Code of Conduct
for the Protection of the Individual's Right to Privacy
in the Handling of Personal Data
within the Deutsche Telekom Group

Preamble and Recitals

(1) Due to increasing networking of information and communications systems, the protection of personal data of customers, sales partners, employees and shareholders is a significant concern of all companies in the Deutsche Telekom Group worldwide.

(2) The most important target of this Code of Conduct, therefore, is to create a uniform and high level of data protection in the Deutsche Telekom Group worldwide. In particular, in the case of transnational data flows it must be guaranteed that personal data is processed by the recipient according to the principles of data protection law that apply for the sender of such data.

(3) Deutsche Telekom Group companies are aware that the success of Deutsche Telekom as a whole is dependent not only on global networking of information flows, but also above all on trustworthy and safe handling of personal data.

(4) In many areas, the Deutsche Telekom Group is perceived by its customers as a single entity. Therefore it is the common concern of Deutsche Telekom Group companies to make an important contribution to the joint success of the company and to support the claim of the Deutsche Telekom Group of being a provider of high quality products and services by implementing this Code of Conduct.

Part One
Scope and Application

§ 1 Legal Nature of the Code of Conduct

This Code of Conduct is a Directive, which is binding for the entire Deutsche Telekom Group and comes into effect upon adoption and publication by the respective company management. It applies to the handling of all the personal data of natural persons, in particular the data of customers, shareholders, employees and other third parties, contracting parties or business partners.

§ 2 Legal Provisions to be Applied

(1) The principles set out below are intended to guarantee a uniformly high level of data protection throughout the entire Deutsche Telekom Group. However, they do not replace the required - and where necessary, statutory - conditions that must exist to legitimize the handling of personal data. Any obligations and regulations applying to individual companies on the processing and use of personal data which go beyond the following principles, or which contain additional limits on processing and use of personal data, shall remain unaffected by this Code of Conduct. Irrespective of the foregoing, the companies agree that laws applying for individual companies shall not prevent these companies from fulfilling their obligations under this Code of Conduct.

(2) Data collected in Europe must be processed according to the legal provisions of the country in which the data was collected, even in the event of transmission abroad.

(3) The collection of personal data and its transmission to public bodies shall - unless within the framework of a normal customer contractual relationship – be done in accordance with the obligatory legal provisions of the country.

(4) This Code of Conduct shall be governed by the law of the Federal Republic of Germany.

§ 3 Termination

The expiry or termination of the Code of Conduct – irrespective of the time, circumstances and reasons – shall not release the companies from the obligations and/or provisions of this Code of Conduct regarding the processing of data already transmitted.

Part Two
Principles

Article 1
Transparency of Data Processing

§ 4 Duty to Inform

The data subjects must be given easy access to information about the appropriate handling of their personal data, for example by publishing privacy policy and this Code of Conduct on the Internet.

§ 5 Content and Form of Information

(1) The data subjects shall be adequately informed about the following:

a) The identity of the data controller(s) and their contact details.

b) The intended scope and purpose of the collection, processing and/or use of personal data. This information should include which data are being recorded and/or processed/used, why and for what purpose and for how long.

c) If personal data are transmitted to third parties, the recipient, extent and purpose(s) of such transmission.

d) The manner of data processing and/or use, especially if it is to be processed or used in another country.

e) Their legal rights (see Article 7).

(2) Irrespective of the chosen medium, data subjects should be given this information in a clear and easily understandable manner.

§ 6 Availability of Information

The information shall be available to data subjects when the data are first collected and , subsequently, whenever it is requested.

§ 7 Consent

(1) Unless the collection, processing or use of the data is required for purposes of initiating or fulfilling a contract or unless there is some other statutory authorization, the consent of the data subject shall be obtained at the latest when data starts to be collected, processed or used.

(2) In addition to the obligations to inform as set out above, the following shall be observed with regard to consent:

a) Content
Consent must be given expressly, it must be voluntary and it must be on an informed basis that points out to the data subject, in particular, the scope of what he/she is consenting to and also the consequences of non-consent. The wording of declarations of consent shall be sufficiently precise and shall inform data subjects of their right to withdraw their consent at any time.

b) Form
Consent shall be obtained in a form appropriate to the circumstances (normally in writing or electronically). In exceptional cases it can be obtained verbally, if the fact of the consent and the special circumstances that make verbal consent seem adequate are sufficiently documented.

Article 2
Use for Specific Purpose

§ 8 Principle

Personal data shall not be used for purposes other than those for which the data was originally collected.

§ 9 Prohibition of Tying-in

The use of services, or the receipt of products and/or services, shall not be made conditional on data subjects consenting to the use of their data for purposes other than the initiation or fulfillment of a contract. This shall only apply if it is not possible or not possible within reason for the data subject to use comparable services or comparable products.

Article 3
Special Data Processing Cases

§ 10 Direct Marketing

(1) Data subjects shall be informed that they may, at any time, object to their personal data being used for direct marketing purposes. Furthermore, they shall be made aware of the nature, content and period within which their data may be used for direct marketing purposes.

(2) Data subjects shall be informed about their right to object whenever they receive direct marketing communications. Furthermore, data subjects shall receive appropriate tools for exercising their right not to receive such communications. They shall receive, in particular, information about the body to whom the objection is to be made.

(3) Special legal provisions pursuant to sentence 2 of § 2 (1) of this Code of Conduct, which make the use of personal data dependent on the consent of the data subject, shall take precedence over other provisions.

§ 11 Automated Individual Decisions

(1) Decisions which evaluate individual aspects of a person and which may entail legal consequences for them, or which may have a considerable adverse effect on them, shall not be based exclusively on automated processing. This includes in particular decisions for which data about the creditworthiness, professional suitability or state of health of the data subject is significant.

(2) If, in individual cases, there is an objective need to make automated decisions, the data subject shall be informed without delay of the result of the automated decision, and shall be given an opportunity to comment within an appropriate period of time. The data subject's comments shall be suitably considered before a final decision is taken.

§ 12 Special Categories of Personal Data

(1) The handling of special categories of personal data shall be subject to express, legal authorization or to the data subject's prior consent. It shall also be permissible if it is necessary to process the data in order to fulfill the rights and obligations of the responsible body in the area of labor law, provided that this is permissible due to national law that provides for adequate guarantees.

(2) Prior to the commencement of such collection, processing or use, the data protection department of the company in question shall be properly consulted, in writing, of all cases where this is necessary. Due consideration should be given to the nature, extent, purpose, necessity and legal basis of using the data .

Article 4
Data Quality, Data Economy and Data Avoidance

§ 13 Data Quality

(1) Personal data shall at all times be correct and, where necessary, kept up do date (data quality).

(2) In light of the purpose(s) for which the data are being collected, processed or used, appropriate measures shall be taken to ensure that any incorrect or incomplete information is erased or, if necessary, corrected.

§ 14 Data Economy, Data Avoidance, Anonymization and Pseudonymization

(1) Personal data shall be appropriate, relevant and not excessive with regard to the use of the data for a specific purpose (data economy). Data shall only be processed within a certain application when it is necessary (data avoidance)

(2) Where possible and economically reasonable, procedures shall be used to erase the identification features of data subjects (anonymization) or to replace the identification features with other characteristics (pseudonymization). Anonymization and pseudonymization shall be carried out in such a manner that the original identities of the data subjects cannot be revealed, or can only be revealed with disproportionately great effort,

§ 15 Profiling, Statistical Analyses

(1) Organizational and technical measures consistent with the appropriate state-of-the-art concepts or technology shall be used to ensure that profiling (e.g. movement profiles, user profiles, consumption profiles) is not allowed unless by express legal permission or the data subject's prior consent.

(2) Purely statistical analyses or studies on the basis of anonymized or pseudonymized data remains unaffected in this regard

§ 16 Data Archiving

The principles of data processing, particularly the principles of data economy and data avoidance, shall be taken into account when developing data archiving rules. Personal data must not be archived without the express consent of the data subject, unless where necessary for operational reasons or required by law.

Article 5
Restriction on Further Transmission

§ 17 Transmission of Data to Third Parties

(1) The transmission of personal data to a third party shall require a legal basis. This may arise because it is necessary to fulfill a contractual requirement towards the data subject or because the data subject has provided their consent.

(2) Paragraph 1 does not apply if national restrictions, in particular for reasons of security of the state, national defense, public safety or the prevention, investigation, detection and prosecution of criminal acts exist which require the transmission of personal data for these purposes.

§ 18 Responsibility

(1) When transmitting data to third parties that are not public bodies, the company that originally collected the data shall ensure that it is being processed or used lawfully. Accordingly, prior to the transmission of the data, appropriate data protection and data security measures shall be discussed and agreed with the recipient. Where agreements are concluded with bodies in countries without adequate data protection levels, sufficient guarantees must be ensured with respect to the protection of the right to privacy of the individual and the exercising of rights connected with this.

(2) In accordance with generally accepted standards, appropriate technical and organizational measures shall be taken to ensure the integrity and security of data during its transmission to a third party.

§ 19 Subcontracted Data Processing

(1) When a company engages the services of a subcontractor, then, in addition to a service agreement comprising the work to be performed, the contract shall also refer to the obligations of the subcontractor as the party engaged for processing the data. These obligations will set out the instructions of the company (the data controlling unit) concerning the type and manner of the processing of the personal data, the purpose of processing and the technical and organizational

measures required for data protection. Sentence 3 of § 18 (1) of this Code of Conduct applies accordingly.

(2) The subcontractor shall not use the personal data for its own or third-party processing purposes without the prior consent of the data controlling unit. In the case of the latter, the above-stated rules shall also be agreed with such subcontractor(s).

(3) Subcontractors shall be selected according to their ability to fulfill the above-stated requirements.

Article 6
Data Protection, Organization and Data Security

§ 20 Data Protection Officers

(1) Each company shall appoint a data protection officer, whose task is to ensure that the individual departments are advised on the statutory and/or Group-internal requirements and on data protection and privacy policy.

(2) The data protection officer must be involved in the design of new products and services from the early stages to ensure that they are in harmony with the principles that are set out in this Code.

§ 21 Checks on the Level of Data Protection

Checks on the level of data protection (e.g. by data protection audits) should be carried out at regular intervals to review the effectiveness and success of the technical and organizational data protection measures implemented. Such audits may be carried out internally by the data protection officer or other organizational units which have been awarded an audit assignment or, alternatively, by an independent external third party approved by the data controlling unit. The basis for establishing the level of data protection shall be the legal and corporate policy requirements that apply for the respective organizational unit as well as the requirements of this Code of Conduct.

§ 22 Technical, Organizational and Employee-Related Measures

Appropriate confidentiality undertakings shall be agreed in writing with employees when commencing their work within the company. In addition, appropriate technical and organizational measures for handling personal data shall be established for the company processes and Information Technology systems.

Such measures shall include

a) preventing unauthorized persons from gaining access to data processing systems on which personal data are processed or used (**physical access control**);

b) ensuring that data processing systems cannot be used by unauthorized persons (**denial-of-use control**);

c) ensuring that those persons authorized to use a data processing system are able to access exclusively those data to which they have authorized access and that personal data cannot, during processing or use or after recording, be read, copied, altered or removed by unauthorized persons (**data access control**);

d) ensuring that, in the course of electronic transmission or during their transport or recording on data carrier, personal data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to examine and establish where personal data are to be transmitted by data transmission equipment (**data transmission control**);

e) ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, altered or removed (**data entry control**);

f) ensuring that personal data which are processed by subcontractors can only be processed in conformance with the instructions of the ordering party (**subcontractor control**);

g) ensuring that personal data are protected against accidental destruction or loss (**availability control**);

h) guaranteeing that data which have been collected for different purposes can be processed separately (separation rule).

Article 7
Rights of Data Subjects

§ 23 Right to Question and Complain

Every data subject has the right at any time to contact the data protection department of the responsible company with questions and complaints regarding the application of this Code of Conduct. If not subsequently specified otherwise, for the purpose of these provisions, the responsible company shall be any company that has a contract relationship with the data subject or that processes the data subject's personal data. The company that the data subject has contacted shall make sure that the data subject's rights are properly observed by the other responsible companies.

§ 24 Right to Information

(1) Every data subject may at any time request information from the responsible company concerning:

a) the personal data recorded on them, including its origin and recipient(s);

b) the purpose of the processing or use;

c) the people and units to whom/which their data are regularly transmitted, particularly if the data are transmitted abroad;

d) the provisions of this Code of Conduct.

(2) The relevant information should be made available to the enquirer in an understandable form within a reasonable period of time. This should generally be done in writing or electronically.

(3) Where permissible under the relevant national law, a company may charge a fee for supplying the relevant information.

§ 25 Right of Protest/Right to Have Data Erased/Blocked

(1) The data subject concerned can protest to the responsible company against the use of his/her data, if he/she has the right to do so.

(2) This right to protest shall also apply in the event that the data subject had previously consented to the use of his/her data.

(3) Rightful requests to have data erased or blocked shall be promptly met. Such requests are rightful particularly when the legal basis for the use of the data ceases to apply. If a data subject has the right to have data erased, but erasing the data is not possible or not possible with reasonable effort, the data shall be protected against non-permitted usage by blocking. Statutory retention periods shall be observed.

§ 26 Right to Correction

The data subject may at any time request that the responsible company corrects the personal data recorded on them insofar as such data are incomplete and/or incorrect.

§ 27 Right to Clarification and Comments

(1) If a data subject claims that his/her rights have been breached in the form of unlawful data processing, particularly in the event that this Code of Conduct has been breached, the responsible companies shall clarify the facts without culpable delay. In this case they shall work together closely and grant each other access to all information necessary for establishing the facts of the case.

(2) The company's responsible data protection department most closely associated with the relevant issues must coordinate all the relevant correspondence with the data subject.

§ 28 Exercising of Rights of Data Subjects

Data subjects shall not be disadvantaged because they have availed themselves of these rights. The form of communication with the data subject - e.g. by telephone, electronically or in writing - should respect the request of the data subject, where appropriate.

Article 8
Data Protection Process Management/Responsibilities

§ 29 Responsibility for Data Processing

(1) The companies shall, in their capacity as Data Controllers, be obliged, particularly vis-à-vis data subjects, to guarantee compliance with the requirements of data protection and with the provisions of this Code of Conduct.

(2) The data protection officer of the respective company shall be informed without delay about any breaches (including suspicion of a breach) of data protection provisions and of this Code of Conduct. In the case of incidents that are of relevance to more than one company, the central Group Privacy Department should also be informed. The company's data protection officer shall also inform the Group Privacy Department if any changes are made to the laws applying for a company that are significantly unfavorable.

(3) The data protection departments of the individual companies shall coordinate their activities within the framework of the Group's data protection policy. Accordingly, they should mutually support each other and make use of existing synergies.

§ 30 Coordination by the Group Privacy Officer

(1) The Group Privacy Officer shall coordinate the processes of cooperation and agreement in all significant issues regarding data protection. The Deutsche Telekom Group Coordination Committee on data protection shall serve as the coordinating body.

(2) It shall be the duty of the Group Privacy Officer to develop and evolve the Group's policy on data protection. Also in this regard, the data protection departments of the companies shall engage in coordination.

§ 31 Supervisory and Consultation Duties

(1) The data protection officers of the respective companies shall be responsible for monitoring compliance with national and international data protection regulations and with this Code of Conduct. In this regard, all departments of the respective companies shall be obliged to inform the relevant data protection officer of appropriate developments and future plans.

(2) In the absence of legal restraints, the respective data protection officers shall be authorized to examine on-site all processing techniques that involve the use of personal data.

(3) Where appropriate, and within the framework of their examination duties, the data protection units of the companies shall use mechanisms which are identical throughout the Group, e.g. in the form of common data protection audits.

§ 32 Employee Training and Commitment

(1) The employees of the companies shall be sufficiently trained with regard to the data protection regulations and application of this Code of Conduct.

(2) The companies shall, with the participation of the competent data protection departments, devise suitable training materials.

§ 33 Cooperation with Supervisory Authorities

(1) The companies shall agree to respond to enquiries by the supervisory authority responsible for them or if applicable for the company exporting the data within a reasonable period of time and to a reasonable extent and to follow the supervisory authority's recommendations.

(2) In the event of a change in the legislation applicable to a company which might have substantial adverse effect on the guarantees provided by this Code of Conduct the relevant company will notify the change to the relevant supervisory authority.

Article 9
Terms and Definitions

Automated individual decisions

Shall mean decisions which produce legal effects for the data subject or which significantly affect him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Data subject

Shall mean any natural person whose personal data is handled in the Deutsche Telekom Group.

Data controller

Shall mean the company which alone or jointly with others determines the purposes and means of the processing of personal data.

Deutsche Telekom Group

Shall mean Deutsche Telekom AG and all companies in which Deutsche Telekom AG directly or indirectly holds more than a 50% share, or over which it has control.

Data processor

Shall mean any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller (subcontracting data processing)

Company

Shall mean any company that has agreed to be bound by this Code of Conduct and that is listed in Annex A hereto.

Personal data

Shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Handling of personal data

Shall mean any operation or set of operations which is performed upon personal data such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This also includes the processing of personal data in structured manual files.

Recipient

Shall mean any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not. However, public authorities that may receive data as part of a single inquiry shall not be considered to be recipients.

Special categories of data

Shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life.

Third party

Shall mean any person or body outside the data controller. Third parties shall not mean the data subject or persons or bodies who by order collect, process or use personal data in Germany, in another member state of the European Union or in another state party of the agreement on the European Economic Area.