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

Version 3.0 final
29.12.2023

Public

Connecting your world.

Publication Details

Published by

Deutsche Telekom AG
Group Privacy
Friedrich-Ebert-Allee 140, 53113 Bonn, Germany

File name	Document number	Document name
[Binding Corporate Rules Privacy DTAG.docx]	[2.9]	[Binding Corporate Rules Privacy]

Version	Last revised	State
3.0 final	29.12.2023State	

Author	Contents reviewed by	Approved by
Dr. Jörg Friedrichs	Jan Lichtenberg, Strategy & Steering	Dr. Claus-Dieter Ulmer, Group Privacy Officer
Bonn, 27.10.2023	[Bonn, 30.10.2023]	[Bonn, 31.10.2023]

Brief summary

Regulation for the handling of personal data in the Group

Change history

Version	Last revised	Edited by	Changes/Comments
2.2	20.01.2013	Sonjy Klauck	Revised version of the Privacy Code of Conduct, German, Version 2.1
2.3	08.02.2013	Dr. Claus-Dieter Ulmer	Full revision
2.4	14.02.2013	Dr. Claus-Dieter Ulmer	Data transfer and liability
2.5	21.03.2013	Marcus Schmitz Dr. Claus-Dieter Ulmer	Revision with comments from German Federal Commissioner for Data Protection and Freedom of Information
2.6	09.04.2013	Daniel Hoff	Revision with comments from German Federal Commissioner for Data Protection and Freedom of Information
2.7	05.12.2013	Daniel Hoff Marcus Schmitz	Revision with comments from the Austrian Data Protection Authority
2.8	19.02.2019	Dr. Jörg Friedrichs Christina Kreft-Spallek	Alignment to General Data Protection Regulation on the basis of WP 256 rev.01
3.0	29.12.2023	Dr. Jörg Friedrichs	Alignment to Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)

Connecting your world.

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As printout of this Group policy may already be outdated.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

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 processing 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.

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.

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 Recommendations 1/2022 of the European Data Protection Board) by all Deutsche Telekom Group companies which have adopted them on a legally binding basis.

§ 2 Scope of application

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

a) 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.

b) 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.

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

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

Data shall be processed 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 legal obligations and regulations which individual companies have to comply with for the processing of personal data that go beyond the principles laid out in these Binding Corporate Rules Privacy, or that contains additional restrictions on the processing of personal data, shall remain unaffected by these Binding Corporate Rules Privacy.

(2) Data collected in the European Economic Area shall be processed generally in accordance with the legal provisions of the country in which the data was collected, regardless of where the data is processed, 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 transferred to third parties shall remain unaffected by the provisions of these Binding Corporate Rules Privacy.

(4) If a company finds that significant sections of these Binding Corporate Rules Privacy contravene national data protection provisions, preventing the parties from complying with 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 processing of data already transferred. Further data transfer from or to this company can only take place if other appropriate safeguards 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 processed 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 controller(s) and their contact details;

b) the contact details of the data protection officer;

c) the purposes of processing of the data; as well as the legal basis for the processing and the period for which the personal data will be stored;

d) if personal data is transferred to third parties, the recipient, scope and purpose(s) of such transfer shall be known;

e) the rights of the data subjects in connection with the processing 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.

§ 8 Record of all categories of processing activities

The companies maintain a record of all categories of processing activities carried out by them. The record shall contain the following information:

a) the name and contact details of the company, of the representative and of the Data Protection Officer;

b) a description of the categories of processing activities and purposes;

c) the categories of recipients and third parties to whom the data will be disclosed or transferred;

d) the names of the third countries and the documentation of appropriate safeguards if these Binding Corporate Rules Privacy are not applicable;

e) where possible, the time limits for erasure and

f) where possible, a general description of the technical and organisational security measures.

Section 2
Conditions of admissibility for the Processing of personal data

§ 9 Principle

(1) Personal data shall only be processed under the following conditions and shall not be processed for purposes that are incompatible with those for which it was originally collected.

(2) The processing of collected data for other purposes shall only be permitted if the conditions of admissibility have been satisfied in accordance with the following conditions (purpose limitation).

§ 10 Lawfullness of personal data processing

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

a) it is clearly legally permissible to process the data in the way intended;

b) the data subject has consented to his/her data being processed;

c) it is necessary to process the data in this way in order for the company to fulfil 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 processed to fulfil a legal obligation of the company;

e) it is necessary to process the data to safeguard the data subject's vital interests;

f) it is necessary to process 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 transferred, provided these interests are not outweighed by interests of the data subject warranting protection.

§ 11 Consent by the data subject

It shall be deemed that the data subject has given his/her consent pursuant to § 10-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-fulfilment 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.

§ 12 Automated individual decision-making including profiling

(1) Decisions which evaluate individual aspects of a person (profiling) 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 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.

§ 13 The processing of personal data for direct marketing purposes

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

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

b) informed about their right to object at any time to the processing 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.

§ 14 Special categories of personal data

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

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

§ 15 Data minimisation, data avoidance, storage limitation, anonymisation and pseudonymisation

(1) Personal data shall be appropriate, relevant and not excessive with regard to the processing of the data for a specific purpose (data minimisation). Data shall only be processed within a certain application when it is necessary (data avoidance). They must be kept in a form which permits identification of data subjects for no longer than it is necessary for the processing purposes (storage limitation).

(2) Where possible and economically reasonable, procedures shall be used to erase the identification features of data subjects (anonymisation) or to replace the identification features with other characteristics (pseudonymisation).

§ 16 Processing of personal data relating to criminal convictions and offences

Processing of personal data collected within the European Economic Area relating to criminal convictions and offences or related security measures based on §10 BCRP shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

§ 17 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 processing 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

§ 18 Nature and purpose of transfer of personal data

(1) Personal data can be transferred either where the recipient determines the purposes and means of the processing or where the recipient only processes the data on behalf of a controller.

(2) Personal data shall only be transferred for the permitted purposes pursuant to § 10 of these Binding Corporate Rules Privacy as part of the company's business activities or legal obligations or following consent from the data subjects.

(3) Personal data shall only be transferred where appropriate data protection and data security requirements are agreed with the recipient before data is transferred.

§ 19 Transfer of data including onward transfers

(1) Personal data collected in the European Economic Area shall only be transferred to controllers or processors in a third country if the appropriate level of data protection has been ensured using these Binding Corporate Rules Privacy or other appropriate safeguards, such as the EU standard contractual clauses or individual contractual agreements that meet the relevant requirements of European law and that enforceable data subject rights and effective legal remedies for data subjects are available in the sense of Part 5 of these Binding Corporate Rules Privacy.

(2) This includes that these Binding Corporate Rules Privacy will be used as a transfer tool following a transfer impact assessment only where a company has assessed that the law and practices in the third country of destination applicable to the processing of the personal data by the recipient do not prevent the recipient from fulfilling its obligations under these Binding Corporate Rules Privacy. This review shall also take into account any requirements to disclose personal data or measures authorising access by public authorities. This applies to all personal data transferred to companies outside the European Economic Area, and onward transfers from companies in third countries to companies in the same or another third country.

(3) A company transferring personal data shall suspend the data transfer if it considers that the Binding Corporate Rules cannot be complied with, or if instructed by the competent supervisory authority to do so. The company has to end the transfer or set of transfers if compliance with the Binding Corporate Rules Privacy is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the company transferring the personal data, be returned to it or destroyed in their entirety.

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

§ 20 Obligations of the recipient in case of access by public authorities

(1) The recipient agrees to notify the company transferring the personal data promptly if it:

a) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Binding Corporate Rules Privacy; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

b) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Binding Corporate Rules Privacy in accordance with the laws of the country of destination; such notification shall include all information available to the recipient.

(2) If the recipient is prohibited from notifying the company transferring the personal data under the

laws of the country of destination, the recipient agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The recipient agrees to document its best efforts in order to be able to demonstrate them on request of the company transferring the personal data.

(3) Where permissible under the laws of the country of destination, the recipient agrees to provide the company transferring the personal data, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(4) The recipient agrees to preserve the information pursuant to paragraphs (1) to (3) for the duration of the contract and make it available to the competent supervisory authority on request.

(5) Paragraphs (1) to (3) are without prejudice to the obligation of the recipient to inform the company transferring the personal data promptly where it is unable to comply with these Binding Corporate Rules Privacy.

(6) The recipient agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The recipient shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the recipient shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the other obligations of the recipient under these Binding Corporate Rules Privacy.

(7) The recipient agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the company transferring the personal data. It shall also make it available to the competent supervisory authority on request.

(8) The recipient agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

§ 21 Data processing on behalf of a controller[1]

(1) When a company (controller) commissions a third party (processor) 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 processor as the party commissioned to process the data. These obligations shall set out the instructions of the controller concerning the type and manner of processing of the personal data, the purpose of processing and the technical and organisational measures required for data protection.

(2) The processor shall not process the personal data (entrusted to it for performing the order) for its own or third-party processing purposes without the prior consent of the controller. The processor shall inform the controller in advance of any plans to sub-contract work out to other third parties in order to fulfil its contractual obligations. The controller shall have the right to object to such use of subprocessors. Where subprocessors are used in the permissible way, the processor shall obligate

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

them to comply with the requirements of the agreements concluded between the processor and the controller.

(3) Companies acting as processor shall notify their controller without undue delay after becoming aware of an incident

(4) Subprocessors shall be selected according to their ability to fulfil the above-stated requirements.

Section 4
Data quality and data security

§ 22 Data quality

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

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

§ 23 Data security – technical and organisational measures – data protection by design and default

The company shall take appropriate technical and organisational measures for company processes, IT systems and platforms used to collect, process or employ data in order to protect this data, which are evaluated on a regular basis regarding their effectiveness.

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 (data access control) and that personal data cannot, during processing be read, copied, altered or removed by unauthorized persons (e.g. by encryption);

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 (processor 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

§ 24 Right of access

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

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

b) the purpose of processing;

c) the recipients to which their data is or have been transferred, particularly if the data is transferred to a third country;

d) the provisions of these Binding Corporate Rules Privacy.

(2) The relevant information is to be made available to the data subject in an understandable form within a reasonable period of time. This is generally done in writing or electronically. In any event the data subject has to be informed within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The data subject shall be informed of any such extension. Providing a hard copy of these Binding Corporate Rules Privacy shall suffice as a means of communicating information about their requirements.

(3) Where permissible under the relevant national law, a company may charge a fee for supplying further copies of the relevant information requested by the data subject.

§ 25 Right to object, right to erasure or restriction of processing, and right to rectification

(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 processing restricted shall be promptly met. Such requests are legitimate particularly when the legal basis for the use of the data ceases to apply. 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-fulfilment of contractual obligations the data subject shall be informed.

§ 26 Right to clarification, comments and remediation

(1) If a data subject claims that his/her rights have been violated by unlawful processing 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 to companies outside of the European Economic Area in particular, the company based in the European Economic Area shall clarify the facts and provide evidence that the recipient 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 shall be informed within one month of the processing status accordingly. This period may be extended by two further months where necessary, taking into account the complexity and number of requests, and the data subject must be informed accordingly.

(3) If a complaint concerns several companies, the Data Protection 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 the Data Protection Officer or a direct contact who can be contacted online).

(5) The Data Protection Officer of the company concerned shall inform the Group Data Privacy Officer of a data privacy incident without delay using the relevant reporting processes and ensure documentation of the data privacy incident, which can be made available to the supervisory authorities on request.

(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.

§ 27 Right to question and complain

Every data subject has the right at any time to contact the Data Privacy Officer of the company processing 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.

§ 28 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.

§ 29 Access to the Binding Corporate Rules Privacy

The current version of these Binding Corporate Rules Privacy and the list of companies which have adopted them on a legally binding basis will be published on *www.telekom.com.*

Part Four
Data Protection Organisation

§ 30 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 and shall be able to demonstrate this at any time.

§ 31 Data Protection Officer

(1) Each company shall appoint an independent Data Protection Officer, whose task is to ensure that the individual organisational units of that company are advised on the statutory and internal company/Group requirements for data protection and, in particular, on these Binding Corporate Rules Privacy. The Data Protection 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 or recalling a Data Protection Officer.

(3) The company shall ensure that the tasks and duties of the Data Protection Officer do not result in a conflict of interest.

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

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

(6) The Data Protection Officer shall be granted the right to report directly to company management and shall be connected organisationally to company management.

(7) The Data Protection 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.

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

§ 32 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 Protection Officers of the Group companies where appropriate. These Data Protection 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 Protection Officers from the national companies shall meet annually to share information at face-to-face events.

§ 33 Duty to inform in case of infringements or changes to the laws and practices applying to the company

The company concerned shall inform its Data Protection Officer immediately of any infringement or clear indication of infringement of data protection regulations in particular of these Binding Corporate Rules Privacy. The Data Protection 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 Group Data Privacy Officer has always to be informed when the competent supervisory authority has imposed an administrative fine on the company.

The company's Data Protection Officer shall also inform the Group Data Privacy Officer if any changes are made to the laws and practices applying to a company that are significantly unfavorable to compliance with these Binding Corporate Rules Privacy.

Companies acting as controller shall inform without undue delay the data subjects where an incident is likely to result in a high risk to their rights and freedoms.

§ 34 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 Protection Officers of the companies and reporting. The annual inspection plan takes into account the risks posed by the processing activities which fall under these Binding Corporate Rules Privacy. Internal and external auditors shall carry out the inspections of the Group Data Privacy Officer. Regular self-assessments can also be carried out within the Deutsche Telekom Group, coordinated by the Group Data Privacy Officer.

(2) 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 Protection Officers of the companies or other organisational 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. Data Protection Officers shall not be the ones in charge of auditing compliance with these Binding Corporate Rules Privacy if such situation can result in a conflict of interest.

(5) In the absence of legal restraints, the Group Data Privacy Officer and the Data Protection 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 Protection Officers full access to the information they require to clarify and evaluate a situation. The Group Data Privacy Officer and the Data Protection Officers shall be entitled to issue instructions in this regard.

(6) As part of their inspections, the Data Protection 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.

§ 35 Data protection impact assessment

The companies shall conduct a structured and documented data protection impact assessment for the processing of personal data. Deutsche Telekom Group Holding provides a centrally available process called Privacy and Security Assessment (PSA) which has to be implemented in its current version uniformly in all companies. Derogations from the use of the PSA process can be made in consultation with and with the prior approval of the Group Data Protection Officer if companies are very small or do not have significant data processing of their own.

§ 36 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 Protection 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.

§ 37 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 transferring 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.

(3) Any dispute related to the Competent Supervisory Authoritys' exercise of supervision of compliance with these Binding Corporate Rules Privacy will be resolved by the courts of the Member State of the Supervisory Authority, in accordance with that Members' State's procedural law. The companies agree to submit themselves to the jurisdiction of these courts.

§ 38 Responsible contacts for queries

The Data Protection 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 Protection Officers of the companies upon request.

The Group Data Privacy Officer can be contacted at

datenschutz@telekom.de

privacy@telekom.de

Friedrich-Ebert-Allee 140,

53113 Bonn

Part Five
Liability

§ 39 Area of application of the rules on liability

(1) This Part Five of the Binding Corporate Rules Privacy shall apply exclusively for the processing of personal data, which falls within the scope of the General Data Protection Regulation 2016/679.

(2) Within the European Economic Area, the legal liability provisions of the country in which a company is headquartered shall apply. For data that is not subject to § 9 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.

§ 40 Indemnitor

(1) Any data subject 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 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 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 shall not be entitled to withdraw from liability by appealing to the responsibility of a processor in case of violation.

(4) The data subject shall be entitled to submit a complaint to the responsible supervisory authority in the Member State of his habitual residence, place of work or place of the alleged infringement or to the supervisory authority responsible for the Deutsche Telekom Group holding company at any time.

(5) The data subject shall have the right to lodge a complaint before the competent courts of the European Economic Area, where he or she considers that his or her rights under this Binding Corporate Rules have been infringed as a result of the processing of his or her personal data in non-compliance with this Binding Corporate Rules.

(6) The data subject shall have the right to mandate a not-for-profit body, organisation or association to exercise the aforementioned rights on his or her behalf.

§ 41 Burden of proof

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

§ 42 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.

§ 43 Place of jurisdiction

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

a) where the individual concerned has his or her habitual residence or

b) within the jurisdiction where the member of the group has an establishment or,

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

§ 44 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 processing of their personal data shall be entitled to request that the Data Protection Officer of the company concerned arbitrate in the matter. The Data Protection Officer shall be entitled to examine the complaint and advise the data subject on his/her rights. In doing so, the Data Protection Officer shall be obligated to maintain the confidentiality of other personal data of the complainant unless the complainant releases the Data Protection 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 Protection 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 either before the supervisory authority in the Member State of his habitual residence, place of work or place of the alleged infringement or to take legal action shall remain unaffected.

Part Six
Final Provisions

§ 45 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 regulatory environment, 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 Protection 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 and practices 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.

(5) The companies transferring personal data in third countries monitor, on an ongoing basis, and where appropriate in collaboration with the recipients, developments in the respective third countries that could affect existing transfer impact assessments and compliance with these Binding Corporate Rules Privacy.

§ 46 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 upon request. Once a year, the competent supervisory authority receives an up-to-date list of the companies that have introduced the Binding Corporate Rules Privacy in a binding manner.

§ 47 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.

§ 48 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

Anonymisation

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 the natural or legal person, which determines the purposes and means of the processing of personal data.

Data subject

shall mean any identified or identifiable 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.

European Economic Area

consists of the Member States of the European Union and three countries of the European Free Trade Association (Iceland, Liechtenstein and Norway; excluding Switzerland).

Group Holding

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

Onward Transfer

shall mean the transfer of personal data from a third country to another third country.

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.

Pseudonymisation

shall mean the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Processing

shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor

shall mean a company which processes personal data on behalf of the controller.

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 genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation of a natural person.

Third party

shall mean a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.