation of payment transactions, financial institutions may use the services of a processor.

### **5.3 Processing of personal data relating to analyses for statistical and scientific purposes**

5.3.1 The processing of personal data for historical, statistical or scientific purposes shall not be regarded as incompatible with the purposes for which they were collected in the first place if the controller has made the necessary provisions to ensure that the further processing of personal data shall be effected for these specific purposes only.

5.3.2 Data warehousing and the analysis of the personal data stored in such data warehouse shall be considered as the processing of personal data for statistical purposes if the provisions of the preceding paragraph are met.

5.3.3 In order to target marketing activities at certain groups, personal data may be analysed that have been collected within the framework of marketing activities.

### **5.4 Processing of personal data relating to marketing activities**

5.4.1 If it has been made sufficiently clear to the customer that the financial institution to whose customer base the customer belongs is part of a group, and that the financial institution considers the customer as a customer of the group, the customer may be approached by all group companies for the purpose of marketing activities, provided that the other provisions of the Data Protection Act have been met.

5.4.2 Marketing activities primarily make use of personal data originating from the data subject himself. As a rule, if any personal data are used that have not been obtained from the data subject himself, the origin of the personal data shall be recorded and the financial institution shall satisfy itself that the WBP is complied with.

5.4.3 When the occasion arises, specialised firms are called in to handle marketing activities. Financial institutions shall ensure that a processor contract is concluded with these firms, which contains the obligations a processor should fulfil within the framework of the WBP and shall ensure due compliance.

5.4.4 Payment transactions may involve an exchange of information needed for the proper settlement of a payment order. The financial institution shall consider the content of such information as confidential and shall refrain from using it for marketing activities.

5.4.5 In the event of marketing activities, it shall always be ascertained whether a customer has made use of his or her right of objection as referred to in paragraph 7.2, in relation to the processing of personal data for these purposes.

### **5.5 Processing of personal data relating to security and integrity, as well as the use of warning systems**

- 5.5.1 The processing of personal data of the data subjects other than by the security department or an officer authorised for this purpose comes within the scope of this code of conduct.
- 5.5.2 If these personal data are entered in a warning system for the use of Dutch-based financial institutions, in respect of which a financial institutions does not act as controller, the code of conduct shall not apply.
- 5.5.3 Insofar as the processing of personal data, including personal data of individuals other than a data subject, is effected within the framework of the security and integrity of the sector by a security department or an officer authorised for this purpose, this code of conduct shall not apply. In view of the nature of the processing and the special measures taken to protect the personal data, the conditions governing such processing of personal data has been laid down in the ‘Protocol in respect of the Incident Warning System for Financial Institutions’ (*Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*).
- 5.5.4 The investigation into the facts of the incident shall be subject to the ‘Code of Conduct for Personal Investigations’.

## **5.6 Processing of personal data in connection with legal regulations**

- 5.6.1 In view of the legal regulations, financial institutions are obliged to provide information on their customers and other data subjects to government institutions and other institutions. The most essential legal obligations are set out below.
- 5.6.2 Disclosure of Unusual Transactions (Financial Services) Act (*Wet melding ongebruikelijke transacties, Wet Mot*): under the Disclosure of Unusual Transactions (Financial Services) Act, a financial institution is obliged to disclose unusual transactions to the legal reporting office, which has to assess whether these data might be relevant to the prevention and investigation of crimes. Which transactions should be qualified as unusual is determined by means of an indicator list. A financial institution is obliged to keep such disclosures confidential.
- 5.6.3 Identification (Services) Act (*Wet identificatieplicht bij dienstverlening, Wid*): Under this act, a financial institution is obliged to establish the identity of a customer before providing a service to such customer. The customer’s identity is established by means of documents detailed or referred to by the act. In connection with this, a financial institution shall record and keep on file a number of specific data.
- 5.6.4 Provision of information to the tax authorities: Financial institutions are obliged to provide information on their customers to the tax authorities. Reference is made to the tax Authorities/Banks Information Regulation (*Voorschrift Informatie Fiscus/Banken*).
- 5.6.5 Credit System (Supervision) Act 1992 (*Wet toezicht kredietwezen 1992*): Under the Credit System (Supervision) Act 1992, De Nederlandsche Bank N.V. is authorised to collect any information from certain financial institutions that it

deems vital to its regulatory task. This will only occasionally result in a request for information on customers.

- 5.5.6 Insurance Industry (Supervision) Act 1993 (*Wet Toezicht Verzekeringsbedrijf 1993*): Under the Insurance Industry (Supervision) Act 1993, the Pension and Insurance Supervisory Board is authorised to collect any information it deems vital to the exercise of its regulatory task. This will only occasionally result in a request for information on customers.
- 5.6.7 Foreign Financial Relations Act 1994 (*Wet financiële relaties buitenland 1994*): Under this act, every institution is obliged to provide such information and data to De Nederlandsche Bank N.V. as are or may be important to the preparation of the balance of payments of the Netherlands and/or ensuring compliance with international treaties concerning the movement of capital and goods. To the customer, unless he is a resident of a country that is subject to United Nations sanctions, or unless he occurs on a list of individuals who are subject to a sanction, the submission to De Nederlandsche Bank N.V. of data needed for the preparation of the balance of payments shall be relevant only. In the event of payments involving larger sums of money, the relevant data (ordering customer, amount, nature of the payment, payee, etc.) will be forwarded to De Nederlandsche Bank N.V.
- 5.6.8 Securities Transactions (Supervision) Act 1993 (*Wet toezicht effectenverkeer 1993*): Under this act the financial institution may be required to provide data concerning financial transactions to investigative authorities within the framework of the fight against insider trading. See also section 42 of the Specific Regulation on the Supervision of the Securities Industry 1999 (*Nadere Regeling Toezicht Effectenverkeer 1999*) (Netherlands Government Gazette 1999, no. 12, p. 8 ff).
- 5.6.9 Consumer Credit Act (*Wet consumentenkrediet, Wck*): Under the Wck, financial institutions engaged in extending loans to natural persons falling within the scope of the Wck, should join a 'systeem of credit registrations' (section 14, paragraph 2 Wck). The Tiel-based Central Credit Registration Office (*Bureau Krediet Registratie, BKR*) operates such a credit registration system. Lenders provide data relating to the origin and settlement of financing to the BKR and also have the data submitted by other lenders at their disposal. The nature of the recorded data, the conditions for recording, use and provision and the rules for removing the data are laid down in the BKR rules and regulations. There is also a BKR code of conduct. Furthermore, in case of a dispute, individuals registered with BKR, as well as having the possibility provided in section 60 of the Data Protection Act, may apply to the BKR arbitration committee.
- 5.6.10 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 tax and social insurance number (*SOFI-nummer*) as a mandatory identifier on the information to be submitted for taxation purposes.
- 5.6.11 Decree on the use of the tax and social insurance number: Under this decree, insurers as referred to in section 2, fourth paragraph, under b of the Pensions and

Savings Funds Act may use the tax and social insurance number for the implementation of pension schemes. The insurers are only allowed to use this number insofar as such is necessary for the performance of their tasks or for the due performance of statutory duties and in the transactions with the person to whom this number relates and in their contacts with the individuals and institutions insofar as these are entitled themselves to use the tax and social insurance number.

## **6. Processing of special categories of personal data**

### **6.1 Personal data relating to a data subject's state of health**

- 6.1.1 Under the responsibility of the medical advisor, collecting data relating to a data subject's state of health is reserved for individuals who are part of the Functional Unit. Reports of a medical officer, a medical expert and/or the Working Conditions Service (*Arbodienst*), as well as information from the therapeutic sector, shall be entered in the medical file that is kept under the responsibility of a medical advisor. The data subject has the right – preferably through a trusted doctor appointed by him or her – to inspect fully a medical file relating to him or her, except for the notes of the medical advisor, and to receive copies thereof, unless such would violate the right of privacy of the third parties discussed in the report.
- 6.1.2 If, within the framework of acceptance and/or claims handling a customer is asked to undergo a medical examination or an additional examination, the insurer shall point out in the medical examiner's documents the importance of identification in order to prevent mistaken identity.
- 6.1.3 The collection of data relating to a data subject's state of health from parties other than the data subject may only be effected after the data subject has authorised such collection. The authorisation shall be worded in such a way that it is solely directed towards the provision of permission for inspection or provision of data needed for handling a concrete case. The data subject about whom information is requested shall be informed on the nature of the information to be requested, as well as the purpose thereof. The authorisation shall also show that the data subject has been informed on the above.
- 6.1.4 Within the framework of the provision of certain services and/or products, personal data relating to an individual's state of health, in the form of customers' own statements, have to be processed. These personal data shall be treated as strictly confidential and only be processed insofar as such is necessary for:
- a. the assessment of the risk to be insured and whether the data subject has made no objection, or
  - b. implementation of an insurance contract, or
  - c. implementation of a financing contract and whether the data subject has given his explicit consent.
- 6.1.5 Data relating to an individual's state of health, that have been processed with a view to the assessment of a risk to be insured or the implementation of an insurance or financing contract shall not be used within the framework of the

assessment of the risk to be insured in respect of another insurance and/or the implementation of another insurance contract or financing contract without the data subject's consent.

6.1.6 The processing of personal data relating to hereditary traits is subject to the 'genetic research moratorium' (*moratorium erfelijkheidsonderzoek*). The text of the moratorium has been attached to this code of conduct as an annex.

6.1.7 The processing of personal data relating to an individual's state of health that can be derived from a blood test is subject to the 'code of conduct for HIV' (*HIV-gedragscode*). The text of the code of conduct for HIV has been attached to this code of conduct as an annex.

## **6.2 Personal data relating to criminal offences**

6.2.1 In view of a sound acceptance policy, financial institutions may inquire about facts relating to a possible criminal record of individuals to be insured and others whose interests are (co-insured on the insurance policy applied for (including directors and shareholders of legal entities) insofar as these facts relate to a period of 8 years prior to the date of the insurance application. In this regard, the criminal record stated may only be used for the assessment of the insurance and/or financing application and legally obtained data relating to a criminal record may be used within the framework of an individual's invoking the right to remain silent as referred to in section 251 of the Commercial Code.

6.2.2 Criminal data relating to crimes committed against any of the financial institutions belonging to a Group, or data serving to establish possible punishable conduct vis-à-vis any of the financial institutions belonging to a Group may be forwarded to all legal entities belonging to such a Group, provided that the data are solely provided to functionaries who need such data for the discharge of their duties.

## **6.3 Other special categories of personal data**

6.3.1 Payment orders may contain special categories of personal data, such as trade union data. Execution of the payment orders implies that such personal data are processed. The processing of personal data is effected, amongst other things, through the filing of the original documents or the copies thereof, whether or not in an electronic form. Such data may only be used if such is necessary for furnishing proof.

6.3.2 Special categories of personal data are processed in connection with the use of camera surveillance as set out in paragraph 8.4, The processing of these personal data is unavoidable in view of the identification of the data subject.

## **7 Rights of the data subjects**

### **7.1 Notice and rectification**

7.1.1 A subject is entitled to apply in writing to a financial institution for an overview of the personal data relating to him or her, which are processed by this financial

institution. Barring the exceptions mentioned in the Data Protection Act, the financial institution shall send the data subject an overview of the personal data and information relating to the processing of these personal data within four weeks after the date of the application. If the financial institution does not process any personal data of the data subject, the financial institution shall inform the data subject of this also within four weeks after the date of the application.

7.1.2 If the overview shows that the personal data are factually incorrect, incomplete or irrelevant for the purpose of the processing operation or are otherwise processed in contravention of this code of conduct or the Data Protection Act, the data subject may request in writing for rectification, addition, erasure or blocking of the data in question. A financial institution shall notify the data subject within four weeks after receipt of such request, in writing, whether or to what extent the request will be met. If the data subject's request cannot be met, or cannot be fully met, the reasons for this shall be duly given.

7.1.3 The above-mentioned requests for inspection or rectification shall be addressed to the controller instigating the processing. The request for rectification shall contain a specification of the personal data that need to be rectified. The controller shall ensure that the person making the request is duly identified.

7.1.4 If it is unclear to the data subject who acts as controller, for instance because the institution is part of a group, the data subject may address his request to the management of the financial institution which (he thinks) is handling the processing of his personal data. The management shall ensure that the request is duly handled.

## **7.2 Objection**

7.2.1 If the legal ground for the processing of the personal data is comprised of the legitimate interest of the controller or of a third party to whom the data have been forwarded, the data subject shall have the right to lodge an objection against the processing of personal data in connection with his special personal circumstances. The controller shall assess within four weeks whether the objection is justified. In that case the processing of personal data of such data subject shall be ceased with immediate effect.

7.2.2 If a financial institution processes personal data with a view to solicitation for commercial or charitable purposes, a data subject may lodge an objection to this at any time free of charge. In case of objection, the financial institution shall take measures to ensure that this form of processing of personal details is ceased with immediate effect. If the data subject is directly notified for the purposes referred to above, the possibility of lodging an objection shall be pointed out to him at any time.

## **7.3 Compensation**

7.3.1 For a request as referred to in articles 7.1.1 and 7.2.1, the controller may demand compensation to offset costs. Such charge shall not exceed the amount laid down by order in council.

7.3.2 If the data are adapted, changed or erased as referred to in article 7.1.2, or if the objection is upheld, the amount referred to in the previous paragraph shall be refunded.

#### **7.4 Decisions based on the automated processing of personal data**

7.4.1 Taking a decision solely based on the automated processing of personal data intended to evaluate certain personal aspects relating to an individual's personality shall only be allowed if:

- a. such decision is taken in the course of the entering into or the performance of a contract, or
- b. such decision is authorised by law which also lays down measures to safeguard the data subject's legitimate interests.

7.4.2 If the decision does not satisfy the data subject's request, he shall be enabled to put his point of view forward. In that case, the controller 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 may be deemed sufficiently reliable may be appointed as officer. For the discharge of his task, the officer shall be independent from 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 in a due manner and shall ensure that his activities will not be detrimental to himself. In connection with this task he shall have protection against dismissal.

8.1.2 The officer shall ensure that the financial institution complies with the regulations by or under any law that contains regulations governing the processing of personal data, and that it complies with the regulations laid down in this code of conduct. He shall prepare an annual report of his activities and findings. The officer has the powers vested in him by the Data Protection Act. The General Administrative Law Act shall be similarly applied.

#### **8.2 Data exchange with countries outside the European Union**

8.2.1 Within the framework of their service, financial institutions exchange personal data with subsidiaries and other financial institutions established outside the Netherlands. This relates in particular to transactions relating to the settlement of orders from customers or potential customers. These orders may reach a financial institution in the form of regular orders, but also in the form of electronic orders or requests for information through the Internet. Where necessary, the processing of personal data relating to such orders falls within the scope of the processing principles set out in article 8.2.3.

- 8.2.2 Subject to the principles governing the processing of personal data, the transfer of personal data to countries outside the European Union or the European economic space is allowed if the country in question ensures an adequate level of protection in respect of the personal data transferred.
- 8.2.3 If a country outside the European Union does not warrant an adequate level of protection in respect of the personal data transferred, transfer will be possible if:
- a. the data subject has given his explicit consent for this, or
  - b. transfer is necessary for the performance of the contract between the data subject and the controller, or for taking steps at the request of the data subject prior to entering into a contract, and that are necessary of the conclusion of a contract, or
  - c. transfer is necessary for the conclusion or performance of a contract to be concluded between the controller and a third party in the data subject's interest, or
  - d. transfer is necessary for an important general interest, or the establishment, implementation or defence at law of any right; or
  - e. transfer is necessary for the protection of vital interests of the data subject, or
  - f. the Minister of Justice has granted permission for the transmissions or categories of transmissions.

### **8.3 Protection of personal data**

- 8.3.1 Having regard to the state of the art and the cost of their implementation and the risks involved in the processing of personal data and the nature of the personal data to be protected, the controller shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, or against all other unlawful forms of processing of personal data.
- 8.3.2 Where the processing of personal data is carried out by an external processor, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing of personal data to be carried out. A written processor contract is concluded with such processor.

### **8.4 Camera surveillance**

- 8.4.1 Financial institutions may use cameras:
- a. for the security and protection of the financial institution, its customers and its employees, and
  - a. for the prevention, investigation and prosecution of offences, and
  - b. for the recording of images to support legal procedures.
- 8.4.2 Such use is only allowed if:
- a. camera surveillance is selectively exercised, i.e. no more locations and individuals may be recorded than is necessary for the above-mentioned purposes. Insurers are also subject to the Code of Conduct for Personal Investigations (*Gedragcode Persoonlijk Onderzoek*);

- b. the personal data obtained through camera surveillance shall not be stored any longer than is necessary for the purposes set out in article 8.4.1. In principle, such period shall not exceed one month, except if the personal data relate to an incident. In such a case, the personal data are kept for the length of time needed to deal with such incident;
- c. the images obtained through camera surveillance are stored and protected in such a way as to ensure that they are not accessible to unauthorised individuals. Technical and organisational provisions shall be taken to prevent the personal data from being manipulated and in order to be able to trace and reconstruct the personal data, if necessary.

8.4.3 If there is camera surveillance, this shall be communicated in a clear fashion.

## **8.5 Recording of telephone conversations**

8.5.1 Save for the use of training, coaching and appraisal purposes, telephone conversations shall only be recorded:

- a. for verification of and research on, or as proof of orders, transactions and other (pre-contractual) agreements with the customer;
- b. if such is necessary in the fight against fraudulent conduct or other offences directed against the financial institution, the group to which the financial institution belongs or customers and employees;
- c. if such is in response to a statutory regulation.

8.5.2 The data subject whose telephone conversations are recorded shall, in principle, be informed of this, unless such is impossible in view of the purposes referred to under b and c of 8.5.1.

8.5.3 The recorded telephone conversations and other personal data relating to the recorded telephone conversations shall be stored and protected in such a way as to ensure that they are not accessible to unauthorised individuals. Technical and organisational provisions shall be taken to prevent the data from being manipulated and in order to be able to trace and reconstruct the personal data, if necessary.

8.5.4 The recorded telephone conversations shall not be stored any longer than is necessary for the purposes set out in article 8.5.1.

8.5.5 In the event of differences or disputes regarding the interpretation of the content of the recorded telephone conversations, the customer shall have the right to listen to the recorded telephone conversation and/or obtain a transcript of the recorded telephone conversation.

## **9. Auditing and supervision**

9.1 Financial institutions set great store by due compliance with the regulations of the Data Protection Act. To this end, they have instructed their audit department or another similar department to oversee compliance with the Data Protection Act and this code of conduct and to report on this. The audit department of the financial institution shall lay down its findings in a report at least once a year.

- 9.2 To advance the audit as referred to in the first paragraph, financial institutions shall draw up internal instructions setting out the way in which the personal data are to be processed. These instructions shall be given in respect of all those subjects that require further explanation for the staff.
- 9.3 As part of the policy pursued by a financial institution in respect of the protection and auditing of the use of personal data, a financial institution may, in addition, appoint an officer of its own as referred to in 8.1.

## **10. Disputes**

- 10.1 Data subjects in whose opinion a bank is violating the code of conduct or is otherwise acting in breach of the Data Protection Act, may address themselves to the Arbitration Committee for Banking Affairs (*Geschillencommissie Bankzaken*), Bordewijklaan 46, 2nd floor, 2591 XR The Hague, Postbus 90600, 2509 LP The Hague, telephone 070-31 05 310. The data subjects may also apply to the CBP or the court.
- 10.2 Data subjects in whose opinion an insurer, who is a member of the Association of Insurers (*Verbond van Verzekeraars*) is violating the code of conduct or is otherwise acting in breach of the Data Protection Act, may address themselves to the Insurance Complaints Authority (*Stichting Klachteninstituut Verzekeringen*), Postbus 934450, 2509 AL The Hague. Data subjects may also apply to the CBP or the court.
- 10.3 Invoking any of the aforementioned arbitration regulations shall not stay ?? the terms mentioned in sections 46 and 47 of the Data Protection Act. A data subject exercising his rights under sections 46 and 47 of the WBP shall retain his right to lodge a complaint or go to arbitration simultaneous with the institution of a procedure as set out in sections 46 and 47 of the WBP, or during or subsequent to that, or to apply for the mediation of any of the above-mentioned organisations, which cannot declare a complaint inadmissible on that ground.

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

### **1 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. To assess adequately the relationship with the customer, the financial institution needs the customer's personal data. The processing of personal data involves different interests. It is in the customer's interest that his privacy is optimally protected, while the financial institution aims to look after its legitimate interests as well as it is able to.

In order to duly reconcile potentially conflicting interests, a set of rules has been set up. Up to 1 September 2001, this system was embodied in the Data Protection Act (*Wet persoonsregistraties, WPR*). From that date on, this act has been replaced with a new Data Protection Act (*Wet bescherming persoonsgegevens, WBP*). Under this act, the financial institution processing these personal data ('the controller') has to fulfil a number of obligations. The individuals whose data are processed (the 'data subjects') have been granted a number of rights (right to inspection and rectification, right to object). There is independent supervision of compliance with the act, exercised by the Board for the Protection of Personal Data (*College Bescherming Persoonsgegevens, CBP*) or the officer in charge of data protection, if such officer has been appointed by a financial institution.

The act leaves institutions or groups of institutions the possibility to take measures themselves that are more closely tailored to their own specific business management. The previous Data Protection Act (*WPR*), too, offered this possibility. In the past, the Netherlands Bankers' Association (*Nederlandse Vereniging van Banken, NVB*) and the Association of Insurers (*Verbond van Verzekeraars, VvV*) each made separate use of this opportunity to draw up codes of conduct, which were approved by the former Registration Board.

Along with the change in legislation it became necessary to harmonise the codes of conduct with the new act. In view of developments taking place in recent years, with banks and insurers becoming more and more interwoven, NVB and VvV decided to draft a single code of conduct: the Code of Conduct for the Processing of Personal Data by Financial Institutions. This code of conduct is a declaration of agreement issued by the Board for the Protection of Personal Data (*CBP*).

### **2. Notes to a number of articles**

#### **2.1 Introduction**

In a code of conduct based on the WBP, it is unavoidable that many terms and regulations are adopted verbatim. This is necessary to ensure consistency and because certain regulations are so general that they cannot readily be tailored to a financial institution's particular situation. In these notes, the terms are used as defined in the code of conduct. For instance, a financial institution is understood to mean a bank and/or insurer. For terms and provisions adopted from the WBP, please refer to the explanatory memorandum and the manual that has been written at the request of the Ministry of Justice. In these notes to the code of conduct we limit ourselves to situations and examples that are specifically relevant to financial institutions.

## 2.2 Definitions

Besides the data subject, i.e. the individual whose personal data are processed, the controller is the chief actor in the WBP. The data subject, in relation to the financial institution, will be detailed in the next paragraph. This paragraph covers the controller, the processor and the functional unit.

The main characteristic of the controller is, on the one hand, the formal and legal power to establish the purpose and means of the data processing. But there is also a functional side to the word, which is supplementary to the former characteristic. This is particularly relevant where several actors are involved in the processing of personal data. In principle, the financial institution with which the data subject, for instance, concludes a contract, will act as controller. However, where the financial institution is part of a group, another legal person within that group may have been designated as controller. It is possible to make provision in the articles of association or through a contract, for conferring the power to determine the purpose and means of the data processing within the group on one particular legal person within the company. The parent company will thus be able to act as controller in respect of all data processing operations taking place within the group, because legal control under the prevailing set-up is vested in that legal person. The financial institutions will each make it sufficiently known which company will act as controller in charge of the processing of personal data.

The processor processes data for the instructing party, i.e. the controller. The processor has no control over the processing but only acts on the instructions of the controller. The following is an example of the relationship between the processor and the controller. Financial institutions have, to a large extent, outsourced the settlement of payments to Interpay. The starting-point in this regard is that Interpay's role consists of the implementation of the orders of the financial institutions. Interpay does not have the independent authority to use the data entrusted to it within the framework of payment transactions for any other purposes. In this situation, Interpay is processor. The situation is different where it concerns independent services that may be offered by Interpay. One example of such a service is the supply and maintenance of POS terminals installed at companies. Where the entrepreneurs' personal data are processed, Interpay acts as controller.

In respect of processing, the WBP prescribes that processing is to be regulated by a controller in a contract or pursuant to another juristic act, creating an obligation between the processor and the controller. The sections of the contract or the juristic act relating to the protection of personal data and security are laid down in writing or in another, equivalent form.

Data relating to health may only be processed insofar as such is vital to the conclusion and performance of an insurance and/or financing contract. The term 'functional unit' plays an important part in this regard. This functional unit consists of individuals who are by necessity involved in the purpose for which the medical data have been asked or provided and who, under the responsibility of a medical advisor, are entitled to receive certain health data. The medical advisor will only make those medical data available to the functional unit (within which the work is carried out) that are needed for handling the insurance application, the assessment of insurance claims, or the assessment of bodily injury.

Being part of one and the same functional unit, rather than belonging to one and the same organisation, is the essential criterion for the granting of access to relevant data relating to health. The medical advisor consults with the members of the functional unit on which

medical data are relevant to them and he is responsible for the provision of information. All individuals who are considered to be part of this functional unit shall be bound to a derived obligation to observe secrecy, whose scope is similar to that of the medical advisor.

### **2.3 Description of the sector, scope and data subjects**

The sector described is strictly limited to NVB and VvV members and institutions associated with Rabobank Nederland. This means, for instance, that while the code of conduct applies when a bank acts as an insurance intermediary, it does not when the insurance is written by an insurance intermediary not associated with NVB, VvV or Rabobank Nederland. Still, other, natural and legal persons not falling under the definition of financial institution, such as independent intermediaries and loss adjusters, are equally allowed to subscribe to the code of conduct.

The processing of personal data of financial institution staff, or of individuals listed in incident registers, does not fall under the scope of this code of conduct. In view of the specific nature of the latter processing and the special steps that have been taken to protect the personal data, an Incident Warning System Protocol for Financial Institutions (*Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*) has been drawn up. In addition, a prior investigation as referred to in section 31 of the WBP will be requested. This type of processing of personal data will be discussed in further detail in paragraph 2.5.

Data subjects include any individual to whom a personal data relates. In relation to a financial institution they will mainly include customers and individuals approaching a financial institution or who are approached by a financial institution. They may also include individuals whose personal data have to be processed as a result of their relationship with a customer, for instance in the capacity of payee or claimant. Furthermore, they may include commercially active individuals, such as intermediaries and mortgage advisors. One-man businesses without legal personality are also regarded as data subjects, their data being considered personal data in view of the fact that there is a real possibility that the data in question are linked to a natural person, in this case the director.

### **2.4 Principles governing the processing of personal data**

The processing of personal data is taken to mean any action performed with personal data. This includes the collection of data up to and including their destruction and all intermediate actions. The main principles of the WBP relate to the specification of the purpose of the processing, the legitimacy of the processing, compatible use and the obligation to provide information. We will discuss any of these principles in further detail, with an emphasis on compatible use, which wholly determines further processing, such as the provision of personal data.

#### *Objects of the processing of personal data*

Personal data may only be collected for certain, explicitly described and legitimate purposes. This implies that the purpose must be clearly formulated. The purpose for which the personal data are collected is the fundamental criterion against which many other regulations, such as compatible use, the storage periods and the condition that no more data are collected than necessary for a specific purpose, must be tested.

The financial institutions have concretised this object in several activities. This includes first of all customer assessment and acceptance and any activities that may follow from this, such as the conclusion and performance of contracts and the settlement of payment transactions. Secondly, the data are used for pursuing targeted market activities designed to maintain or expand the relationship with the customer or to solicit new customers. A third activity concerns risk management in general terms: the fight against and the prevention and investigation of conduct directed against a financial institution or the sector in general. In addition, financial institutions are increasingly obliged to process personal data in order to meet legal regulations. All of these activities will be discussed in further detail.

### *Legitimate ground*

The processing of personal data must be based on any of the grounds specified in the WBP. The following four grounds are relevant to financial institutions:

- the data subject's unambiguous consent;
- the data are necessary for the performance of a contract to which the data subject is party or in order to take steps prior to entering into a contract;
- the data are necessary for compliance with a legal obligation to which the controller is subject;
- the data are necessary for the purposes of the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except where such interests are overridden by the interests or the fundamental rights and freedoms of the data subject. To make a due assessment of this, this particular ground involves that both interests at stake must be weighed in a general sense.

If any of these grounds is missing, the processing of personal data is not permitted. Where personal data are used for multiple activities, processing will often be based on several grounds. Where it concerns financial institutions, this ground will mainly be the conclusion and performance of a contract, the need to fulfil a legal obligation, or because processing is necessary to serve the legitimate interests of the financial institution. This latter ground applies, amongst other things, when personal data are processed within the framework of marketing activities or risk management.

### *Compatible use*

As referred to above, financial institutions have concretised the purpose of collection in several activities. As regards compatible use, this means that the question of whether personal data obtained within the framework of certain activities may also be processed within the framework of other activities and, if so, to what extent, depends on the question of whether the purpose of the processing in question is compatible with the activity or activities for which the personal data have originally been obtained.

Before processing personal data any further, a financial institution should therefore consider whether such would be incompatible with the activity or the activities for which the data have been obtained. In answering the question of whether the use of data may be qualified as compatible, various factors are playing a role. A number of these factors are listed (on a non-limitative basis) in section 9, paragraph 2 of the WBP and explained in further detail in the explanatory memorandum to the act. The question of whether the further processing of the personal data is compatible must be considered in light of several factors, such as the

relationship with the purpose or the products for which the personal data have been collected, the nature of the data, the consequences of the processing for the data subject and the extent to which adequate safeguards have been put into place in respect of the data subject. As regards the nature of data, section 16 of the WBP sets out which personal data are, by their very nature, sensitive. Furthermore, data may be sensitive as a result of the context within which they are used, for instance the personal data regarding an individual's creditworthiness or financial resources. The more sensitive the data, the less readily it may be assumed that its use is compatible if the object of the processing differs from the original purpose. The factors must be assessed and weighed in their specific context. None of the factors is, in itself, of crucial import. For instance, even if there is a certain relationship with the purpose for which a data was originally collected, its use in a specific context could increase its sensitive nature to such an extent that the consequences could be far-reaching for the data subject and compatible use would be out of the question. Where the data subject has given his explicit consent, the requirement of compatible use is definitely fulfilled.

Compatible use involves open criteria that must be assessed and weighed from case to case in order to determine whether the exchange of certain data is permitted. If it is not immediately clear whether further processing is permitted, it will be carefully examined, on the basis of actual circumstances, whether processing may go ahead. The individuals who will be dealing with the use of personal data for (in)compatible purposes are to be instructed as to which individuals must be consulted in case of doubt, before passing on any information.

This may be illustrated with some examples.

- The 'Pay Efficiently' (*Betaal op maat*) campaign is an example of the compatible use of data on payment orders for efficiency purposes. In order to encourage customers to make greater use of payment slips or direct debit orders and less use of regular (more expensive) payment order forms, customer were informed about a mix of payment methods tailored to their specific needs. This involves data obtained within the framework of a current account contract and subsequently used to improve the quality of the service. This does not compromise the customer's interests.
- Financial institutions are frequently approached with requests for information on the creditworthiness of their customers. These requests are often made by status enquiry agencies. However, such information may not be provided by the financial institution because it is incompatible with the purpose for which the data have been collected. Only if the customer has given his explicit consent will the financial institution be allowed to provide the information requested.
- If any irregularities occur during the performance of a contract, the employees of the financial institution may pass on data on the contract and the observed irregularities to the security department or an officer authorised for this purpose. He may further process these data within the framework of fraud control and enter the data (or have the data entered) in in-house and industry-wide warning systems. The processing of personal data by such a department or officer is subject to the Incident Warning System Protocol for Financial Institutions (*Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*). This protocol has been attached to this code of conduct as an annex.
- The bank may be able to derive information from order data that is relevant to determining a customer's interest in financial services offered by the bank. If the context does not increase the sensitivity of the data to such a level that, in combination with the other factors, their use must be considered as incompatible, the bank may use such information for the provision of these services. For instance, a customer who

obviously is a student (receives student loan money on his current account) may be approached by the bank for a student account. This does not alter the fact that notifications as referred to in article 5.4.4 of the code of conduct will be regarded as confidential and are not to be used for marketing activities.

- Within a company, the existence of a debt payable by the data subject may result in an exchange of information designed to establish whether another section of this company still owes compensation in connection with a non-life insurance policy. This way, the debt and the claim for compensation may be set off against each other or, if such is not possible, an attachment by garnishment may be levied on the compensation payable. The personal data on which the payment of compensation is based will generally not be available to other sections of the company.
- A textbook case of compatible use within a company is the bank which, following the extension of mortgage loans, draws a non-life insurer's attention to the possibility of dispatching a mailing in respect of residential premises insurance. The relationship between both products is obvious, the consequences for the data subject are not far-reaching and the context in which the data will be used does not increase the sensitivity of the data to be processed to a level that such action would constitute incompatible use. A health insurer may also pass on name and address details and birth dates of his customer base to a pension insurer belonging to the same group in order to enable it to draw the data subjects' attention (through a mailing) to the advantages of taking out supplementary pension insurance. In this case, too, the consequences for the data subject are not far-reaching and the context in which the data are used will not make them so sensitive as to render their use incompatible with the purpose for which they were obtained by the health insurer. Moreover, being part of a group, the health insurer has a legitimate interest in using the personal data of the insured in this way and to this extent in order to serve the interests of other operating companies within that group, while this course of action does not prejudice the privacy interests of the insured to any disproportionate degree.
- Things are different when the health insurer, on the basis of the claim behaviour of his customer base, makes a selection and passes the results of this selection on to the permanent health insurance company also belonging to the group. In that case, the context in which the data are used renders them so sensitive that, in combination with the other factors, this course of action may no longer be considered as compatible use. The code of conduct therefore forbids such use.

### *Obligation to provide information*

The ratio underlying the obligation to provide information is that the controller may be held accountable by the data subject. The standard is that the obligation to provide information applies unless the data subject 'is already cognizant'. Depending on the circumstances, the controller may assume such cognizance, for instance because the data subject has been handed or sent information, or because the data subject's behaviour shows that he is cognizant. When a relationship with a financial institution is started, the opening or application form will generally explicitly set out the purposes for which the data are collected. If the data are collected from a source other than the data subject himself, the obligation to provide information applies, unless the party providing the data has already notified the data subject.

Where the provision of information proves impossible or would involve a disproportionate effort, the obligation to provide information does not apply unless the origin of the 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 instance at the time when the data subject is contacted in writing.

The obligation to provide information also applies when the financial institution engages in on-line communication with a data subject and processes personal data. In that case the obligation can be fulfilled by placing a prominent Privacy Statement.

## **2.5 Processing of personal data**

The purpose for which a financial institution processes personal data involves the whole body of activities that a financial institution normally carries out in order to conclude the contracts, to draw and retain good customers, and to discourage (or terminate contracts with) bad customers. In a more general sense, it involves activities that are important for a financial institution as a whole to be able to maintain the relationship with the customer. These activities make up an interrelated whole. Therefore, only when they are carried out in an interconnected way can the business management be conducted in an effective and efficient manner. Still, 'interrelated' does not imply that all activities are by definition compatible. Except if the data subject has given his consent, data relating to health may only be used within the framework of the contract for which the personal data have been obtained. The same also applies to data relating to criminal offences. Nor is it permitted to use special categories of data as a selection criterion for marketing activities, unless the data subject has given his explicit consent. This could be the case, for instance, with ethno marketing, in which ethnic groups are approached with products specific to them. In respect of other personal data (not falling within the category of special data), too, it must be considered whether they can be processed for another purpose. In all cases it must be assessed for each situation what activity is being pursued and which personal data may be used for this. If the context in which the personal data are used would render them so sensitive that, in combination with the other factors, use of them should be regarded as incompatible use, no further processing should take place. Therefore, use of the data within the framework of the various activities should always be tested against the principles governing data processing. Below, a number of these essential activities are examined in some further detail.

### *Conclusion and performance of a contract*

Within the framework of efficient and effective business management, financial institutions are increasingly operating integrated customer information systems. There are different types of customer information systems. Of course, these systems are only accessible to the financial institution's staff authorised to handle these data in connection with their work. These tasks (and by extension the access to data) differ from employee to employee. In its limited form – for instance the system the call centre staff must be able to consult – the system needs to contain only a limited amount of personal data: Name and address details and type of contract. As more data are entered in the system and the system is used for multiple activities, the requirements made to access control will become more and more stringent and tighter authorisations will be put into effect. At that point it will be laid down exactly who is authorised to take cognizance of these data. Access to integrated customer systems is not limited to individual legal persons but, subject to the aforementioned provisions, may apply to all legal persons within the group.

Within the framework of payments, a distinction may be drawn between data being provided for the execution of the payment order, the so-called order data, and the data stated by a customer in the space reserved for messages. The order data may be used for marketing purposes where the context in which the data are used does not render them so sensitive that, in combination with the other factors, such use would be incompatible. Statements made in the space reserved for messages (for instance: concerns membership fee for ..., membership of ...) may not be used for marketing purposes.

### *Statistical analyses*

Statistical analyses, including data mining and credit scoring, in which personal data (not being special categories of data) are processed, are not incompatible with the purpose for which the personal data have been collected. The use of personal data for the preparation of group profiles is a form of statistical use that is generally considered permissible. In this regard it does not make any difference that the results can be traced to an individual natural person, provided that measures have been taken to ensure that the data are used for statistical analyses only. These measures may involve laying down in writing that the data will not be used for taking measures or decisions relating to a specific individual. Another possibility is that the data are processed in such a way as to ensure that they can no longer be traced to an individual natural person. In that case the information may be used for all kinds of (other) purposes, such as marketing.

As long as the personal data are not processed with a view to the establishment or maintenance of a direct relationship with the data subjects, no objections can be made against their use. Such is the case, for instance, when a company collects personal data in order to prepare statistics showing the relationship between place of residence and buying behaviour so as to map out potential locations for establishing points of sale. Of course, such processing does remain subject to the other regulations of the WBP.

Where the outcome of a statistical analysis is attributed to an individual data subject, as in the case of individual scores, the regime of statistical research does not apply. If the outcome is attributed to an individual in order to approach him for marketing purposes, it should be considered as processing for marketing purposes and it will have to be checked whether such use is compatible with the purpose for which the data have been acquired. In that case, the data subject may invoke his absolute right to object.

### *Marketing activities*

The use of personal data for marketing activities is governed by the general principle that such data must be fairly and duly processed. Fair and due processing is emphasised by stating that use is preferably made of personal data originating from the data subject himself. If the data do not originate from the data subject himself, the aforementioned provisions relating to the obligation to provide information apply. This means that the customer, in the event of the external purchase of personal data with the aim of approaching customers more efficiently, for instance through enrichment, statistical analysis, or mailing, will be notified of the marketing objective and that the source of the data will be recorded. Furthermore, a processor contract will be concluded with companies specialising in marketing, such as mailing agencies, and there will be a constant check on whether the customer has not invoked his right to demand exclusion from this type of processing.

Customers buying products from a company belonging to a group may be approached by that particular company as well as by the other companies belonging to that group within the framework of product marketing. Of course, in both cases the preconditions set out in the previous paragraph continue to apply. If the activity does not follow from the purpose of the activity for which the data have originally been collected, it should be considered whether the proposed processing is incompatible with it. In weighing this, the extent to which the customer has been informed about the composition of the group plays a role. Such information may be given, for instance, by means of an advertising spot or statement detailing the composition of the group in all communications aimed at the customer. The customer may invoke his right of objection at any time.

### *Fraud and crime*

Within financial institutions the department in charge of fraud and crime control constitutes a separate unit. The data on events collected by this department are recorded in so-called incident registers. The content of these registers is solely meant for use by authorised security officers within the framework of the prevention, investigation, or prosecution of fraud and crime. Staff of the financial institution's *customer business* have *no* access to these registers. The set-up and use of the incident registers fall outside the scope of this code of conduct and are regulated in a separate 'Incident Warning System Protocol for Financial Institutions' (*Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*).

Still, it is unavoidable that employees of the *customer business* of the financial institution play a role in fraud and crime control. The code of conduct always applies if *customer business* staff process data themselves within the framework of the prevention or detection of fraud and crime. Within this framework, *customer business* staff of the financial institution can report relevant incidents to the security officer or, in case of doubt, ask for advice from a security officer on how to act in respect of certain customers. The code of conduct equally applies in such cases. The security officer will record a disclosure in accordance with the criteria of the 'Incident Warning System Protocol for Financial Institutions'. In the event of a request for information, he will check whether the data concerning the (prospective) customer are available and, if necessary, advise in accordance with the provisions laid down in the protocol whether or not a customer should be refused. If the customer wishes further information, he will be referred to the security officer.

So actions of *customer business* staff fall under this code of conduct. Actions of security officers fall under the 'Incident Warning System Protocol for Financial Institutions'.

### *External Verification Systems*

In certain cases, personal data relating to credit applications, claims and incidents are also entered in registers that are kept by a legal person which is independent from the financial institution. Examples include the Central Credit Registration Office (*Stichting BKR*) and CIS Board (*Stichting CIS*), which act as controllers for, respectively, the Central Credit Information System and the Central Information System (CIS) and the Confidential Statements System (*Systeem Vertrouwelijke Mededelingen, SVM*). The provision of personal data to and their retrieval from these systems are subject to this code of conduct. The processing of personal data in the systems themselves falls outside the scope of the code of conduct. Both controllers have separately reported their processing procedures to the Data Protection Board (*CBP*).

### *Personal investigation*

A special type of processing of personal data, subject to the principles of proportionality and subsidiarity, relates to personal investigations. This may be necessary to ensure that no compensation is paid for fraudulent loss claims. The legitimacy of a claim will then, for instance, be verified through a door-to-door inquiry or video recording. A Code of Conduct for Personal Investigations (*Gedragscode Persoonlijk Onderzoek*) has been prepared for these types of investigation.

### *Personal data relating to an individual's state of health*

The processing of personal data relating to an individual's state of health is subject to a number of supplementary regulations. These relate to all areas of data-processing: collection, filing and disclosure. The processing of data relating to an individual's health is reserved for individuals belonging to the functional unit, under the responsibility of the medical advisor. This medical advisor is the only individual who is authorised to assess the data. If supplementary investigations are carried out, or if data are collected from parties other than the data subject, the explicit consent of the data subject will be asked. Special rules of conduct have been drawn up for the processing of very specific data, such as data relating to heredity and HIV.

### *Tax and social insurance number*

Financial institutions enter tax and social insurance numbers in their records in connection with the mandatory provision of information to the tax authorities. The tax and social insurance number is used as an ordering instrument in the administration, insofar as such is necessary for duly fulfilling the above-mentioned obligation to provide information. An agreement about this has been concluded with the Minister of Finance. The tax and social insurance number may also be used for the implementation of pension schemes.

### *Voice logging*

Within financial institutions telephone conversations are recorded in several locations for a variety of reasons. This is often done because customers increasingly give payment instructions by telephone.

Cases in point include orders that are provided through a call centre or by telephone to an advisor. The reason for recording these conversations is that the content of the order can be established where such is necessary in the event of a dispute with a customer, for instance over an order for buying or selling securities. Another reason for recording a telephone conversation is, for instance, establishment of the exact time on which the loss or theft of a bank card is reported to the bank, or where it concerns threats directed against the financial institution or its employees. Financial institutions will inform their customers as much as possible about the recording of telephone conversations, for instance through their product conditions. The financial institution will also instruct its personnel on the matter. On the customer's request, further information will be provided at any time.

## **2.6 Rights of data subjects**

The WBP, as the previous Data Protection Act (*WPR*) confers rights on the data subjects: the right to inspect his own personal data and the right to rectify, supplement, erase or block such data. Elements that are new compared to the WPR are 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.

#### *Right to take cognizance of the data*

The right to take cognizance of one's own data is a generally recognised right, which only ceases to have effect in exceptional cases. Besides being informed on his own data, the data subject must also be informed on the purpose of the processing, the categories of data to which the processing relates, the recipients or categories of recipients and the available information on the source of the data.

The exceptions relate to three situations. The first one is that inspection may be refused where it involves such matters as national security and the prevention, investigation and prosecution of criminal offences. A second situation may occur where not only the data of the data subject are processed but also those of another individual who might object to the granting of access to his or her data as well. In that case, such third person must be enabled to give his or her viewpoint. A third situation may occur where data are processed for scientific or statistical purposes. Then, too, a request for inspection may be turned down under certain conditions, namely if the investigation is carried out by an agency or institution for scientific research purposes.

As part of the right of inspection, the data subject has the right to be informed, at his request, of 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 protecting the software. However, this should not result in denial of access to all information.

Two additional provisions apply to the right of inspection. Firstly, a fee may be charged to defray the costs connected with a request for perusal of (and objection to) the data. This amount has been fixed at a maximum of € 4.50 per message. Secondly, the controller must see to it that the applicant is duly identified to ensure that the correct person is provided access to the personal data. Therefore, in the event of a written request for inspection, adapted measures must be taken such as the obligation to enclose a copy of a passport or driving licence so as to be able to compare the signatures, possibly with signatures that are already on record.

#### *Right to rectify, supplement, erase, or block the data*

Where appropriate, the data subject may rectify, supplement, erase, or block the data if they are substantially incorrect, incomplete, or irrelevant to the purposes of the processing, or are otherwise being processed in contravention of legal regulation. The ability to invoke this right is subject to the condition that the data subject has taken cognizance of his personal data.

Where a controller has met a request to rectify, supplement, erase or block data, he is obliged to notify any third party to whom (which) he has provided data of the changes, unless such proves impossible or would involve a disproportionate effort.

### *Right to object*

The WBP specifies the system of objection in further detail, distinguishing between relative and absolute requests for objection. Relative requests may be lodged if the legal ground for the processing is constituted by section 8f: protection of the legitimate interests pursued by the controller. In that case the data subject may request that the processing of his personal data is ceased on the ground of his special personal circumstances. In that concrete case, the controller must reconsider the processing and weigh his interest against the data subject's (special) interest.

An objection raised against the processing of personal data for the purpose of using such data for commercial or charitable solicitation is absolute and must be allowed unconditionally. In case of objection, the controller must take steps to cease this form of processing of personal data of the data subject with immediate effect. When approaching the data subject, the controller must always point out the possibility of raising an objection if it concerns messages for commercial or charitable purposes.

### *Decision based on automated processing*

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 affect 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 personal aspects.

The regulation is not absolute and states that there are situations in which such a decision is permissible, for instance where a decision is taken within the framework of the conclusion or performance of a contract and adequate measures have been taken, or where the decision is taken on legal grounds. Examples of the latter situation are the conclusion of an insurance or financing contract and the first paragraph of section 28 of the Consumer Credit Act (*Wet op het consumentenkrediet*). 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.

## **2.7 Complaints procedure**

Both the Netherlands Bankers' Association (*NVB*) and the Association of Insurers (*VvV*) have an independent disputes settlement scheme in place. The rules observed by the banks have been embodied in the Arbitration Committee for the Banking Industry (*Geschillencommissie Bankzaken*) which, besides disputes of a general nature, also handles disputes relating to the use of personal data. The opinion given by the Committee is binding. Prior to the submission of a complaint or a dispute, the procedure and effects of a decision must be made clear to a data subject. The data subject is then free to decide not to go through with this procedure and to turn directly to the court or the Board for the Protection of Personal Data (*CBP*).

The disputes settlement scheme of the Association of Insurers has been embodied in the Arbitration Institute for the Insurance Industry (*Stichting Klachteninstituut Verzekeringen*). The Board of the institute has an independent Chairman, while the members are nominated by both the Consumers' Association and the organisations of insurers and intermediaries. The Board does not handle actual cases, but appoints one or more independent ombudsmen and

the members of the Insurance Companies Complaints Authority (*Raad van Toezicht Verzekeringen*). The task of the ombudsman and the Complaints Authority has been laid down in a set of regulations. Here, too, the data subject may opt to turn directly to the court or the Board for the Protection of Personal Data.

## **Annex I: Information**

- 1 An overview is given below of documents containing further information concerning the processing of personal data by financial institutions and of the documents referred to in the Code of Conduct.
  - a. *Gedragscode DMIN* was published in the Netherland Government Gazette, No. 194, 1992.
  - b. *Geschillenreglement Bankzaken* may be ordered from the Arbitration Committee for the Banking Industry (*Geschillencommissie Bankzaken*), Bordewijklaan 46, 2<sup>nd</sup> floor, 2591 XR The Hague, Postbus 90600, 2509 LP, The Hague, telephone 070 31 05 310.
  - c. *Reglement Stichting Klachteninstituut Verzekeringen* may be ordered from *Stichting Klachteninstituut Verzekeringen*, Postbus 93450, 2509 AL The Hague.
  - d. *Regelingen BKR* (including rules and regulations of the arbitration committee) may be ordered from BKR (Bureau Krediet Registratie), Postbus 6080, 4000 HB Tiel, telephone 0344 616041.
  - e. *Regeling Organisatie and Beheersing (ROB)* of De Nederlandsche Bank NV concerning the reliability and continuity of automated data processing in the banking industry, dated 20 September 1988, since supplemented with a letter from De Nederlandsche Bank NV regarding the outsourcing of automated data processing, dated 27 May 1994.
  - f. *Gedragsregels voor Privacy and Kaartintegriteit Open Infrastructuur voor Chipkaarttoepassingen van het Nationaal Chipcard Platform* of 18 September 1996.
2. For any questions concerning the code of conduct you may also contact the Netherlands Bankers' Association, Postbus 3543, 1001 AH Amsterdam, telephone 020-55 02 888, fax no. 020-62 39 748 and the Association of Insurers, Postbus 93450, 2509 AL The Hague, telephone 070 333 8500, fax no. 070 333 8510.
3. The following documents have been attached to this code of conduct for further information:
  - A. *Voorschrift Informatie Fiscus/Banken*
  - B. *Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*
  - C. *Gedragscode Persoonlijk Onderzoek*
  - D. *Moratorium erfelijkheidsonderzoek Verbond van Verzekeraars*
  - E. *HIV-gedragscode*