Guideline

Guideline on the Implementation of Technical and Organizational Data Protection Measures

Deutsche Telekom Gruppe

Version	5.0
Last revised	20.11.2015
Status	final

Internal

Erleben, was verbindet.

Table of contents

1 Introduction and objectives

When information and communications technology are used in company practice, technical security data protection measures and IT security are often summarized and implemented conceptually. Whereas IT security is risk-oriented, data protection is based on existing legal provisions for protecting personal data. IT security must take into consideration additional threat scenarios beyond the possible violation of data protection, although this is not the focus for data protection officers who are always concerned with personal data. The various procedures complement each other, since IT security is incomplete unless data protection is explicitly considered in terms of legal and corporate policy requirements.

The annex to § 9 BDSG specifies the organizational and technical measures to be taken from a data protection perspective in abstract terms. The following requirements document is intended to explain to persons in the Deutsche Telekom AG Group who are involved in implementing the data protection requirements which measures are obligatory, and which are optional. To this extent, this document adds detail the statutory requirements.

The requirements presented here are specified depending on the project in the Operating Model Privacy and Security Assessment. If supplementary requirements are necessary with special business models, they are defined by GRP in individual cases and shall be considered to be binding.

1.1 Technical and organizational measures

Data protection requirements are described methodically in the annex to § 9, sentence 1, BDSG, “Technical and organizational measures.” The requirements formulated there are subsumed under the following terms:

1) Admittance control
2) System access control
3) Data access control
4) Disclosure control
5) Input control
6) Job control
7) Availability control
8) Intended use control
9) Organizational control

As the eighth item in the requirements catalog, it “must be ensured that data collected for different purposes can be processed separately.” This requirement is referred to below by the term “Intended use control.”
"Organizational control" refers to general measures for ensuring an appropriate level of data protection which implicitly results from § 9 of the BDSG itself and from an overview of the individual measures according to the Annex to § 9 of the BDSG. This includes, for example, the obligation of an employee involved in data processing work to observe data protection training beyond the general data protection obligation.

1.2 Structure of the document

The document is divided into the nine above-mentioned categories. First there is a quote from the BDSG – if available – and this is followed by an explanation in the continuous text.

Req n	The document defines consecutively numbered requirements that are mandatory for all of the nine above categories. They are highlighted in the following format.

The requirement is followed by another explanation in the continuous text.

Implementation proposals
Alternative or complementary implementation proposals are provided for most requirements. These are specifically described technical or organizational solutions for fulfilling the requirement.

1.3 Summary

Scope	Target group	Information	Standardization	Regulation type
Germany	Deutsche Telekom employees	Guideline on the Implementation of Technical and Organizational Data Protection Measures	Based on the BDSG	Guideline

2 Admittance control

Annex to § 9, sentence 1, of the Federal Data Protection Act [Bundesdatenschutzgesetz, BDSG] states the following: "... to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data" (admittance control).
The term "admittance" refers to the physical access by individuals to buildings and facilities in which IT systems are operated and used. These include computer centers where web servers, application servers, databases, mainframes and storage systems are operated and office space where employees use desktop computers. This also includes the facilities where network components and network cables are located and laid.

2.1 Basic requirements

Req 100	Definition of security areas

The security requirements of a building or room shall be determined on the basis of the data processing systems located therein and any other documents on which personal data is processed or stored.

Req 101	Implementation of effective admittance protection procedures

Suitable technical measures (e.g., special glazing, intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organizational measures (e.g., security guard) shall be taken to safeguard security areas and their admittance points against entry by unauthorized persons.

Implementation proposal: fenced area
The premises can be secured by walls or fences, meaning that the premises can only be accessed through defined access points. The building or part of the building must usually be accessed before access can be gained to individual facilities in which data processing systems are located. Monitoring and authorization

functions must be implemented at this point at the latest to prevent unauthorized access. Within the building, access to the individual IT operation rooms must also be regulated according to the minimum principle.

Implementation proposal: secure entrances and exits
Entrances and exits must either be monitored or else only be accessible using keys, electronic cards or other locking systems. Emergency exits and escape routes are exceptions to this rule. They must be protected by alarm systems. The alarms must be forwarded to a control center that immediately determines the cause of the alarm.

Implementation proposal: access via PIN
If access is controlled exclusively or additionally by entering a PIN, then the PIN must be changed regularly and the group of persons who are aware of the PIN must be restricted according to the need-to-know principle. Easy-to-guess sequences such as 1234, 4711, etc. must not be used as PINs. If technically feasible, the PIN must contain at least 5 digits.

Req 102	Admittance logging

Admittance to facilities in which personal data is processed should, if possible, be logged. The retention period for logs depends on the rules agreed with employees' representatives. In the absence of such rules, the retention period is 3 months. Suitable procedures shall be agreed with the employees' representatives and the data privacy team in order to identify improper use and carry out incident-related evaluations.

Req 104	Specification of persons with admittance authorization

The requirements for and the group of persons with general admittance authorization must be defined and the authorizations for admittance to security-relevant areas limited to absolute necessity ("principle of minimal authorization"). Admittance shall be denied to anyone without authorization. Means of admittance to buildings or premises must only be issued to specific persons and may not be passed on to third parties. Users shall be made aware of this.

Implementation proposal: definition of authorization groups
Authorizations can be defined by assigning users to certain groups. In addition to defining user groups within employees, authorization groups must also be defined for external companies, consultants, visitors and maintenance or cleaning companies.

Req 105	Management and documentation of individual admittance authorizations throughout the entire life cycle

A process shall be established for requesting, approving, issuing, managing and accepting the return of means of admittance or for withdrawing admittance rights (including management of keys, visual IDs, transponders, chip cards, etc.); this process shall be described and implemented. Rules and procedures for blocking admittance authorizations shall be described. If an individual leaves the company or moves to a different department, all means of admittance and admittance authorizations for all premises that are no longer necessary for the performance of that person's duties shall be immediately returned/revoked. All persons entrusted with security duties, in particular security gate duty, shall be notified of employees who have left the company or whose duties have changed.

Implementation proposal: visual IDs
Visual IDs are issued for all persons with admittance authorization, which they can use to legitimately identify themselves in the building.

Implementation proposal: centralized administration of keys
All keys for a building must be managed centrally for the respective building. For each key that is issued, the person who received the key and the date when the key was issued must be documented as a minimum. The recipient confirms in writing having receiving the key. This can be documented and archived in a database or on paper. The issue and withdrawal of access means and authorizations must be archived in a tamper-proof manner for at least 3 months. The process must ensure that employees who leave the company return any keys issued.

Implementation proposal: administration of electronic access authorizations
Access via an electronic locking system can usually be managed considerably more efficiently, since authorizations are generally logged in the system. Ideally, there would be a link to central systems (such as central identity and account management systems) that can provide information about employees leaving or relocating so that actions such as blocking access authorization can be carried out automatically or semi-automatically.

Req 106 Accompanying visitors and external personnel

Written rules must exist governing the admittance of people external to the company, such as guests and suppliers. At the minimum, these rules shall require that people external to the company be able to prove at all times that they are authorized to be in the building, e.g., through a guest pass, visitor's pass or supplier ID. The person's name and origin (employer, business or home address) must be logged. A random check of authorizations to be in the building is obligatory. If there is a need for enhanced protection (protection class 3 or higher), non-company personnel shall be accompanied and supervised during the performance of their work.

Implementation proposal: regulations for cleaning staff/cleaning companies
Whether it is possible for the premises to be cleaned during regular business hours, and therefore under supervision, must be ascertained. If they are cleaned outside of regular business hours, appropriate regulations (such as requirements for cleaning staff) must be agreed.

Implementation proposal: regulations for external on-site maintenance personnel
On-site maintenance work that is performed by external staff must be carried out in such a way that only the commissioned work is possible. This can be achieved through monitoring, or by precisely logging/recording the activities. In any case, access must be granted only temporarily, and only to the rooms and the server cabinets, for example, where access is necessary.

Req 107 Monitoring rooms outside of business hours

The building or facilities that house IT systems on which personal data or data that can be associated with a person is processed and/or stored shall be monitored outside regular business hours.

Implementation proposal: patrols
Authorized security personnel can monitor the premises by performing regular patrols.

Implementation proposal: electronic monitoring
Monitoring may also take the form of video monitoring or motion sensors. Both must be connected to a control room.

3 System access control

Annex to § 9, sentence 1, of the Federal Data Protection Act states the following: "...to prevent data processing systems from being used without authorization (access control)...".
In addition to admittance control, the aim of access control is to prevent unauthorized persons from using data processing systems in which personal data is stored, processed or used.

3.1 Basic requirements

Req 201	Definition of the protection requirement

The protection level of the IT process must be defined and depends on the criticality of the data processed in the IT process and the risk associated with unauthorized access. If data from data protection level 3 or higher can be accessed after the access control, then a high protection requirement applies. Otherwise, a protection requirement of low to medium should be assumed.

Req 202	Access protection (authentication)

Access to data processing systems on which data is processed shall be possible only after the authorized person has been identified and successfully authenticated (e.g., with a user name and password or chip card/PIN), using state-of-the-art security measures. Access shall be denied to anyone without authorization.
For low to medium data protection needs, simple access mechanisms such as user name and password are permitted alongside a few additional requirements. For high data protection needs, more extensive authentication (e.g. by means of chip cards/certificates and PIN) is required.

Req 203	Implementation of secure access procedures (strong authentication) for protection level "very high"

Strong authentication is always based on multiple (at least two) factors, such as something owned, something known, or on the basis of a unique factor that is specific to the user (usually biometric processes).

Implementation proposal: chip card with certificates and a PIN
In the Deutsche Telekom Group, smart cards (TIKS cards/MyCard) with certificates can be used for authentication. The cards with certificates and PIN entry are a strong form of authentication.

Implementation proposal: one-time passwords (OTP) + device
Robust authentication is also possible using one-time passwords that are transmitted to a particular device if necessary (e.g. to a cell phone), or that are created by a device when a PIN is entered (SecurID card, OTP on TIKS card, OTP generator software on MDAs, etc.).

Implementation proposal: use of biometric procedures
Biometric procedures such as voice recognition, iris scans, thumb prints and similar are secure authentication processes if they are set up correctly. However, broad use of these technologies is not currently advisable, since not all technologies are reliable and, furthermore, there are considerable problems due to the need to store personal information. Deployment makes most sense wherever voice recognition systems (IVR - Interactive Voice Recognition) are used, such as call centers/help desks. This is where voice-based authentication is most likely to make sense.

Implementation proposal: indirect login (e.g., Kerberos)
If an IT process performs indirect authentication against a central directory service such as the Active Directory using the Kerberos protocol, for example, then the data protection level corresponds to the level of the

registration at the central directory/authentication service. This process only makes sense for a high data protection level if the registration was converted to chip card registration at the Active Directory.

Req 204	Implementation of simple authentication via a user name/password (up to the 'medium' protection level)

Passwords must comply with appropriate minimum rules, such as a minimum password length and complexity. Passwords have to be changed at regular intervals. Initial passwords must be changed immediately.

Implementation proposal: indirect login (e.g., Kerberos)

- If an IT process performs indirect authentication against a central directory service such as the Active Directory using the Kerberos protocol, for example, then the data protection level corresponds to the level of the registration at the central directory/authentication service. This process is currently adequate for low and medium data protection levels, since the registration on the Active Directory is currently based on a user name and password. The advantage of this is that the following password rules are already implemented in the Active Directory and can therefore be ignored.

Implementation proposal: separate user and password management

- The passwords and processes must at least satisfy the requirements of the currently applicable Group policies.
- The implementation of/compliance with the requirements for password length, password complexity and validity must be ensured by technical settings, if possible.
- The password should not be visible in plain text on the screen when it is being entered.
- The initial password must be provided to the user through secure channels and/or the user must at least be prompted to change the password immediately after logging in for the first time.

Req 205	Logging access

All successful and rejected access attempts must be logged (user ID, computer, IP address used) and archived in an audit-compliant form. The retention period for logs depends on the rules agreed with employees' representatives. In the absence of such rules, the retention period is 3 months. To detect improper use, regular evaluations through sampling shall be carried out.

Req 206	Secure transmission of authentication credentials in the network

The authentication credentials (such as user ID and password) must never be transmitted unprotected over the network.

Implementation proposal: encrypting the transmission links

Between IT systems, for example from the client to the server, the credentials have to be protected from unauthorized interception by means of encryption procedures.
Examples include:

- Secure Socket Layer/Transport Layer Security (SSL/TLS) in conjunction with valid certificates in web applications (also known as https)
- Secure Shell in the administrative field
- Secure Network Communication (SNC) for communication between SAP GUI, PAS and AAS
- Secure FTP (SFTP)
- IPSec

Implementation proposal: use of challenge response processes

With challenge response processes, the actual authentication credentials are never transmitted. Rather, they are used to code a sequence (challenge) that is randomly sent by the server, so that the server can determine the

ownership of the credentials based on the correct coding. Since a new challenge is sent with each authentication process, the authentication may be intercepted by an attacker and so cannot be used again for registration.

Req 207 Blocking passwords on failed attempts/inactivity and process for resetting blocked access IDs

Access must be blocked after repeated incorrect authentication attempts. A process shall be established for resetting or unlocking blocked access IDs; this process shall be described and implemented. User IDs that are not used for a long period of time (a maximum of 180 days) must be automatically blocked or set to inactive.

Implementation proposal: resetting after authentication with the help desk
A block can be removed by special request, for example, and after the corresponding user has been authenticated (e.g. meeting with the administrator). Ensure that when the password is reset, you do not set passwords that are simple, always the same, or easy to guess.

Implementation proposal: automated reset
If it can be ensured that no brute force attacks are possible on the access credentials, then automated mechanisms can be used. If necessary, the password can be automatically unblocked over night or after a certain period of time. The blocked user must be informed of this, however, so that he or she can note any possible misuse.

Req 208 Banning storage of passwords and/or form input (server/clients)

Access passwords and/or form input shall not be stored unencrypted or unprotected on the client itself or in its vicinity (such as storage in the browser, unencrypted password tables, post-it notes etc.). Users shall be made aware of this.

Implementation proposal: deactivation of storage of passwords and/or form input
If the operating system or the application (e.g. the browser) provides the option of saving passwords and/or form input unencrypted, then the use of this function must be technically prevented.

Implementation proposal: no storage of passwords in plain text
Access passwords must be saved securely in the system and must not be stored in plain text.

Req 209 Identification of authorized individuals

The group of people authorized to access data processing systems on or with which data is processed and/or stored must be limited to the absolute minimum necessary to allow people to perform their specific duties or functions within the ongoing operational organization. Access for people employed temporarily (consultants, interns, trainees) must be assigned on an individual basis. Reusable IDs (such as consultant1, guest1) should not be assigned.

Req 210 Managing and documenting individual authentication media and access authorizations

A process shall be established for requesting, approving, issuing, and accepting the return of authentication media and access authorizations; this process shall be described and implemented. This includes at least a request and approval process as well as a process for accepting the return of authentication media and revoking access authorizations.
Access authorizations must always be assigned only for the data processing systems/types which need to be accessed for performing the person's work ("principle of minimal authorization"). Authentication media and access IDs for accessing data processing systems shall, in principle, be assigned on an individual basis and be linked (user ID) to a personal credential (such as a password, token or chip card). Authentication media and/or

user ID/password combinations must not be passed on to third parties. Users shall be made aware of this. Rules and procedures for blocking access IDs or deleting them in compliance with data protection rules must be described. If an individual leaves the company or moves to a different department, all authentication media and access authorizations for all data processing systems that are no longer necessary for the performance of that person's duties shall be immediately returned/revoked. Steps must be taken to ensure that all parties involved are notified of the fact that employees have left the company or changed jobs (in particular, IT/authorization administrators).

Implementation proposal: connection to central directories (e.g. Active Directory)
An initial measure would be to avoid using separate user management or a separate directory, and instead access existing central directories such as Active Directory. When an employee leaves the company, this at least ensures that access is no longer possible.

Implementation proposal: paper workflow and archiving
A process for managing accounts can be implemented on the basis of a paper workflow. Accounts must be requested in writing and signed by the relevant approvers. Only then may an account be set up. The requests must be stored so that existing and requested accounts can be compared at any time. This comparison should be carried out several times a year if possible depending on the criticality of the application. The withdrawal of accounts must also be documented. This approach is recommended for a smaller number of users as it requires a lot of effort to maintain an overview.

Implementation proposal: electronic workflow
Ideally, there would be a link to central systems (such as central identity and account management systems or electronic ordering systems) that can also provide information about employees leaving or changing tasks so that actions such as blocking accounts can be carried out automatically or semi-automatically. Request and approval processes can be mapped efficiently in these electronic workflow systems and everything can be documented automatically.

3.2 Measures taken at the user's workstation

Req 211	Automatic access blocking

If the workstation or terminal is inactive for more than five minutes, a password-protected screensaver must be activated automatically using mechanisms specific to the operating system.

Req 212	Manual access blocking

When users temporarily leave their workplaces, the workstations and terminals must be protected against unauthorized use (e.g., by manually activating the password-protected screensaver, locking the system via the Task Manager or logging off). Employees shall be made aware of this.

4 Data access control

Annex to §9, sentence 1, of the Federal Data Protection Act states the following: "...to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording" (data access control).
The object of the data access control requirements is to ensure that only authorized persons can access the data which they are authorized to access, and to prevent the data from being manipulated or read by unauthorized persons.

4.1 Basic requirements

Req 301 Creating an authorization concept

An authorization concept (user and administration rights) ensures that access to the data in the system is enabled only to the extent required for the user to complete the relevant task according to the user's internal task distribution and separation of functions. Rules and procedures for creating, changing and deleting authorization profiles and user roles in compliance with data protection rules shall be described therein. The authorization concept must show which job holder may carry out administrative tasks (system, user, operation, transport) and which user groups may perform which activities in the system. Responsibilities are regulated.

Req 302 Implementing data access restrictions

Each access authorization must be linked to a data access authorization, for example by linking it to one or more roles defined in the authorization concept. With the applications and within these applications, each access-authorized person may access only the data that he specifically needs to process the current transaction according to the order and which is configured in his individual authorization profile. To the extent that data of multiple customers is stored in the same database or is processed with the same data processing system, logical access restrictions must be provided which are aimed exclusively at processing the data for the customer concerned (multi-tenancy). The data processing function itself shall be limited to the extent that only the minimum functions needed can be used to process the personal data. Unique features are incorporated into the data processing systems which enable the accessing person to determine that the data processing system is authentic. The person authorized to access the data must also identify and authenticate himself to the data processing system on the basis of unique, verifiable factors, such as using ID reader on the terminals.

Implementation proposal: link authorizations to roles (role based access control - RBAC)
Specific and precise authorizations are linked to defined roles. These are read or write rights to certain records, or initiating certain actions and processes in the IT process, for example.

Implementation proposal: authentication of individual critical transactions using TAN
Another very secure option is to start certain critical transactions within the IT process from a list only after they have been re-authenticated using a TAN (transaction number). This procedure is known in online banking. It ensures that access with the corresponding authorizations does not enable any large-scale or improper use of the IT process.

Implementation proposal: additional authentication of individual transactions using the customer's credentials
Another very secure method is to authorize individual transactions by the customer, for example for IT processes that are used in interaction with the customer. This can be achieved by the customer giving the processor a certificate that is only known to the customer, for example; the processor then uses it to authenticate the individual access. It is even better if the start of a transaction triggers a one-time PIN to be sent to the customer's cell phone, for example. The customer notifies the processor of the PIN, and the processor uses it to authenticate access to the transaction. The advantage of the latter method is that it is a one-time password, and the customer does not have to provide the processor with his credentials. The aim of this method is to ensure that a processor does not gain improper access to transactions using the customer data. These procedures are suitable for customer contact at the point of sale (POS) or in call centers, for example.

Implementation proposal: reducing access to data that is necessary for the transaction
During a transaction, only the data that is required for this transaction may be displayed. This applies above all to search functions. Wildcards may only be used extremely sparingly and the quantity of data to be output must be clearly restricted.

Req 303 Assigning minimum authorizations

The scope of the authorizations shall be limited to the minimum needed to perform the authorized person's duties and functions. Time limits shall be put on access to personal data and authorizations to the extent possible that time limits can be put on certain functions without lowering the data processing quality.

Req 304 Managing and documenting individual data access authorizations

A process must be established for requesting, approving, assigning, revoking and checking data access authorizations; this process must be described and implemented. Rules and procedures for granting/revoking authorizations or assigning user roles must be described. The data access rights must be implemented by the rights management process of the IT system. Authorizations must be linked to a personal user ID and an account. This excludes the use of group IDs/passwords used by multiple people. When granting authorizations or assigning user roles, only the number of data access rights needed for performing the person's duties should be assigned (need-to-know- principle). Steps must be taken to ensure that the separation of functions mapped in the system is not canceled by cumulative authorizations. If an individual leaves the company or moves to a different department, all data access rights for all data processing systems and data storage areas that are no longer necessary for the performance of that person's duties must be immediately revoked. Steps must be taken to ensure that all parties involved are notified of the fact that employees have left the company or changed jobs (in particular, IT/authorization administrators). The documentation must be retained for 3 months.

Implementation proposal: paper workflow and archiving
A process for managing roles/authorizations can be implemented on the basis of a paper workflow, where roles/authorizations must be requested in writing and signed by the relevant approvers. Only then may a role/authorization be set up. The requests must be stored so that existing and requested roles/authorizations can be compared at any time. This comparison is to be carried out several times a year according to the criticality of the application. The withdrawal of the role/authorization must also be documented. This approach is recommended for a smaller number of users as it requires a lot of effort.

Implementation proposal: electronic workflow
Ideally, there would be a link to central systems (such as central identity and account management systems or electronic ordering systems) that can also provide information about employees leaving or changing tasks so that actions such as withdrawing roles/authorizations can be carried out automatically or semi-automatically. Request and approval processes can be mapped efficiently in these electronic workflow systems and everything can be documented automatically.

Req 305 Avoiding the concentration of functions

A concentration of functions shall be avoided in applications as well as the administrative area. The concentration of various roles or access rights in a single person can, in combination, give this person an excessively powerful overall role and raises the possibility of controls being circumvented; this situation shall be avoided. For example, a database administrator who is also a user of the application can manipulate transactions through direct access to the database management system or view data that is not appropriate for his role. This applies, in particular, to logging techniques for access to personal data. The people who administer the logging system and the people whose potentially unauthorized access to the data is to be detected and logged must not be the same people.

Req 306 Logging data access

All read, input, modification and deletion transactions must be logged (user ID, transaction details). The retention period for logs depends on the rules agreed with employees' representatives. In the absence of such rules, the

retention period is 3 months. Suitable procedures shall be agreed with the employees' representatives and the data privacy team in order to identify improper use and carry out incident-related evaluations.

5 Disclosure control

Annex to § 9, sentence 1, of the Federal Data Protection Act states the following: "... to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control)".

5.1 Basic requirements

Req 401	Determining instances/persons authorized to receive/transmit data

The Contractor must agree which bodies/persons are allowed to send which data to whom and the particular transmission path via which this may take place.

Implementation proposal: documentation
At which points transmission is permitted, and in which way, is defined in writing (e.g. in a procedural instruction). This can be achieved using a data-related communication matrix.

Req 402	Checking the lawfulness of transmission to other countries

If data is to be disclosed to persons outside Germany, the legal restrictions shall be checked prior to transfer. In particular, transmission to countries outside the European Union shall only be possible subject to additional conditions (standard EU contract clauses, for example) and not for all classes of data. It must also be noted that access from other countries already represents a transmission. This issue is relevant at the development, testing and operational levels as well as at application/user level.

Req 403	Logging every disclosure or a representative selection

For each IT/NT system in which personal data is transmitted, the transmission must be logged. The form this takes (full description or, for example, description according to type of data/sender and receiver) depends in individual cases on whether the scope of logging is justifiable, who exchanges the data with whom (transmission between two trustworthy instances?) and how the transmission takes place (encrypted/unencrypted). The retention period for logs depends on the rules agreed with employees' representatives. In the absence of such rules, the retention period is 3 months. Suitable procedures shall be agreed with the employees' representatives and the data privacy team in order to identify improper use and carry out incident-related evaluations.

5.2 Transport via networks

Req 404	Secure data transmission between servers and clients

The transmission of personal data between clients and servers in IT networks must generally be encrypted. Exceptions to this are permitted for data classified up to data protection level 2 and only if the transmission takes place within the Deutsche Telekom intranet. Client-server data transmissions may only leave the Deutsche Telekom intranet if they are encrypted.

Implementation proposal: encrypting the transmission links
For example, the transmission between the client and server can be protected as follows:

- Secure Socket Layer/Transport Layer Security (SSL/TLS) in conjunction with valid certificates in web applications (also known as https)
- Secure Shell
- Secure Network Communication (SNC) for communication between SAP GUI, PAS und AAS
- Secure FTP (SFTP)
- IPSec
- VPN-Technologien
- RPC with RC4 encryption option
- SFTP
- SQLNet with Advanced Security Option (ASO)
- Encrypting XML files with XML encryption for SOAP protocols

Req 405 Safeguarding transmission in the back end

If personal data is exchanged between individual systems within the back-end, the way in which the individual connections are protected against unauthorized data access shall be carefully considered. If the data does not leave the secure area of the data center, and if it is not possible for the administrators of the network components, for example, to intercept the data, there is no need to encrypt the transmission link in situations where low or medium levels of protection are required. Data requiring a high level of protection shall be encrypted during transport. Where the data is transmitted over longer distances (for example, to another data center), it is mandatory to encrypt the transport.

Implementation proposal: encrypting the transmission links
For example, the transmission between the client and server can be protected as follows:

- Secure Shell
- Secure FTP (SFTP)
- IPSec
- VPN technologies
- RPC with RC4 encryption option
- SFTP
- SQLNet with Advanced Security Option (ASO)
- Encrypting XML files with XML encryption for SOAP protocols

Req 406 Transmission to external systems

If personal data are transmitted to external systems (outside of Deutsche Telekom), encryption is generally required from data protection class 2 upward.

Implementation proposal: encrypting the transmission links
For example, the transmission between the client and server can be protected as follows:

- Secure shell
- Secure FTP (SFTP)
- IPSec
- VPN-Technologien
- RPC with RC4 encryption option
- SFTP
- SQLNet with Advanced Security Option (ASO)
- Encrypting XML files with XML encryption for SOAP protocols
- E-mail encryption using S/MIME or PGP

5.3 Logical access to systems

Req 407 Minimizing risks through network separation

To lower the risk of personal data that is transmitted between IT systems being read on the network, network segments must be created for these IT systems. Network segmentations of this type can be configured with the aid of switches and routers. Data packets on all levels leave and reach the IT systems in these segments only via defined interfaces where additional transmission control measures can be taken. This segmentation must at least involve separating the front-end and back-end systems. A reasonable segmentation within the back end is also highly recommended.

Implementation proposal: protection of back-end systems
The back-end systems must be located in a separate network segment that is separate from any networks from which access is possible. This applies to use from the Telekom network, for example, as well as to use from partner networks or the Internet. The same also applies to operational network segments (backup, monitoring etc.) and administrative networks.

Implementation proposal: segmentation within the back-end systems
There should also be separation within the back ends. The architecture that makes sense in each case can vary greatly. Generally, the back-end systems of an IT process must be separated from the back-end systems of other IT processes provided no shared resources are used. Even within the IT process's back-end architecture, it makes sense to separate the web server from the application and database servers.

Req 408 Implementing security gateways at the network handover points

The IT/NT systems on which personal data is processed shall be protected against unwanted access or data flows from both the same or other networks by using state-of-the-art measures (usually firewalls). Regardless of whether the firewalls are network/hardware-implemented or whether host-based firewalls are also used, the firewalls must be permanently activated. Steps must be taken to effectively prevent any form of deactivation or circumvention of the functions by the users. The rules must be set up in such a way that all but the necessary communications links are blocked automatically.

Implementation proposal: firewalls, IP filter
The traffic between the network handover points can be realized using simple IP packet filters, depending on the protocols that are used. Starting from the any-any-deny approach, only the required communication relationships should be activated. This applies to all networks, even those networks that are required for administrative or operational reasons. Corresponding firewalls can be used for increased protection or if protocols are used with dynamic port assignments.

Implementation proposal: Network Intrusion Prevention Systems (NIPS)
It makes sense to use network-based intrusion prevention systems together with IP filters. The NIPS analyzes the permitted communication relationships for alleged attack traffic and blocks it. It makes sense to use these systems where data protection requirements are especially high.

Implementation proposal: use of proxies/load balancers with IP filters
The use of dedicated load balancers or proxies together with protection by IP filters can replace the use of a firewall and offers similarly high protection. The prerequisite for this is that the proxies/load balancers are also hardened and securely configured.

Req 409 Hardening the back end systems

The back-end systems need to be hardened in order to prevent unauthorized attackers from gaining unauthorized access to the systems and data through vulnerabilities in the system. In addition to DTAG's Security Requirements, there are also other generally applicable best practices. In the case of system hardening, at least the following factors must be taken into account:

- Current patch level
- All unneeded software elements must be uninstalled
- All unneeded services must be uninstalled or deactivated
- Whenever possible, the required services must be tied to the interfaces where they are needed
- Unnecessary preconfigured service accounts must be deleted and default passwords must be changed

Implementation proposal: set up new systems according to hardened standards
New systems to be set up should be set up according to standard policies that meet IT-Security departments hardening guidelines

Implementation proposal: implementing hardening using automatic processes (e.g. group policies)
Automatic processes can be used to ensure that the hardening measures are implemented and updated centrally. In the Windows Server environment, hardening can be ensured using corresponding active directory policies. Other Telekom-internal tools such as SIUX can also be used.

5.4 Interfaces

Req 410 Describing all interfaces and the transmitted personal data fields

All interfaces to other IT processes must be documented. This documentation must contain at least the following information:

- all personal data fields
- direction of transmission (import/export)
- the purpose for which the transmission will be used
- the IT process/interface where the data is exported to
- type of interface authentication
- transmission protection (e.g., encryption)

In particular, import and export interfaces from and to files must be described as well as how their use will be protected through technical or organizational means. Data migrations must also be described accordingly as interfaces.

Implementation proposal: documentation in the data protection concept
As information about interfaces is an essential component of a data protection concept, documentation is absolutely mandatory.

Req 411 Implementing machine/machine authentication

If personal data is exchanged between IT/NT systems, each system should have a unique and verifiable electronic identity. This makes it possible to limit the risk of unauthorized systems being able to take over and receive personal data or simulate an authorized recipient.

Implementation proposal: SSL certificates
In practice, this can be achieved by using valid SSL server certificates, for example. In doing so, it should be remembered that certificates expire and have to be renewed. Appropriate mechanisms must ensure that this can be done in time, otherwise, communication will be stopped abruptly.

Implementation proposal: identification and password
The use of user name and password is not recommended since it requires compliance with fundamental mechanisms such as password change cycles. If these requirements can be met similarly to user passwords, then this can also be implemented.

Implementation proposal: IP/port filters
If the communication between two systems takes place across trustworthy networks so that IP spoofing can be ruled out in all probability, then access to the interface can be limited by means of IP/port filtering. The IP/port filter is ideally implemented in the system.

5.5 Storage and retention

Req 412 Secure data storage

To securely store personal data with data protection class 3 or higher, an encrypted data storage system shall be provided. This also applies to any backups.

Implementation proposal: encrypted databases
Especially data classified to privacy protection level 3 or higher can be stored in a database by means of the database's encryption mechanisms.

Implementation proposal: encryption in the application
Data classified to privacy protection level 3 or higher can also be encrypted in the application, so that only this additionally encrypted content is stored in the database alongside the non-critical plain text data.

Implementation proposal: encrypted file systems
Another option is to use encrypted file systems, whereby here too, the decryption key must not be directly accessible to the system administrator for example.

Req 413 Automatically erasing temporary storage areas

Temporary storage areas (such as a browser cache or the TEMP folder of an operating system) are to be configured so that their contents are automatically deleted immediately after exiting or, at the latest, when the application (e.g., the browser) or operating system starts up.

Req 414 Access to local temporary storage areas

All access to any locally stored temporary storage areas or databases that contain personal data is prohibited and must be technically prevented, where possible.

Req 415 Secure storage on mobile data media

Storing data on mobile data media should be avoided due to the high risk of loss. However, if storing data on such media is unavoidable, the usage on this media shall be controlled and for the data stored thereon encryption shall be technically assured by default. Any data that is no longer needed must be immediately erased in compliance with data protection rules. The hardware used shall also be protected against loss/theft (by using cable locks, suitable lockable transport containers, etc.) .

Req 416 Introducing a process for managing data media

A qualified data media management system must exist. The data media management system must document how many data media containing personal data were created for which tasks and processing operations and where these media are stored up to the time they are destroyed. Regular inventory checks shall be carried out on the data media inventory. It is obligatory to store the created data media in a monitored security area if they contain personal data. The creation of data media copies must also be documented and retained for a period of 3 months after the assignment or activity has ended.

Req 417 Secure data media retention

The provided or retrieved personal data shall be stored in security cabinets, such as data safes, if the assignment or data processing activity requires that availability be guaranteed.

5.6 Secure shipment of data

Req 418 Introducing and implementing shipping regulations

If personal data is sent, it must be secured against unauthorized access.

Implementation proposal: unencrypted data media
If data media is sent, it must be encrypted. Access to the encrypted data must at least be protected by a complex password, which the recipient is notified of using an alternative, secure method. The encryption ensures that unauthorized access is prevented during transport or if the media is lost.

Implementation proposal: secure the transport route
If information is transported in plain text by transportation companies (e.g., unencrypted data carriers or in document form), the data may only be issued after prior authentication of the transport company (Deutsche Post AG, freight company, courier service, taxi driver, etc.), if necessary by calling the transport company by telephone. Reliable transport mechanisms with documented confirmation of receipt and tamper-proof packaging must be used. If very large volumes of data in plain text are shipped (>250,000 data records), the shipment must be escorted. After transport, the transmitted data must be checked to ensure it is complete and undamaged.

5.7 Secure deletion, disposal and destruction

Req 419 Collection and disposal process

A process for collecting, disposing of, destroying or deleting non-electronic data media and information media must be established and described. Rules and procedures for the secure collection and internal forwarding as well as the storage and destruction of the media, taking into account the properties typical for the media, must be described in an organizational policy/process instruction. Destroying or erasing data media in compliance with data protection rules shall be carried out at the workstation in a timely fashion to largely avoid temporary media storage. This also limits the number of people handling the data media and increases security. Organizational steps shall be taken to rule out alternative disposal methods. Employees shall be made aware of this on a regular basis.

Implementation proposal: secure disposal of paper data
Small quantities can be destroyed using a local shredding machine/multi-shredder (known as "one-4-all devices" for example) with a cross-cutting facility that meets the requirements of security level P-3 at least, in accordance with DIN 66399. Each device must be identified according to the standard.

Implementation proposal: collection points

If it is necessary to store the data temporarily, the data media and information carriers must be protected against unauthorized removal or access. If generally accessible collection containers are used for this, they must be uniquely identifiable (e.g. using numbering or a bar code system), have a secure locking mechanism, and be protected against unauthorized removal.

Implementation proposal: passing on of devices/data media
When devices with built-in data media (such as PCs/notebooks, multifunction copiers and fax devices) are withdrawn from service or passed on, for security reasons one must ensure that the internal memory is deleted beforehand in accordance with data protection requirements before it is passed on to external departments or companies.

Implementation proposal: replacement or external repair of faulty devices/data media
If, in the case of repairs, faulty devices which have built-in data media (e.g., PC/notebook, multi-function copier, fax machine) are sent to external firms for replacement or repair, and if the data they contain is not encrypted, the data media which such devices contain must be securely erased before handover if possible. If this is not possible (for example because the device can no longer be accessed and/or the data media cannot be expanded), or the data media itself is defective and no appropriate deletion equipment is available, then it may only be handed over as part of a data protection subcontracting relationship.

Req 420 Introducing erasure and destruction methods in compliance with data protection rules

For security reasons, unencrypted data media must be erased in compliance with data protection rules before being reused internally (e.g., changing primary user) or passed on to external parties. Formatting is unsuitable as a secure erasure method. Other secure erasure/destruction methods must be selected which make it extremely difficult to reconstruct the data.

Implementation proposal: multiple overwriting
Physical deletion that is sufficient for normal protection requirements can only be achieved by overwriting the entire data media multiple times. The overwriting procedure for normal data must consist of at least two runs, and at least three for data that is subject to telecommunications secrecy. With the second overwrite, a data pattern that is complementary to the first run (bit sequence) should be used. Random data should be used for the third overwrite. If deletion or securely overwriting are not possible (e.g. DVDs/CDs, defective data media), the data media must be destroyed.

Implementation proposal: physical destruction
The data is destroyed by physically destroying the information carrier (shredding or material conversion) and can be achieved using professional shredders, but thermal procedures such as burning or melting are also suitable. For the destruction of paper and plastics, for example, the requirements for security level 3 destruction as specified by DIN 66399 (destruction of non-magnetic data media) are to be applied as a minimum standard. Magnetic or optical data media (such as magnetic tapes, disks, identification cards with magnetic strips, CDs/DVDs) can be physically destroyed according to the same minimum standards.

Implementation proposal: magnetic neutralization
As an alternative to physical destruction, magnetic data media can also be magnetically neutralized. The minimum requirements for magnetic tapes, disks, identification cards with magnetic strips etc. are derived from DIN 66399 (deletion of data in need of protection on magnetic data media). In the same vein, data on hard and removable disks can be destroyed using appropriate deletion devices (Degausser) using powerful magnets, instead of being physically destroyed.

Implementation proposal: confidentiality through encryption
The confidentiality of information on electronic data media can also be guaranteed by ensuring that the data is encrypted on the data media, and that the information can only be accessed following user authentication (e.g.

using a smart card/token and password). This means it is not necessary to destroy/delete the encrypted data media.

Req 421	Maintaining erasure logs

The complete and permanent deletion of data and data carriers with personal data in compliance with data protection rules shall be logged. The logs shall be archived in an audit-compliant form for at least 3 months.

6 Input control

Annex to §9, sentence 1, of the Federal Data Protection Act states the following: "... to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control)".

6.1 Basic requirements

Req 501	Logging input

The inputting of personal data into the data processing system shall be logged. The retention period for logs depends on the rules agreed with employees' representatives. In the absence of such rules, the retention period is 3 months. Suitable procedures shall be agreed with the employees' representatives and the data privacy team in order to identify improper use and carry out incident-related evaluations.

Req 502	Documenting the input authorizations

Records must be kept of which persons in their roles are authorized and responsible for inputting into the data processing system.

7 Job control

Annex to §9, sentence 1, of the Federal Data Protection Act states the following: "...to ensure that personal data processed on behalf of others are processed strictly in compliance with the Customer's instructions (job control)".

7.1 Basic requirements

Req 601	Conclusion of an agreement on commissioned data processing (CDP)

If a third party (including other legal entities within the company) is commissioned to record, process or use data, a CDP agreement shall be concluded. The templates provided by GPR (datenschutz.telekom.de) shall be used for this purpose.

Req 602	Issuing and receiving instructions

The persons at the Contractor's end who are authorized to receive and execute the Customer's instructions are specified by the Contractor in binding terms and documented, for example, in an instruction spreadsheet. The Contractor communicates the persons authorized to receive instructions to the Customer immediately after the order has been placed and when changes occur. When receiving instructions or exercising their authority, these persons must prove their identity to the Customer's departments responsible for this.

Req 603 Order execution rules and limitations

Only the work set forth in the service description to be prepared may be carried out. All activities that go beyond this scope must be discussed specifically in advance with the competent Customer party and approved in writing. The Contractor must coordinate the scheduling of the work carried out on behalf of the Customer with the Customer in advance.
The Contractor must inform the Customer without undue delay of any incidences of serious disruptions of operations, any suspicion of data protection violations, if errors or other irregularities occur in the handling of Customer data. The Contractor must immediately remedy these problems.
At the end of the contractual relationship, the work results and the data, documents and operating supplies received must be handed over in the agreed manner.

Req 604 Logging the order execution on the part of the contractor

Suitable documentation must make it possible to fully track the individual activities required for performing the work on behalf of the Customer and, on request, prove that the work in question was carried out strictly according to the Customer's instructions (minimum details: Customer/customer, action/partial order, precise specification of processing steps/parameters, processor, deadlines and, if applicable, recipient). The logs shall be archived in an audit-compliant form for at least 3 months.

8 Availability control

Annex to §9, sentence 1, of the Federal Data Protection Act states the following: "...to ensure that personal data are protected against accidental destruction or loss (availability control)".

8.1 Back-up concept

Req 701 Back-up concept

Data shall be backed up regularly in order to ensure that data is available even in an emergency. To achieve this, a backup concept shall be devised that enables authorized employees to use all available means to restore data so that it can be made available again within a reasonable time after an incident.

Implementation proposal: creating a back-up concept
The back-up concept should provide information about:

- Storage location of the data in normal operation
- An inventory of the backed-up data
- Type and scope of the data back-up (full back-up, incremental back-up, daily or weekly back-up, encrypted back-up, etc.)
- The procedure for backing up data and for reconstructing the backed-up data and
- the location of of the stored data (including reference to required means of admittance)

The back-up concept must also be regularly checked to establish whether it is up-to-date, i.e., it must be ensured that only the minimum data that is required for the further operation of the IT/NT system is stored.

Implementation proposal: regular performance of data back-ups
The back-up concept must also define which system is used for regularly backing up data. The schedule that is created must be adhered to. Responsible persons must be determined who ensure that data is backed up on schedule. Whether the data can be restored (emergency exercises) in full and within the schedule specifications must also be checked at regular intervals.

Implementation proposal: secure storage of back-up data
The same requirements and security standards apply to storing data as in ongoing operation, i.e., it must be ensured that admittance protection and access protection requirements are implemented. Similarly, data must be destroyed/deleted in accordance with the applicable data protection guidelines when it is no longer required.

8.2 Disaster recovery

Req 702 Emergency plan

The Customer shall be notified as quickly as possible of any disturbance (such as intentional internal or external attacks) or shutdown of the data processing work. If signs of a disturbance have been identified, immediate action shall be taken to minimize damage and avoid any further damage. A contingency plan shall be drawn up for this purpose, which lists the steps to be taken and determines the people, in particular those on the Customer's side, who need to be notified of the incident.

Req 703 Regular inspection of emergency equipment

Emergency facilities, e.g., emergency generators and surge protection installations, must be checked on a regular basis and the operating parameters constantly monitored.

9 Intended use control

Annex to §9, sentence 1, of the Federal Data Protection Act states the following: "...to ensure that data collected for different purposes can be processed separately."

9.1 Basic requirements

Req 801 Minimizing the amount of data collected

Only the amount of data that is essential to directly serve the actual purpose and perform the work or carry out the process shall be collected, stored or processed. This purpose may not change in any subsequent processing steps, including after transmission.

Implementation proposal: describing the intended purpose of the collected data
To ensure that the minimum amount of data is collected, it makes sense to describe the intended purpose of the data. Data that is not specifically needed to fulfill the task must not be used.

Req 802 Separate processing of different data records

Rules and measures for ensuring the separate processing (saving, editing, deletion and transmission, etc.) and/or storage of data and or data media with different purposes must be documented and applied.

Implementation proposal:
Examples of such requirements are:

- Implementation and documentation of a separation of functions (e.g. principle of dual control, closed-shop operation)
- Existence of Policies and work instructions
- Existence of procedure documentation
- Implementation of programming rules

- System and program auditing guidelines
- Implementation of a coordination and control system
- Existence of job descriptions

Req 803 Regular intended use control and deletion

The responsible unit (the requester) must regularly check whether the data saved for an individual is still needed. If the intended use no longer applies, the corresponding data must be deleted. A documented procedure (deletion concept) must be established for implementation.

Implementation proposal:
The technical and functional details for the regular review of the intended purpose and automated deletion are to be defined in a standardized deletion concept (a template is available under datenschutz.telekom.de). This review must be designed to ensure that the maximum permissible retention period of the data is not exceeded. A review of whether the data is still needed in general must be performed at least once per year. This procedure applies to all personal data used within the Group, particularly customer and employee data.

10 Organizational control

10.1 Basic requirements

Req 901 Implementation and control of suitable processes

Processes and workflows must be defined for processing data in companies. Implementation and compliance with the processes shall be monitored.

Req 902 Implementation of training measures.

All individual who deal with personal data or who are otherwise involved in order processing (such as maintenance companies or data destruction companies, where agreed) must be verifiably instructed in the following areas:

- The principles of data protection, including technical and organizational measures
- The requirement to maintain data secrecy and confidentiality about company and trade secrets, including Customer transactions (BDSG §5)
- The proper, careful use of data, data media and other documents
- Telecommunications secrecy (requirement defined in §88 TKG)
- Other specific confidentiality obligations, where necessary
- Other specific information that can result from the contractual agreement and from this catalog of minimum requirements, where necessary.

The instruction must take place through suitable measures that are appropriate to the order, and it must be repeated at least every two years, or even at shorter intervals, if needed (e.g., if the circumstances of the order or legal provisions change).

Req 903 Commitment to data and telecommunications secrecy

All persons who handle personal data (especially also non-company personnel, such as guests, suppliers) must make a verifiable commitment to data and, if necessary, also telecommunications privacy and other secrecy obligations.

Req 904	Regulations on internal distribution of tasks

The functions to be performed in connection with the provision of the service or the use of data processing/IT systems must be defined. A distinction must be made here between two levels:

- The first level comprises functions that enable or support the provision of services and use of IT (e.g., work preparation, data post-processing, operation, programming, network administration, rights management, internal auditing).
- The second level comprises functions that use the available IT/NT systems to provide services or carry out tasks (e.g., functional managers, IT application managers, data entry staff, administrators, persons authorized to make payments).

Req 905	Observation of separation and assignment of functions

A separation of functions must be defined, documented and explained, i.e., which functions cannot be combined with each other, and thus may not be performed by the same person at the same time. Requirements for this can result from the task itself, the requirements of this agreement, (especially the list of minimum requirements and supplementary standards) or from legal regulations. In principle, operational functions cannot be combined with controlling functions. After the separation of functions to be observed has been defined, the functions must be assigned to people.

Req 906	Introduction of an appropriate deputy arrangement

As part of the distribution of tasks and functions , deputy arrangements must also be taken into account and documented.

Req 909	Listing in internal procedure directories (Verfahrensverzeichnis)

In the case of IT procedures, it must be ensured that the information specified in Section 4e (1) No.1 of the German Federal Data Protection Act [BDSG] is included in the internal procedure directories (Verfahrensverzeichnis) of all German legal entities that use the procedure.
Implementation proposal:

Requirements according to Section 4e (Contents of the obligatory registration):
1. Name or company of the office responsible
2. Owners, members of the Board of Management or other legal executives or those appointed in accordance with the company's statutes to manage data processing.
3. Postal address of the responsible party
4. Purpose of data collection/processing or use
5. Description of the groups of people concerned and the relevant data or data categories
6. Recipients or categories of recipients to whom the data may be communicated
7. Standard intervals for data deletion
8. Planned data transfer to third countries

In almost all Group companies, this is ensured by the CAPE inventory management system of Telekom IT. The IRON/NOR workflow must be observed in CAPE in order to record the legally required data. Group companies that do not manage all IT procedures in CAPE must provide GPR with comparable documentation of all IT procedures used on a quarterly basis as a Adobe Acrobat pdf.

11 Applicability

11.1 Scope

This policy represents the implementation of valid data protection regulations for the Deutsche Telekom Group in Germany. The regulations are based largely on the EC Protection Directive, the Federal Data Protection Act, the German Telecommunications Act and the German Telemedia Act.

11.2 Target groups and audiences

This policy is aimed at all employees of Deutsche Telekom AG and the Group companies who work with existing systems and in facilities of Deutsche Telekom AG. Employees working on new projects apply the binding data protection requirements (SDSK) of the PSA procedure.

11.3 Implementation

This Data Protection Requirement was authorized by the Group Data Privacy Officer (L GPR) for implementation in the national Group companies. It provides assistance for the specialist departments to ensure compliance with data protection.

During implementation, the precedence of German law (in particular the Federal Data Protection Act and the Works Constitution Act), international and supranational law, and the existing collectively agreed regulations and participation rights of the responsible employee representatives shall be observed.

A List of abbreviations

Abbreviation	Meaning
GPR	Group Privacy
BDSG	Bundesdatenschutzgesetz - Federal Data Protection Act
PSA	Privacy and Security Assessment process
SDSK	Standardized data privacy and security concept

B Other applicable documents

Please see the following documents:
Binding Corporate Rules Privacy (BRCP)
Group Policy on IT/NT Security

C Terms and definitions

Term	Meaning
IT/NT system	This terms corresponds to the definition in Group Policy "IT/NT Security".

D Publication details

Published by

Deutsche Telekom AG
Data Privacy, Legal Affairs and Compliance division
Group Security Policy / Group Privacy
Friedrich-Ebert-Allee 140, 53113 Bonn, Germany

File name	Document number	Document type
Implementation of techn_orga data protection measures v5-0 fin.docx	91133	Guideline

Version	Last revised	Status
5.0	20.11.2015	final

Contact

Group Privacy
http://datenschutz.telekom.de

Approved by

Head of Group Privacy
Dr. Claus Dieter Ulmer

Bonn, January, 2016

Summary

This template is used to create policies and data protection requirements from Group Privacy.

Keywords

general data protection, data protection courses, data protection for GBS, general regulation documents, customer data, employee data, TSI focus documents, TDG focus documents, domestic data protection documents, data protection information, other

E Change history

Version	Last revised	Contacts	Changes/comments
2.0	July 17th, 2012	Andreas Link	Creation of follow-up version to 1.3
4.0	February 05th, 2014	Andreas Link	Creation of follow-up version to 4.0
5.0	November 20th, 2015	Andreas Link	Creation of follow-up version to 5.0

Note: As a general principle, the version of the document currently stored in myDMS is the valid version (http://mydms.telekom.de).

F Comments and feedback

Please send comments and feedback to the e-mail address listed under "Contact persons" in the change history, specifying the full title of the document and as detailed a comment as possible.