BINDING CORPORATE RULES PRIVACY (BCRP)

BINDING CORPORATE RULES FOR THE PROTECTION OF PERSONAL RIGHTS IN THE HANDLING OF PERSONAL DATA WITHIN THE DEUTSCHE TELEKOM GROUP

Deutsche Telekom AG, Group Privacy

Version 2.7
Last revised Dec. 05, 2013
Status *final*

Enacted by the Board of Management of T-Systems Nederland B.V. date: Jan. 01, 2016
And upfront also agreed with the Local Workers Council (O.R.)

LIFE IS FOR SHARING.

IMPRINT

Editor

Deutsche Telekom AG
Data Privacy, Legal Affairs and Compliance Board department
Group Privacy
Friedrich-Ebert-Allee 140, 53113 Bonn, Germany

Title	Version	Document type
Binding Corporate Rules Privacy DTAG.docx	2.7	Germany and abroad

Authors	Released by	Contact
Daniel Hoff Marcus Schmitz, GPR Dr. Jörg Friedrichs, GPR	Head of Group Privacy Dr. Claus-Dieter Ulmer	Marcus Schmitz, GPR Dr. Jörg Friedrichs, GPR Stephanie König, GPR
Status and last revised	**Date of validity**	**Location of document**
Final Dec. 05, 2013	For Deutsche Telekom AG from July 01, 2014 in accordance with approval by the Board of Management on June 10, 2014. In the domestic Group companies, as per board approval or decision of the responsible board member.	DTAG Corporate Rule Base (http://policies.telekom.de)

Brief summary

Regulation for the handling of personal data in the Group; New version of the Privacy Code of Conduct

CHANGE HISTORY

Version	Status of	Editor	Changes / Comments
2.2	Jan. 20, 2013	Sonja Klauck	Revised version of the Privacy Code of Conduct, German, Version 2.1
2.3	Feb. 08, 2013	Dr. Claus-Dieter Ulmer	Full revision
2.4	Feb. 14, 2013	Dr. Claus-Dieter Ulmer	Data transfer and liability
2.5	Mar. 21, 2013	Marcus Schmitz Dr. Claus-Dieter Ulmer	Revision with comments from German Federal Commissioner for Data Protection and Freedom of Information
2.6	Apr. 09, 2013	Daniel Hoff	Revision with comments from German Federal Commissioner for Data Protection and Freedom of Information
2.7	Dec. 05, 2013	Daniel Hoff Marcus Schmitz	Revision with comments from the Austrian Data Protection Authority

Please note: As printout of this Group policy may already be outdated. Please always check the Corporate Rule Base of Deutsche Telekom AG (http://policies.telekom.de) to determine whether this is the current version of the Group policy.

CONTENTS

Note:

In case these Binding Corporate Rules Privacy shall be implemented by individual rules in the companies each existing collective bargaining arrangements and participation rights of the relevant employee representative bodies must be observed.

PREAMBLE

(1) Protecting the personal data of customers, employees and other individuals connected with the Deutsche Telekom Group is a top priority for all companies within the Deutsche Telekom Group.

(2) 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.

(3) In many areas, the Deutsche Telekom Group is perceived by its customers and the general public 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 innovative services by implementing these Binding Corporate Rules Privacy.

(4) In providing these Binding Corporate Rules Privacy, the Deutsche Telekom Group is creating a standardized and high level of data privacy worldwide, applicable to the use of data both within one company and across companies, and to the transfer of data within Germany and internationally. Within the Deutsche Telekom Group, personal data must be processed by the recipient according to the principles of data protection law that apply to the transferring party.

PART ONE
SCOPE

§ 1 Legal nature of the Binding Corporate Rules Privacy

The Binding Corporate Rules Privacy shall be binding with regard to the processing of personal data (according to working paper 133, Article 29 of the working group of the European Commission) by all Deutsche Telekom Group companies which have adopted them on a legally binding basis. The Binding Corporate Rules Privacy shall also be binding on all companies that can be required by Deutsche Telekom to adopt them and on all companies that have adopted them on a voluntary basis, regardless of where data is collected.

§ 2 Scope of application

The Binding Corporate Rules Privacy shall apply to all types of personal data use within the Deutsche Telekom Group, regardless of where the data is collected. Personal data shall be used within the Deutsche Telekom Group for the following purposes in particular:

(1) To manage employee data when initiating, implementing and processing employment contracts and to address employees with products and services offered to them by the Deutsche Telekom Group or third parties.

(2) To initiate, implement and process business-customer and consumer agreements, and to carry out advertising and market-research activities aimed at informing customers and interested third parties about products and services offered by the Deutsche Telekom Group or third parties as appropriate.

(3) To initiate and implement agreements with Deutsche Telekom Group service providers as part of the provision of services for the Deutsche Telekom Group.

(4) To enable appropriate dealings with other third parties, in particular shareholders, partners or visitors, and to comply with binding legal regulations.

Data shall be used in line with the current and future business purposes of the Deutsche Telekom Group companies, which include the provision of telecommunications services, digital services for consumers and business customers, IT services (including data center services) and advisory services.

§ 3 Relationship to other legal provisions

(1) The provisions of the Binding Corporate Rules Privacy are designed to ensure a high and standardized level of data privacy throughout the Deutsche Telekom Group. Existing obligations and regulations which individual companies have to comply with for the processing and use of personal data that go beyond the principles laid out in these Binding Corporate Rules Privacy, or that contains additional restrictions on the processing and use of personal data, shall remain unaffected by these Binding Corporate Rules Privacy.

(2) Data collected in Europe shall be used generally in accordance with the legal provisions of the country in which the data was collected, regardless of where the data is used, but at the very least in accordance with the requirements of these Binding Corporate Rules Privacy.

(3) The applicability of national legislation decreed for reasons of state security, national defense or public safety, or to prevent and investigate crimes and prosecute criminals, that requires data to be passed on to third parties shall remain unaffected by the provisions of these Binding Corporate Rules Privacy. If a company finds that significant sections of these Binding Corporate Rules Privacy contravene national data privacy provisions, preventing the parties from signing these Binding Corporate Rules Privacy, then the Group Data Privacy Officer of the Deutsche Telekom Group shall be informed without delay. The responsible supervisory authority of the company shall be involved in a mediatory capacity.

§ 4 Expiry and termination

These Binding Corporate Rules Privacy shall cease to be binding on a company if it leaves the Deutsche Telekom Group or invalidates these rules. However, the expiry or invalidation of the Binding Corporate Rules Privacy shall not release the company from the obligations and/or provisions of the Binding Corporate Rules Privacy governing the use of data already transmitted. Further data transfer from or to this company can only take place if other appropriate procedural guarantees are provided in line with the requirements of European law.

PART TWO
PRINCIPLES

SECTION 1
TRANSPARENCY OF DATA PROCESSING

§ 5 Duty to inform

The data subjects shall be informed about how their personal data is used in line with applicable legislation and the following conditions.

§ 6 Content and form of information

(1) The company shall inform the data subjects adequately about the following items:

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

b) the intended use and purpose of use of the data. This information is to include which data is being recorded and/or processed/used, why, for what purpose and for how long.

c) If personal data is transferred or transmitted to third parties, the recipient, scope and purpose(s) of such transfer/transmission shall be known.

d) the rights of the data subjects in connection with the use of their data.

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

§ 7 Availability of information

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

SECTION 2
CONDITIONS OF ADMISSIBILITY FOR THE USE OF PERSONAL DATA

§ 8 Principle

Personal data shall only be used under the following conditions and shall not be used for purposes other than those for which it was originally collected.

The use of collected data for other purposes shall only be permitted if the conditions of admissibility have been satisfied in accordance with the following conditions.

§ 9 Admissibility of personal data use

Personal data can be used if one or more of the following criteria have been satisfied:

a) It is clearly legally permissible to use the data in the way intended.

b) The data subject has consented to his/her data being used.

c) It is necessary to use the data in this way in order for the company to fulfill its obligations under an agreement with the data subject, including its contractual duties to inform and/or secondary duties, or in order for the company to implement pre- or post-contractual measures for initiating or processing an agreement that have been requested by the data subject.

d) The data must be used to fulfill a legal obligation of the company.

e) It is necessary to use the data to safeguard the data subject's vital interests.

f) It is necessary to use the data to complete a task that is in the interest of the general public or that forms part of the exercise of public authority and with which the company or third party to whom the data is transferred was charged.

g) It is necessary to process the data in order to realize the legitimate interests of the company or the third party/parties to whom data is being transmitted, provided these interests are not clearly outweighed by interests of the data subject warranting protection.

§ 10 Consent by the data subject

It shall be deemed that the data subject has given his/her consent pursuant to § 9 (1), item b) of these Binding Corporate Rules Privacy if:

a) Consent has been given expressly, voluntarily and on an informed basis that makes the data subject aware of the scope of what he/she is consenting to. 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. For business models in which the withdrawal leads to a non-fulfillment of contractual obligations the data subject shall be informed.

b) Consent has been obtained in a form appropriate to the circumstances (written form). 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.

§ 11 Automated individual decisions

a) 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 data use. This includes in particular decisions for which data about the creditworthiness, professional suitability or state of health of the data subject is significant.

b) 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 The use of personal data for direct marketing purposes

Where data is used for direct marketing purposes, data subjects shall be:

a) informed about the way in which their data will be used for direct marketing purposes;

b) informed about their right to object at any time to the use of their personal data for direct marketing communications, and

c) equipped to exercise their right not to receive such communications. They shall receive, in particular, information about the company to whom the objection should be made.

§ 13 Special categories of personal data

a) The use of special categories of data shall only be permitted where it is governed by legal regulations or where the data subject's consent has been obtained in advance. It shall also be permissible if it is necessary to process the data in order to fulfill the rights and obligations of the company in the area of labor law, provided that suitable protection measures are taken and that this is not prohibited under national law.

b) Prior to the commencement of such collection, processing or use, the company shall inform its Data Privacy Officer accordingly and document this action. When assessing admissibility, particular consideration should be given to the nature, scope, purpose, necessity and legal basis of using the data.

§14 Data minimization, data avoidance, anonymization and aliasing

(1) Personal data shall be appropriate, relevant and not excessive with regard to the use of the data for a specific purpose (data minimization). 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 (aliasing).

§15 Prohibition of tying-in

The use of services, or the receipt of products and/or services, shall not be made conditional upon data subjects consenting to the use of their data for purposes other than the initiation or fulfillment of an agreement. 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.

SECTION 3
TRANSFER OF PERSONAL DATA

§16 Nature and purpose of transfer of personal data

(1) Personal data can only be transferred where the receiving party assumes responsibility for the data received (transmission) or where the recipient only uses the data in accordance with the instructions and requirements of the transferring party (commissioned data processing agreement).

(2) Personal data shall only be transferred for the permitted purposes pursuant to § 9 of these Binding Corporate Rules Privacy as part of the company's business activities or legal obligations, or following consent from the data subjects.

§ 17 Transmission of data

(1) If a company transmits data to bodies that are headquartered in a third country or that transfer data across national borders, steps shall be taken to ensure that this data is transmitted properly Appropriate data privacy and data security requirements shall be agreed with the recipient before data is transmitted. In addition, personal data, particularly data collected in the EU or the EEA, shall only be transmitted to controllers outside of the European Union if the appropriate level of data privacy has been ensured using these Binding Corporate Rules Privacy or other appropriate measures, such as the EU standard contractual clauses or individual contractual agreements that meet the relevant requirements of European law.

(2) Based on the requirements of the Deutsche Telekom Group and generally recognized technical and organizational standards, appropriate technical and organizational measures shall be taken to guarantee the security of personal data, including during its transmission to another party.

§ 18 Commissioned data processing[1]

(1) When a company (customer) commissions a third party (contractor) to provide services on its behalf in accordance with its instructions, then, in addition to a service agreement comprising the work to be performed, the agreement shall also refer to the obligations of the contractor as the party commissioned to process the data. These obligations shall set out the instructions of the customer concerning the type and manner of processing of the personal data, the purpose of processing and the technical and organizational measures required for data protection.

(2) The contractor shall not use the personal data (entrusted to it for performing the order) for its own or third-party processing purposes without the prior consent of the customer. The contractor shall inform the customer in advance of any plans to sub-contract work out to other third parties in order to fulfill its contractual obligations. The customer shall have the right to object to such use of subcontractors. Where subcontractors are used in the permissible way, the contractor shall obligate them to comply with the requirements of the agreements concluded between the contractor and the customer.

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

SECTION 4
DATA QUALITY AND DATA SECURITY

§ 19 Data quality

(1) Personal data shall be correct and, where necessary, kept up to date (data quality).

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

[1] This § is not a provision in the sense of working paper 195 of Art. 29 working group of the European commisssion.

§ 20 Data security – technical and organizational measures

The company shall take appropriate technical and organizational measures for company processes, IT systems and platforms used to collect, process or employ data in order to protect this data.

Such measures shall include:

a) preventing unauthorized persons from gaining access to data processing systems on which personal data is processed or used (admittance 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 the 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 its transport or recording on data media, personal data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to check and identify the controllers to which personal data is 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 has been entered into data processing systems, altered or removed (data entry control);

f) ensuring that outsourced personal data can only be processed in accordance with the instructions of the customer (contractor control);

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

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

PART THREE
RIGHTS OF DATA SUBJECTS

§ 21 Right to information

(1) Data subjects shall be entitled at any time to contact any company using their data and request the following information:

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

b) the purpose of use;

c) the persons and controllers to whom/which their data is regularly transmitted, particularly if the data is transmitted abroad;

d) the provisions of these Binding Corporate Rules Privacy.

(2) The relevant information is to be made available to the enquirer in an understandable form within a reasonable period of time. This is generally done in writing or electronically. Providing a hard copy of these Binding Corporate Rules Privacy shall suffice as a means of communicating information about their requirements.

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

§ 22 Right of protest, right to have data erased or blocked, and right to correction

(1) Data subjects can object to the use of their data at any time if this data is being used for purposes that are not legally binding.

(2) This right of protest shall also apply in the event that data subjects had previously consented to the use of their data.

(3) Legitimate requests to have data erased or blocked shall be promptly met. Such requests are legitimate 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 unreasonable, the data shall be protected against non-permitted usage by blocking. Statutory retention periods shall be observed.

(4) Data subjects can request from the company to correct the personal data it holds on them at any time if this data is incomplete and/or incorrect.

(5) For business models in which the withdrawal or the erasure leads to a non-fulfillment of contractual obligations the data subject shall be informed.

§ 23 Right to clarification, comments and remediation

(1) If a data subject claims that his/her rights have been violated by unlawful use of his/her data, particularly by providing evidence of a verifiable violation of these Binding Corporate Rules Privacy, the responsible companies shall clarify the facts without deliberate delay. For data transferred or transmitted to companies outside of the European Union in particular, the company based in the European Union shall clarify the facts and provide evidence that the receiving party has not violated the requirements of these Binding Corporate Rules on Data Privacy or is responsible for any damage caused. The companies shall work together closely to clarify the facts and shall grant each other access to all information they require to do so.

(2) The data subject concerned can file a complaint against the Deutsche Telekom Group Holding at any time if he/she suspects that a Deutsche Telekom Group company is not processing his/her personal data in accordance with legal requirements or with the provisions of these Binding Corporate Rules

Privacy. The substantiated complaint shall be dealt with within an appropriate period of time and the data subject informed accordingly.

(3) If a complaint concerns several companies, the Data Privacy Officer of the company most familiar with the subject matter shall coordinate all relevant correspondence with the data subject. The Group Data Privacy Officer shall be entitled to exercise his/her right of subrogation and takeover at any time.

(4) There shall be suitable channels in place for reporting data privacy incidents (such as a special purpose e-mail account provided by Data Privacy, Legal Affairs and Compliance or a direct contact who can be contacted online).

(5) The Data Privacy Officer of the company concerned shall inform the Group Data Privacy Officer of a data privacy incident without delay using the relevant reporting processes.

(6) Data subjects can make a claim pursuant to Part Five of these Binding Corporate Rules Privacy if their rights have been infringed or if they have suffered any loss.

§ 24 Right to question and complain

Every data subject has the right at any time to contact the Data Privacy Officer of the company using his/her personal data with questions and complaints regarding the application of these Binding Corporate Rules Privacy. The company most familiar with the subject matter or the company that collected the data subject's data shall make sure that the data subject's rights are properly observed by the other responsible companies.

§ 25 Exercising of rights of data subjects

Data subjects shall not be disadvantaged because they have made use 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.

§ 26 Hard copy of the Binding Corporate Rules Privacy

A hard copy of these Binding Corporate Rules Privacy shall be provided to anyone upon request.

PART FOUR
DATA PRIVACY ORGANIZATION

§ 27 Responsibility for data processing

The companies shall be obligated to ensure compliance with the legal provisions on data protection and with these Binding Corporate Rules Privacy.

§ 28 Data Privacy Officer

(1) Each company shall appoint an independent Data Privacy Officer , whose task is to ensure that the individual organizational units of that company are advised on the statutory and internal company/Group requirements for data privacy and, in particular, on these Binding Corporate Rules Privacy. The Data Privacy Officer shall use suitable measures, in particular random inspections, to monitor compliance with data protection regulations.

(2) The company shall consult with the Group Data Privacy Officer before appointing a Data Privacy Officer.

(3) The company shall ensure that the Data Privacy Officer possesses the relevant expertise for evaluating the legal, technical and organizational aspects of data privacy measures.

(4) The company shall provide the Data Privacy Officer with the financial and personnel resources necessary for carrying out his/her duties

(5) The Data Privacy Officer shall be granted the right to report directly to company management, and shall be connected organizationally to company management.

(6) The Data Privacy Officer of each company shall be responsible for implementing the requirements of the Group Data Privacy Officer and of the Deutsche Telekom Group's data privacy strategy.

(7) All departments of each company shall be obligated to inform their company's Data Privacy Officer of any developments in IT infrastructure, network infrastructure, business models, products, staff data processing and corresponding strategic plans. The Data Privacy Officer shall be brought in on new developments at an early stage in order to ensure that any data privacy matters can be considered and evaluated.

§ 29 Group Data Privacy Officer

(1) The Group Data Privacy Officer shall coordinate the processes of cooperation and agreement on all significant issues regarding data privacy within the Deutsche Telekom Group. He shall inform the CEO of the Deutsche Telekom Group Holding about current developments and draft recommendations where necessary.

(2) It shall be the duty of the Group Data Privacy Officer to develop and evolve the Deutsche Telekom Group's policy on data privacy, consulting with the Data Privacy Officers of the Group companies where appropriate. These Data Privacy Officers shall develop the data privacy policy for their company in line with the Group data privacy policy. The Group Data Privacy Officer and the Data Privacy Officers from the national companies shall meet annually to share information at the International Privacy Leader Meetings (face-to-face events).

§ 30 Duty to inform in case of infringements

The company concerned shall inform its Data Privacy Officer immediately of any infringement or clear indication of infringement of data protection regulations in particular of these Binding Corporate Rules Privacy. The Data Privacy Officer shall in turn inform the Group Data Privacy Officer immediately if the incident has a potential impact on the public, affects more than one company, or entails a potential loss of over EUR 500,000. The company's Data Privacy Officer shall also inform the Group Data Privacy Officer if any changes are made to the laws applying to a company that are significantly unfavorable to compliance with these Binding Corporate Rules Privacy.

§ 31 Review of the level of data privacy

(1) Reviews to find out about the compliance with the requirements of these Binding Corporate Rules Privacy and the level of data privacy derived there from shall be carried out by the Group Data Privacy Officer as part of an annual inspection plan as well as by other measures such as inspections carried out by the Data Privacy Officers of the companies and reporting.

(2) Internal and external auditors shall carry out the inspections of the Group Data Privacy Officer. Regular self-assessments shall also be carried out within the Deutsche Telekom Group, coordinated by the Group Data Privacy Officer. The CEO of the Deutsche Telekom Group Holding shall be informed of the results of key inspections and the subsequently agreed measures. The responsible data supervisory authority shall be sent a copy of the inspection results upon request. The supervisory authority responsible for the company can also initiate an inspection. The company shall provide as much support as possible for these inspections and shall implement the measures derived there from.

(3) The company shall take relevant measures to remedy any weaknesses identified during an inspection, and the Group Data Privacy Officer shall monitor the implementation of these measures. If the company fails to implement the measures without sufficient reasons, the Group Data Privacy Officer shall assess the impact on data privacy and take the necessary action, escalating the matter where necessary.

(4) The Data Privacy Officers of the companies or other organizational units commissioned to conduct inspections shall also carry out checks based on dedicated audit plans documented in writing to determine whether the companies are complying with data protection requirements.

(5) In the absence of legal restraints, the Group Data Privacy Officer and the Data Privacy Officers shall be authorized to check, at all companies and at their own company respectively, whether personal data is being used properly. The companies concerned shall grant the Group Data Privacy Officer and the Data Privacy Officers full access to the information they require to clarify and evaluate a situation. The Group Data Privacy Officer and the Data Privacy Officers shall be entitled to issue instructions in this regard.

(6) As part of their inspections, the Data Privacy Officers of the companies shall use standardized procedures valid for the entire Group, e.g. common data protection audits, wherever possible. Such procedures can be made available by the Group Data Privacy Officer.

§ 32 Employee commitment and training

(1) The companies shall obligate their employees to maintain the data and telecommunications secrecy upon commencing their employment at the latest. Employees shall receive sufficient training in data privacy matters as part of this commitment. The company shall initiate suitable processes and provide resources to this end.

(2) Employees shall receive training in the basics of data privacy regularly, or at least every two years. The companies shall be entitled to develop and run dedicated training courses for their own employees. The Data Privacy Officer of each company shall document the delivery of these training courses and inform the Group Data Privacy Officer on an annual basis.

(3) The Group Data Privacy Officer can make resources and processes available centrally for obligating and training Deutsche Telekom Group employees.

§ 33 Cooperation with supervisory authorities

(1) The companies shall agree to work together on the basis of trust with the supervisory authority responsible for them or for the company transmitting data, in particular, to respond to queries and follow recommendations.

(2) In the event of a change in the legislation applicable to a company which might have substantial adverse effects on the guarantees provided by these Binding Corporate Rules Privacy, the company concerned shall notify the responsible supervisory authority of the change.

§ 34 Responsible contacts for queries

The Data Privacy Officers of the companies or the Group Data Privacy Officer are the contacts responsible for dealing with queries about these Binding Corporate Rules Privacy. The Group Data Privacy Officer shall provide the contact details for the Data Privacy Officers of the companies upon request.

The Group Data Privacy Officer can be contacted at

datenschutz@telekom.de

privacy@telekom.de

+49-228-181-82001

during normal business hours (Central European Time).

PART FIVE
LIABILITY

§ 35 Area of application of the rules on liability

(1) This Part Five of The Binding Corporate Rules shall apply exclusively for the processing of personal data collected in the EU / the EEA, which falls within the scope of the EU Directive on Data Protection 95/46/EC.

(2) Within the EU/EEA, the legal liability provisions of the country in which a company is headquartered shall apply. For data that is not subject to § 35, Section 1 of the BCRP the legal liability provisions of the country in which the respective company that collected the data has its registered office, or if there are no legal provisions existing, the terms and conditions of the company that collected the data shall apply.

(3) Payment of exemplary damages, where a company must make payments to a data subject that exceed the damage itself, shall be explicitly ruled out.

§ 36 Indemnitor

(1) Any individual who has suffered loss as a result of one or more of the duties specified in the Binding Corporate Rules Privacy being violated by a Deutsche Telekom Group company or by data recipients to which a Deutsche Telekom Group company has transferred or transmitted data, shall be entitled to claim corresponding damages against the Deutsche Telekom Group companies concerned.

(2) The data subject shall also be entitled to claim damages against the Deutsche Telekom Group holding company. If the holding company pays damages, it shall be entitled to claim reimbursement from the companies that are responsible for the loss or that commissioned a third party which caused it. .

(3) The data subject shall claim damages initially against the company that transferred or transmitted the data. If the transferring company is not liable de jure or de facto, the data subject shall be entitled to claim damages from the recipient company. The recipient company shall not be entitled to withdraw from liability by appealing to the responsibility of a contractor in case of violation.

(4) The data subject shall be entitled to submit a complaint to the responsible supervisory authority or to the supervisory authority responsible for the Deutsche Telekom Group holding company at any time.

§ 37 Burden of proof

The burden of proof for the proper use of the data subject's data shall rest with the liable companies.

§ 38 Third-party benefits for data subjects

If the data subject has no direct rights, he/she shall be entitled, as a third-party beneficiary, to assert claims against companies which have violated their contractual duties, based on the provisions of these Binding Corporate Rules Privacy.

§ 39 Place of jurisdiction

At the individual's discretion, the place of jurisdiction to assert liability claims may be

a) applicable to the individual concerned or

b) within the jurisdiction of the member of the group at the origin of the transfer or,

c) the EU headquarters or the European member of the group with delegated data protection responsibilities.

§ 40 Out-of-court arbitration

(1) Third parties who consider their individual right to privacy to have been violated as a result of actual or suspected use of their personal data shall be entitled to request that the Data Privacy Officer of the company concerned arbitrate in the matter. The Data Privacy Officer shall be entitled to examine the complaint and advise the data subject on his/her rights. In doing so, the Data Privacy Officer shall be obligated to maintain the confidentiality of other personal data of the complainant unless the complainant releases the Data Privacy Officer from such obligation. At the request of the individual concerned, an attempt shall be made to reach an agreement regarding the complaint, with the involvement of the data subject and the Data Privacy Officer. Such an agreement may also include a recommendation regarding compensation for any loss suffered as a result of the data subject's right to privacy being violated. This recommendation shall be binding on the companies concerned if it is approved by mutual consent.

(2) The right to submit a complaint to the responsible supervisory authority or to take legal action shall remain unaffected.

PART SIX
FINAL PROVISIONS

§ 41 Reviewing and amending these Binding Corporate Rules Privacy

(1) The Group Data Privacy Officer shall examine the Binding Corporate Rules Privacy at regular intervals, but at least once a year, to find out about their compliance with applicable legislation, and shall make any necessary adjustments.

(2) Any significant amendments to these Binding Corporate Rules Privacy that become e.g. necessary as a result of adjustments made to bring them in line with legal requirements shall be agreed with the supervisory authority. These amendments shall apply directly to all companies that have signed the Binding Corporate Rules Privacy following an appropriate transition period.

(3) The Group Data Privacy Officer shall inform all companies that have introduced the Binding Corporate Rules Privacy of the amended content.

(4) The Data Privacy Officers of the companies shall be obligated to examine whether amendments to these Binding Corporate Rules Privacy have any implications for legal compliance in their own country or whether they conflict with the legal provisions in their respective country. If the company is unable to implement the amendments for biding legal reasons, it shall inform the Group Data Privacy Officer and the responsible supervisory authority immediately and, if relevant, these Binding Corporate Rules Privacy shall be suspended temporarily for this company.

§ 42 List of contacts and companies

The Group Data Privacy Officer shall keep a list of companies that have introduced these Binding Corporate Rules Privacy and the contacts for these companies. He shall keep this list up to date and inform data subjects and data protection authority upon request.

§ 43 Procedural law / severability clause

These Binding Corporate Rules Privacy shall be subject to the procedural law of the Federal Republic of Germany in the case of disputes.

If individual provisions of these Binding Corporate Rules Privacy are or become void, they shall be deemed to have been replaced by the provisions that most closely approximate the original intentions of these Binding Corporate Rules Privacy and the void provisions. In case of doubt, the applicable data protection regulations of the European Union shall apply in these cases or in the absence of relevant provisions.

§ 44 Publication

The companies shall make information about the rights of data subjects and the third-party benefit clause available to the public in a suitable format, such as in the notes on data protection on the Internet. This information shall be published as soon as these Binding Corporate Rules Privacy have become binding on a company.

PART SEVEN
DEFINITIONS AND TERMS

Aliasing

Shall mean the replacement of a person's name and other identification features with another characteristic in order to prevent the data subject being identified or make it considerably harder to identify the data subject.

Anonymization

Anonymization shall mean the process of changing information in such a manner that personal details and other facts can no longer be traced back to an identified or identifiable natural person or can no longer be traced back to such a person without a disproportionately large amount of effort in terms of time, cost and energy.

Automated individual decisions

Shall mean decisions which have legal implications for the data subject or which have a significant adverse effect on him/her and which are based solely on automated processing of data intended to evaluate certain personal aspects of the data subject, such as his/her performance at work, creditworthiness, reliability, conduct, etc.

Company

Shall mean any company that is subject to these Binding Corporate Rules Privacy. A separate list of these companies is kept for reference purposes and updated on an ongoing basis. The list can be viewed by anyone at any time.

Controller

Shall mean any body that processes personal data, but is not necessarily a legal person.

Data subject

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

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 which are fully consolidated.

Group Holding

The Group Holding is currently Deutsche Telekom AG, headquartered on Friedrich-Ebert-Allee 140, 53113 Bonn, Germany.

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/her physical, physiological, mental, economic, cultural or social identity.

Recipient

Shall mean any natural or legal person, public authority, agency or any other body to whom personal data is 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 personal 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 controller outside the body in charge. Third parties shall not mean the data subject or persons or controllers who are commissioned to collect, process or use personal data in Germany, in another member state of the European Union or in another state party to the agreement on the European Economic Area.

Use

Shall mean any handling of personal data, particularly collection, processing and use, including transfer, of such data.