NATIONAL GROUP POLICY ORGANIZATION OF DATA PROTECTION

ASSUMPTION OF RESPONSIBILITY FOR DATA PROCESSING

Deutsche Telekom AG, Group Privacy

Version	2.1
Last revised	January 02, 2019
Status	Final

Internal

PUBLICATION DETAILS

Published by

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

Title	Version	Scope
National Group Policy Organization of Data Protection	2.1	Germany

Author	Approved by	Contact
Dr. Jörg Friedrichs, GPR STS-1 Christina Kreft-Spallek, GPR STS-10	Dr. Claus Ulmer, Head of GPR	Christina Kreft-Spallek, GPR STS-10

Status and last revised	Validity	Location of document
Final version January 02, 2019	Within Deutsche Telekom AG, as per the Board of Management resolution of November 17, 2015, effective March 1, 2016. At the German Group companies, as per board resolution or decision of the responsible board member	DTAG Policies Database (http://policies.telekom.de)

Summary

This national Group Policy defines the governance and implementation functions regarding data protection in the Group companies. It implements roles relating to the assumption of responsibility for data processing in the Group companies located in Germany.

CHANGE HISTORY

Version	Last revised	Edited by	Changes/comments
1.0	Sept. 21, 2001	Alexandra Abach	Final version
2.0	Aug. 21, 2015	Jörg Friedrichs, Christina Kreft-Spallek	Final version
2.0	Dec. 13, 2015	Jörg Friedrichs Christina Kreft-Spallek	Editorial amendments Part 3 Implementation functions
2.1	Jan. 02, 2019	Christina Kreft-Spallek	Editorial amendments due to Group Security Policy 1.0, General Data Protection Regulation 2016/679 and amendments of the Binding Corporate Rules Privacy

Note: The current version of the document in the Group's Policies Database shall apply (http://policies.telekom.de).

TABLE OF CONTENTS

1 GENERAL INFORMATION

1.1 Framework regulations

The obligations for data protection and the processing of personal data within the Deutsche Telekom's Group companies in Germany arise, out of various statutory and legal provisions, which apply to all Group companies in Germany irrespective of their business mission.

Provisions relevant under data protection law governing the processing of employees' personal data may arise from the collectively agreed regulations applicable to the Group companies included in works agreements and collective agreements.

The Group is also committed to other measures to protect the personal data of customers, employees and shareholders. These give rise to the following additional requirements:

- Implementation of the Binding Corporate Rules Privacy (BCRP)
- Increase in data privacy awareness
- Internal Control System (ICS) checks on data privacy
- Privacy Security Assessment (PSA process)
- Service provision for the Group customers in line with data protection provisions
- Implementation of the Group Data Privacy Officer's data protection requirements.

1.2 Objective

This Group Policy aims to meet the statutory requirements governing data protection, the implementation of the Binding Corporate Rules Privacy (BCRP) and the achievement of a Group-wide uniform, high level of data protection within the Deutsche Telekom's national Group companies.
The Group Data Privacy Officer carries out a regulatory and supervisory function (Chapter 2) to achieve this objective.
It is the Group companies' Board of Management duty to set up the roles described in Chapter 3 and to ensure the associated duties are carried out.
To this end, clear, transparent definitions of roles with rights and obligations and a chronological documentation of responsibilities in the Group companies' business processes are being introduced.

1.3 Addressees and scope and implementation of this national Group Policy

This national Group Policy shall apply to the Deutsche Telekom Group in Germany to the extent that the responsible management body or responsible member of the Board has approved or decided the validity of this national Group Policy.

It is aimed at the responsible management body or responsible member of the Board as well as the companies' position holders and data privacy coordinators described in this Group Policy.

When implementing this national Group Policy, the precedence of German law and the existing collectively agreed regulations and participation rights of the responsible employee representatives shall be observed.

2 GOVERNANCE FUNCTIONS

2.1 The Group Data Privacy Officer

The Group Data Privacy Officer, as head of Group Privacy, carries out the function of data protection officer within the meaning of the Binding Corporate Rules Privacy (BCRP) and the statutory provisions on data protection, and fulfills the associated duties in Deutsche Telekom's Group companies in Germany. The Group Data Privacy Officer supervises the national Group companies directly in questions relating to data protection and works Group-wide toward achieving a suitable level of data protection in the Deutsche Telekom Group. The Group Data Privacy Officer reports directly to the managing board of Group companies.
The Group Data Privacy Officer defines the Group's strategic alignment in data protection matters and represents the Group in all data protection matters both internally and externally.

In all questions relating to data protection, the Group Data Privacy Officer shall be entitled to exercise his/her right of subrogation at any time.

2.1.1 Requirements

The Group Data Privacy Officer works toward compliance with the applicable statutory data protection regulations within the Group companies. In particular, the Group Data Privacy Officer stipulates and complies with data protection requirements, as well as putting in place the prerequisites for operating systems in line with the data protection requirements, as well as for products and business models that comply with data protection requirements.

2.1.2 Consulting with regard to data protection law

The Group Data Privacy Officer is responsible for advising Group companies with regard to data protection law.
This applies in particular to the implementation of statutory and in-house data protection requirements, with regard to the structuring of processes as well as review and approval processes for business models, products and systems.
All employees and customers may turn to the Group Data Privacy Officer with complaints at any time, within the Group Data Privacy Officer's function as data protection officer of the Group companies in Germany within the meaning of the Binding Corporate Rules Privacy (BCRP).

2.1.3 Carrying out data privacy checks

The Group Data Privacy Officer is responsible for monitoring the proper usage of data processing procedures that are used to process personal data. To this end, the Group Data Privacy Officer may carry out relevant privacy checks, recommend any resulting measures and insist on their implementation.

2.1.4 Commitment to data and telecommunications secrecy, training and awareness

The Group Data Privacy Officer shall identify the statutory and group internal requirements regarding the obligations of employees to comply with data and telecommunications secrecy. The Group companies receive standard instructions for the fulfillment of these requirements. Suitable measures are adopted to inform employees regularly about the content of this obligation and the importance of data protection in the company, and to raise awareness of data protection. Instructions and tools (text modules and document templates) for different employment contracts are provided. The Group companies are advised and supported on how to implement the obligation on employees. The functional requirements regarding training measures are drawn up.

2.1.5 Interface to data protection supervisory authorities

The Group Data Privacy Officer constitutes the interface to the data protection supervisory authorities. In individual cases the Group Data Privacy Officer may request support from the Group companies or approve direct interaction.

2.1.6 Duty to furnish information in the case of data privacy incidents

The Group Data Privacy Officer shall ensure that suitably detected incidents and suspected cases regarding data privacy infringements can be submitted at any time to Group Privacy for review and assessment in order to fulfill statutory and in-house requirements. To this end, the Group Data Privacy Officer shall provide suitable special-purpose mail accounts or other contact details.

In addition, the Group companies are advised and supported with structuring relevant reporting paths and information channels to identify potential incidents and suspected cases.

2.1.7 Appointment of data privacy coordinators

The Group Data Privacy Officer appoints data privacy coordinators in the Group companies in Germany to support the performance of his or her duties as data protection officer of the Group companies.

Within the intended scope of this Policy, one data privacy coordinator shall always be appointed in the Group companies for each 1,000 employees. If the Group company has more than 1,000 employees, additional data privacy coordinators are set up for each center, company, OZT (org. unit reference no.) or in accordance with the organization and size of the respective Group company. Here too the rule of thumb applies of 1 per 1,000. In the case of Group companies with fewer than 1,000 employees, a data privacy coordinator shall always be set up if the Group companies are responsible for a separate business segment.

Furthermore, in the case of Group companies and units with fewer than 1,000 employees, the Group Data Privacy Officer may, together with the respective operational data privacy bridgehead as per Chapter 4 section 8, decide whether the units are merged and supervised jointly across the board by a single data privacy coordinator.

The Group company's operational data privacy bridgehead shall propose suitable employees for this function; the Group Data Privacy Officer may reject the appointment in justified exceptional cases. In this case, another data privacy coordinator from the relevant unit shall be suggested to the Group Data Privacy Officer.

If a data privacy coordinator can no longer carry out his or her task, the Group Data Privacy Officer officially discharges the employee from his or her function. In this case, a new data privacy coordinator shall be appointed.

The Group Data Privacy Officer arranges at regular intervals, once a year as a minimum, a joint meeting of the data privacy coordinators as an overarching information event. An induction event is offered, where required, for newly appointed data privacy coordinators in order to familiarize them with the fundamentals of data privacy and their function.

Steps shall be taken to enable data privacy coordinators to take part in these information events and the recommended training. Travel expenses incurred by the data privacy coordinators are assumed by the data privacy coordinator's respective cost-center owners.

2.2 The data privacy coordinators

The data privacy coordinators support the Group Data Privacy Officer with carrying out his or her duties. They are supervised by the Group Data Privacy Officer functionally in this respect and are subject to the functional instructions of the Group Data Privacy Officer when carrying out their data privacy coordinator duties.

The Group Data Privacy Officer or an authorized representative officially appoints an employee as the data privacy coordinator by handing over an appointment document. At the request of the data privacy coordinator, the Group Data Privacy Officer informs the respective line manager in writing about the employee's appointment as the data privacy coordinator. To this end, the Group Data Privacy Officer shall be notified about the respective line manager and the supervised unit.

The employer's right to give instructions remains unaffected. The Group Data Privacy Officer informs the data privacy coordinators about the fundamentals and current developments in the area of data protection. Moreover,

the data privacy coordinators should take part in data privacy training (e.g., fundamentals of data protection) and always be able to consult information on the Group Privacy intranet sites.

An employee may be appointed as data privacy coordinator if his or her main duty is to carry out highlighted activities independently under his or her own responsibility for complex areas of responsibility or difficult coordination duties.

0.1 FTE should be envisaged on average as the time required for acting as a data privacy coordinator.

The data privacy coordinator returns the document issued to him or her to the Group Data Privacy Officer upon termination of his or her activity.

2.2.1 General support services

The data privacy coordinators support the Group Data Privacy Officer and the operational data privacy bridgehead with implementing the data privacy requirements, the employees' obligations to comply with data and telecommunications secrecy, the carrying out of company training courses relating to the protection of employee and customer data, and the carrying out of privacy ICS checks, where applicable.

They also support the Group Data Privacy Officer in determining the facts with regard to matters and complaints pertaining to data privacy law.

The data privacy coordinators are on hand to employees in their sphere of responsibility as the first point of contact with queries relevant to data privacy. In the case of lack of clarity or uncertainty, they provide the contact to the Group Data Privacy Officer or the operational data privacy bridgehead.

2.2.2 Disclosure duty in the case of data privacy violations

The data privacy coordinators shall inform the Group Data Privacy Officer directly in accordance with the established reporting processes as soon as the suspicion of a data privacy infringement exists and provide support in clarifying the facts.

2.2.3 Coordination duties during execution of the Group data privacy audit

The data privacy coordinators carry out coordination duties during execution of the Group data privacy audit and are on hand as the point of contact. Moreover the Group Data Privacy Officer may ask them to carry out random checks on the audit results. They are informed beforehand about the audit results and are asked to present these in their sphere of responsibility and to discuss improvement measures with their managers.

2.2.4 Employee complaints

Following suitable training, data privacy coordinators are entitled to review employee complaints and to advise employees with regard to their rights. In this respect they are obliged to keep confidential the identity of the person making the complaint, unless the latter exempts them from this obligation in writing. In the case of doubt, the Group Data Privacy Officer shall be involved in the process. If relevant training was not completed, the task is restricted to establishing contact with the Group Data Privacy Officer.

2.2.5 Random samples and right of inspection

To verify compliance with data protection regulations, data privacy coordinators may take random samples following prior consultation with the Group Data Privacy Officer in compliance with codetermination and data protection law provisions. If they require in this respect access to information, hardware and software components used to process personal information or information that can be associated with a specific individual, this shall be granted to them on the instruction of the Group Privacy officer or the operational data privacy bridgehead (e.g., as part of privacy ICS checks) for the specific individual case. Similarly, the information and documents required in this respect shall be handed over to them.

3 IMPLEMENTATION FUNCTIONS

3.1 The Group Company

The Group Company assumes responsibility for data processing in accordance with the statutory provisions governing data protection and the Binding Corporate Rules Privacy (BCRP) for all systems, products and business models, which it operates or has third parties operate for it to carry out its business processes.

This is done by identifying all data-processing business processes and by the managing board of the Group company cascading responsibility for data processing for every IT/NT system operated by or operated on behalf of the Group company as part of these business processes to the roles described in this Policy.

3.2 The managing board of the Group company

There is a direct reporting path between the Group Data Privacy Officer and the managing board.

The managing board shall ensure that local structures governing data privacy are in place in the respective Group company and its majority holdings. It shall also ensure that responsibility is clearly assigned for data processing in accordance with the applicable statutory provisions and in-house regulations, especially the works agreements and collective agreements for each IT/NT system operated to support the business processes as illustrated below:

- Functional unit data controller,
- Functional system owner,
- Technical system owner.

All role holders shall be informed about the rights and obligations associated with their task. These arise out of this Policy and the arrangements set out in the Group Security Policy[1].

The responsibility associated with the particular role shall be documented in a transparent, clear manner in the business missions.

The managing board is also responsible for ensuring that the function of an operational data privacy bridgehead is implemented for the Group company, insofar as it acts as a business unit, and its majority holdings. The operational data privacy bridgehead supports the Group company and its majority holdings with implementing the Group Data Privacy Officer's data privacy requirements and with conducting internal and external checks on the level of data privacy in the data-processing business processes.

[1] See also Group Security Control Set 3.1

3.3 Roles regarding the assumption of responsibility for data processing[2]

3.3.1 The functional unit data controller

The managing board appoints for each business segment a functional unit data controller on the nearest reporting level.[3]

The functional unit data controllers are responsible for compliance of the Group company's obligations under data protection law for the IT/NT systems for which they are responsible in the business segment for the respective reporting level.

There shall be a direct reporting path between the functional unit data controller and the managing board.

The functional unit data controller informs the managing board at regular intervals, once a year as a minimum, or as and when necessary about the assumption of responsibility for data processing in his or her business segment.

The functional unit data controller engages in text form (e.g., e-mail) a functional system owner in accordance with the Group Security Policy[4] for each IT/NT system for which responsibility exists in the business segment.

The functional system owner is responsible at operational level for the data privacy conformity of the respective IT/NT system.

This obligation shall be updated in the event of personnel or organizational changes or, if required, in the event of technical changes. Any changes to the functional system responsibility shall be documented chronologically for each IT/NT system within the functional unit data controller's sphere of responsibility.

If an in-house functional service provider (contractor chain) is placed upstream of a technical IT service provider when processing personal data in an IT/NT system within the functional data owner's sphere of responsibility, the functional system owner's role and duties may be delegated by the functional unit data controller contractually to the functional service provider along the lines of responsibility for organizational implementation.

The functional unit data controller shall guarantee that the functional system owners fulfill their duties properly.

The functional unit data controller shall ensure that the functional system owner attends the trainings provided by the Group Data Privacy Officer.

3.3.2 The functional system owner

The functional system owner supports the functional unit data controller with the assumption of responsibility for data processing for the IT/NT system whereby the functional unit data owner engaged the functional system owner in text form to provide operational supervision. As part of this task, the functional system owner shall follow the functional unit data controller's instructions.

The functional system owner is operationally responsible for data privacy conformity of the IT/NT system supervised by him or her as well as for ensuring regular, demonstrable auditing of the congruence (consistency) of the Standardized Data Privacy and Security Concept with the works agreement applicable to the IT/NT system. This applies to any change or new introduction of the IT/NT system supervised by him or her.

---

[2] Role model assumption of responsibility for data processing Version 1.0 see Annex

[3] In individual cases (e.g., with DTAG GHS or smaller companies) the data owner may also be appointed on reporting level 2 – starting from the managing board – in consultation with the Group Data Privacy Officer. In these cases, the data owner reports to the respective head of reporting level 1, who in turn reports to the managing board.

[4] The Group Security Policy as amended shall apply.

The functional system owner shall ensure that a technical system owner is appointed for the IT/NT system.

The functional system owner shall clarify the respective system-relevant assignment of roles and duties with the technical system owner in accordance with the Group Security Policy.

There is a direct reporting path between the functional system owner and the technical system owner.
The functional system owner shall check to a reasonable extent that the technical system owner is carrying out the duties properly.

In the case of IT/NT systems with demonstrable low criticality documented in writing, the roles of the technical and functional system owner may be combined.

Further details on the duties of the functional system owner are set out in the Group Security Policy.

3.3.3 The technical system owner

The technical system owner shall clarify the respective system-relevant assignment of roles and duties with the functional system owner in accordance with the Group Security Policy. The duties of the technical system owner can be found in the Group Security Policy.

The technical system owner and the functional system owner shall share information at regular intervals on current developments in their unit and agree further measures.

4 THE OPERATIONAL DATA PRIVACY BRIDGEHEAD

The managing board shall ensure that the function of the operational data privacy bridgehead is carried out for the Group company and its majority holdings.

The selection of the operational data privacy bridgehead shall be coordinated with the Group Data Privacy Officer taking into account the specialist qualifications. Steps shall be taken to ensure that the operational data privacy bridgehead has adequate decision-making power as well as personnel and material resources in order to fulfill the duties assigned to him or her.

The managing board may delegate to the operational data privacy bridgehead individual duties or partial duties under their responsibilities as part of the existing authority to give instructions. The responsibility remains unaffected, however. The Group Data Privacy Officer shall be notified in this respect.

The operational data privacy bridgehead is responsible for implementing privacy governance in the Group company and the majority holdings assigned to it and for implementing the duties listed below.

4.1 Support for the managing board

The operational data privacy bridgehead supports the managing board with cascading the data responsibility by appointing the functional unit data controllers.

4.2 Support for the functional unit data controller

The operational data privacy bridgehead supports the functional unit data controllers with assuming data responsibility within their sphere of responsibility.

4.3 Implementation of data protection requirements

The operational data privacy bridgehead works toward uniform operational implementation of the Group Data Privacy Officer's data protection requirements. In this respect, the operational data privacy bridgehead may also impose separate enterprise-specific implementation requirements as part of the Group Data Privacy Officer's requirements.

4.4 Records of processing activities

The operational data privacy bridgehead provides up-to-date records of processing activities in accordance with the Group Data Privacy Officer's requirements for the Group company supervised in each case. In this respect, the Group Data Privacy Officer provides the operational data privacy bridgehead with methodology support.

4.5 Internal and external checks on the level of data privacy

The operational data privacy bridgehead supports the conducting of internal and external checks and the taking of necessary measures where vulnerabilities are found. The operational data privacy bridgehead is the central point of contact and conducts the privacy ICS checks including documentation in consultation and coordination with the responsible data privacy coordinators and departments.

4.6 Commissioned data processing

The operational data privacy bridgehead works in relation to the conclusion of commissioned data processing contracts within the meaning of the Binding Corporate Rules Privacy (BCRP) toward ensuring that relevant documents (contracts and audit evidence) are managed systematically and demand-based access (including reporting) to such documentation is possible. To this end a suitable process shall be introduced with the functional support of the Group Data Privacy Officer.

4.7 Disclosure duty in the case of data privacy violations

The operational data privacy bridgehead shall inform the Group Data Privacy Officer as soon as he or she becomes aware of data privacy incidents.

4.8 Proposal from data privacy coordinators for the appointment by the Group Data Privacy Officer

The operational data privacy bridgehead is responsible for updating and providing an overview of data privacy coordinators in the respective unit. The operational data privacy bridgehead proposes to the Group Data Privacy Officer suitable employees for appointment as data privacy coordinator and ensures in collaboration with the Group Data Privacy Officer that no vacancies occur.

5 MISCONDUCT

Culpable, willful misconduct shall be punished in accordance with the applicable provisions of the law and in-house provisions.

6 REVIEW OF THIS NATIONAL GROUP POLICY

The Group Data Privacy Officer checks and amends as required the provisions of this national Group Policy on an annual basis.

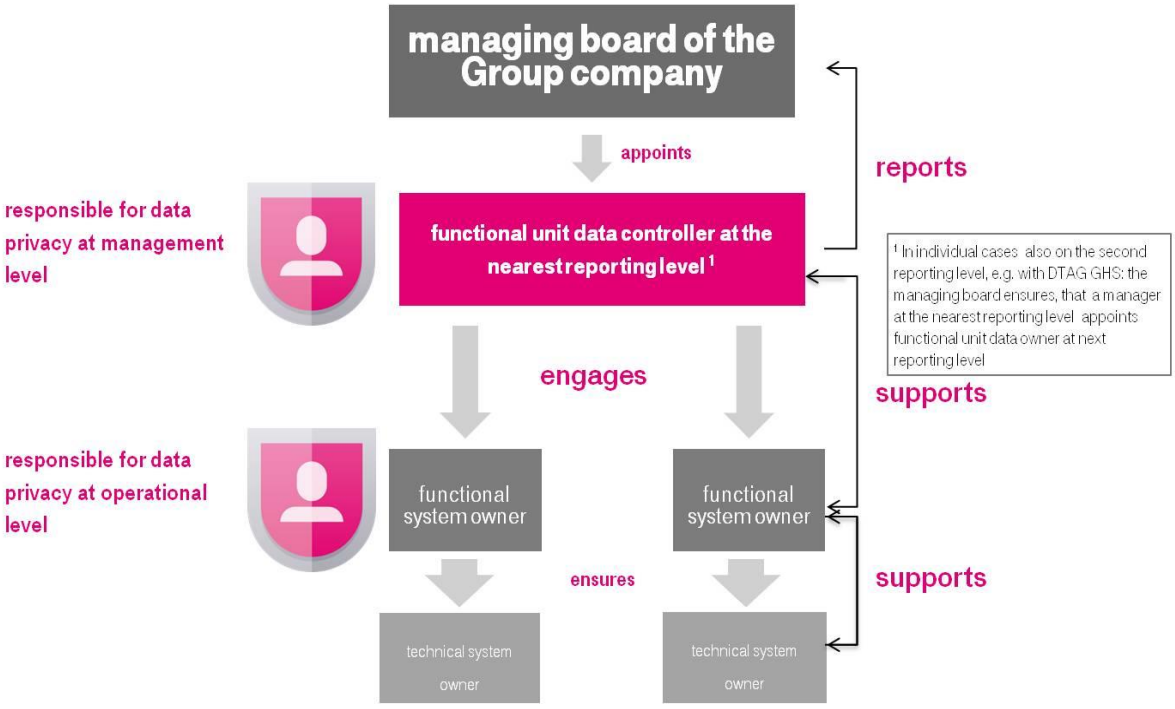
7 ENTRY INTO FORCE

Following approval by the Board of Management of Deutsche Telekom AG on November 17, 2015, this Group Policy shall become valid on March 1, 2016 for Deutsche Telekom AG and shall replace the Group Policy on the Organization of Local Data Privacy dated September 21, 2009. For the Group companies in Germany, the national Group Policy shall enter into force as per the resolution adopted by the competent management body or by the responsible member of management.

8 ANNEX

8.1 Other applicable documents

The Group Security Policy as amended.
Binding Corporate Rules Privacy (BCRP) as amended.



8.2 Figures

Role model 'Assumption of Responsibility for Data Processing' Version 1.0