

Report Data Privacy and Data Security 2010.

Life is for sharing.



About this report.

Deutsche Telekom broke new ground when it published its first data privacy report in 2008. Since then, other companies have also decided to publish a report of this type, since the subject has become more important to their customers and the general public. Deutsche Telekom is now updating its annual report for 2010. For the first time, the company takes a look at all departments that deal with data processing and protection. This is why the 2010 report is the first to be titled Report on Data Privacy and Data Security.

With this report, Deutsche Telekom wishes to “provide transparency.” The idea is not just to describe the events of 2010 that relate to the company’s handling of data. Instead, the report is intended to familiarize customers, regulatory authorities, supervisory bodies, politicians as well as shareholders and employees with important processes and structures where data are processed. In a second step, we explain why Deutsche Telekom implements certain processes and works within certain structures.

The report maintains the structure known from last year: The management report provides an overview of special events that took place at Deutsche Telekom in 2010 and explains future scenarios for data privacy and data security. The chapter “Data privacy in detail” gives readers information on data privacy and data security for important reference groups within the company, such as consumers and business customers or employees. Deutsche Telekom views data privacy and security as a service. For the first time, therefore, the current report contains a guide for safe web surfing, which is also available in the Telekom shops.

In the future, Deutsche Telekom will continue to focus its data privacy and data security efforts on transparent communication in the public interest. With this practice, it plans to assume a pioneering role. Please let us know if you have any suggestions for improvement. We want to continue along the path we have begun. And we know that there is still a long way to go.

Send your opinions to: datenschutzbericht@telekom.de



Contents.

■	2 Foreword	
■	5 Management report	
	6	Overview of data privacy and data security in 2010
	6	Special events in 2010
	9	New legal provisions
	9	Audits and inspections by external and internal bodies
	10	Provision of information to government agencies and individuals
	12	Research and development
	13	Outlook – Data privacy and data security in 2011
■	15 Developments in individual areas	
	16	Consumers
	24	Business Customers
	27	Employees
	28	International developments
	30	Systems and processes
	38	Internal and external communications
■	41 Deutsche Telekom's Data Privacy Advisory Board	
■	45 Guide on the secure handling of data	
■	55 Appendix	
	56	Special data privacy and data security measures since 2008
	57	Organization of Group Privacy
	58	Organization of Group Data Security
	60	Glossary
	63	Abbreviations
	65	Imprint, Contact



In detail



Glossary

Foreword.



Dr. Manfred Balz

Dear Readers,

Many of us have got used to finding our vacation hotels on the Internet via satellite images or sharing our photos with friends around the world. 2010 has added a few new aspects to our idea of unlimited networking. Views of privacy on Facebook, the heated debate surrounding Google Streetview and the furor over Wikileaks demonstrate that the issue of how to handle data has become a central social concern.

For the first time since the German Federal Constitutional Court established the right to information self-determination in what is known as the Census Verdict on the basis of the Constitution, the interpretation and scope of this right are being subject to intensive public discussion. In late 2010, the German Federal Minister of the Interior presented benchmark figures for a draft bill that would draw the line between permissible and impermissible collection and linking of data.



“Data is the raw material of our networked world. Like water, data is fleeting. And also like water, data requires special protection.”

However, do the users possess the necessary skills to handle their own data responsibly? There is still need for education in this area. Our children should learn to use the Internet not only through unsupervised experimentation. Parents, kindergartens and schools all need to help them. But media skills on the part of consumers is not all that is needed. Providers must also explain in comprehensible terms what happens to the data.

Data is the raw material of our networked world. For our report, we chose imagery that reflects water. Like water, data is fleeting. And also like water, data requires special protection.

Deutsche Telekom recently had to pay a price for lost data. We have learned from our mistakes. Since 2008, therefore, we have used our report to disclose how data is processed and protected within our company. We post slip-ups and incidents on our website so that customers as well as regulatory authorities, politicians, shareholders and employees can form their own opinions. We welcome criticism – please let us know if you have any suggestions: datenschutzbericht@telekom.de.

I hope you will find this report both entertaining and informative.

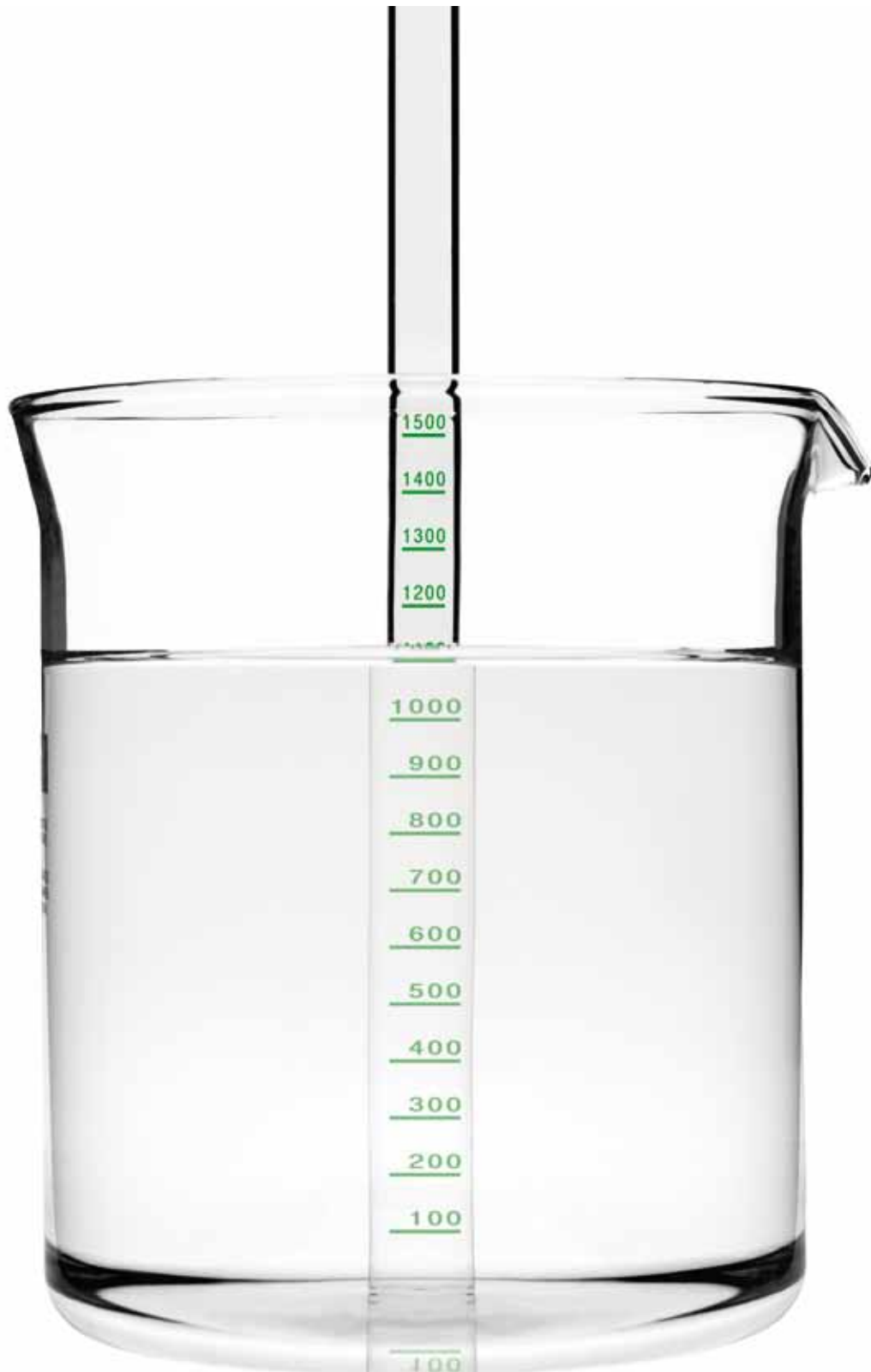
Best regards

Dr. Manfred Balz
Board member responsible for Data Privacy, Legal Affairs and Compliance.




Management report.

- ➡ Those who take data privacy and data security seriously must allow themselves to be measured by their results.



Overview of data privacy and data security in 2010.

In 2010, issues relating to data privacy and data security have dominated the public debate more than in any year in recent memory. Up to now, reports on the protection of personal data have drawn attention primarily in instances of data breaches. At other times, data privacy and security have been assumed as a matter of course. The year 2010 brought about a paradigm shift. Prompted by the launch of the Google Streetview panorama service in 20 German cities, broad segments of the public discussed the concept of privacy and protection-worthiness for weeks on end, along with the limits to what citizens should reveal about themselves in the age of the Internet.

The political response was swift. In December, the then Federal Minister of the Interior, Thomas de Maizière, presented a draft bill on protecting citizens' right to privacy on the Internet ("Red Line Act") . As a result of the public discussion, the industry also drew up a data privacy code for geodata services (which can be downloaded from <http://www.bitkom.org>), in which Deutsche Telekom played a crucial role (see below).

The discussion was also driven by repeated reports on the handling of personal data on the Facebook social network. Politicians took action in this debate; Ilse Aigner, German Federal Minister for Consumer Protection, deleted her Facebook account and called for a boycott of the network. In June, Thomas de Maizière published the first demands for systems that could wipe information off the Internet as part of his "14 Theses on the Fundamentals of a Common Internet Policy."

A new dimension was added in the fall of 2010, when Wikileaks published 250,000 classified documents belonging to the U.S. State Department.

Deutsche Telekom followed these developments closely and, where reasonable, responded by providing guides that contained detailed information for consumers.

Data privacy.



refers to the protection of individuals against the misuse of their personal data. The purpose of data privacy is to protect the individual's right to information self-determination from being violated through the use of his/her personal data.

Data security.

covers the technical and organizational measures taken to protect data against modification and loss.

Special events in 2010.


Deutsche Telekom's participation in data privacy initiatives.

Deutsche Telekom sees itself as a driving force behind data privacy and data security. In addition to delivering opinions on national and international legislative proceedings, the company is therefore active in associations and cross-company initiatives aimed at strengthening both issues in the business community and society. Examples include the "Mobile Privacy Initiative" initiated by the GSM Association (GSMA) , which deals with cross-industry standards for data privacy in localization services, and the German Association for Information Technology, Telecommunications and New Media (BITKOM) . Deutsche Telekom was involved in establishing a Data Privacy Code for geodata services as a result of extensive discussions on services such as Google Streetview. The goal of the Code is to promote the acceptance of geodata services by establishing principles for a reasonable balance between the interests of persons entitled to object to publication and users and providers of the services by way of a self-imposed obligation. At the 5th National IT Summit in Dresden, which took place in early December 2010, the industry association BITKOM presented a Data Privacy Code, which was submitted to the then German Minister of the Interior, Thomas de Maizière, by Deutsche Telekom and others during the CeBIT trade show in Hannover on March 1, 2011. The Federal Commissioner for Data Protection praised this Code as the first step toward a legally vested right of citizens to control their own data.

A paper titled "Key Points on the Privacy-Compliant Design of Home Networks," which was prepared with Deutsche Telekom's involvement, was also presented at the IT Summit. The paper describes approaches for the user-friendly, privacy-compliant and secure design of connected appliances within the home.

Judicial handling of the spying affair.

The criminal trial on the so-called “spying affair” took place before the Bonn Regional Court between early September and the end of November 2010. Employees of Deutsche Telekom’s Group Security department at the time collected data on the telephone calls of 50 people between 2005 and 2006 in order to clear up supposed indiscretions, and had the data evaluated by a Berlin contractor. The people affected included, in particular, several representatives of Deutsche Telekom’s Supervisory Board, works council members, trade union representatives and journalists. In May 2008, Telekom reported the activities to the public prosecutor’s office in Bonn. Upon conclusion of the investigations, the public prosecutor’s office brought charges against a former department head of Group Security, the Berlin contractor and two other former Group Security employees. The public prosecutor’s office dropped its investigation of Kai-Uwe Ricke, the former Chairman of the Board of Deutsche Telekom, as well as Dr. Klaus Zumwinkel, the former Chairman of the Supervisory Board of Deutsche Telekom.

In late November 2010, the Bonn Regional Court sentenced the former Group Security department head as the main defendant to three years and six months in prison for violating telecommunications secrecy and the German Data Protection Act  as well as for breach of trust. The ruling had not yet become enforceable at the time this report went to press on March 1, 2011. Proceedings against the two former employees who were charged along with the department head were terminated following payment of a fine. The Berlin contractor who was also charged had argued that he was unable to stand trial. The proceedings against him will take place at a later time.

As a result of the spying affair, Deutsche Telekom will donate around 1.7 million euros to charitable organizations. The company views this as a token of the corporate responsibility that it has assumed for its past actions. In addition, the Group and the attorneys for the members of the Supervisory Board/works council and the trade union representatives reached an agreement on individual damage compensation to be paid by Deutsche Telekom. Talks on individual damage compensation have also been initiated with the journalists and other parties who had been spied on, or such talks will be initiated in 2011.

Misuse detection systems.

International organizations estimate that telecommunications providers, including Deutsche Telekom and its customers, sustain damage amounting to a combined €50 million per year worldwide through misuse. Such misuse ranges from registration fraud and failure to pay for services to avoiding termination charges (forwarding charges), hacking into telephone systems, use of flat rates under non-contractual conditions as well as misuse of value-added services.

To identify, track and prevent such scenarios, Deutsche Telekom maintains various misuse detection systems on the basis of Section 100 of the German Telecommunications Act (Telekommunikationsgesetz). Due to different configurations, these systems are able to examine the various fraud scenarios from different points of view. The Federal Commissioner for Data Protection and the German Federal Network Agency were notified of all systems in writing.

The misuse detection systems evaluate traffic and signaling data (traffic data corresponds to billing data; signaling data is used as a technical means for setting up and clearing a call). The content of calls is never the object of the analysis. Therefore, the spoken conversations are not recorded, but only which call number was engaged in a phone call with which call number and for how long. The systems do not look for certain calls, but rather for conspicuous patterns on the basis of scenarios and filters previously approved by the Data Privacy department. By default, the systems search for cases of fraud as well as for specific suspicious incidents.

Assessment of misuse detection systems.

A number of Deutsche Telekom’s misuse detection systems had been improperly used in 2005 and 2006 during the course of the spying affair (see above) in order to track call data. Once the misuse became known, a series of measures were adopted to prevent this theoretically possible use of the systems.

In 2009, for example, Deutsche Telekom further tightened and fleshed out the regulations on the use of misuse detection systems. Data Privacy drew up a specific list of known fraud scenarios and approved the resulting filter settings for the detection systems which can search for these scenarios. Since then, each possible new scenario and each new filter must be approved by the independent Data Privacy department.

Deutsche Telekom also took a number of further steps:

- Separation between the staff-related and organizational aspects of the process steps “request for research”, “research based on a specific initial suspicion”, “investigation” and “consequence management”
- Recording of the individual activities carried out by system users to track possible misuse of the systems
- Double-checking principle in system-critical activities, such as setting and approving a new filter

Lothar Schröder, Chairman of the Data Privacy Advisory Board and Deputy Chairman of the Supervisory Board of Deutsche Telekom, and Dr. Manfred Balz, Board member responsible for Data Privacy, Legal Affairs and Compliance, reviewed the misuse detection systems in April 2010 in order to gain an understanding of the effectiveness of the adopted measures. They assured themselves of the quality of the data privacy practices and the high level of procedural and systematic standards that ensure the strictly lawful use of these systems. Lothar Schröder reported the results of the review to the Data Privacy Advisory Board of Deutsche Telekom in May 2010.

Expert opinions on data privacy.

After the data privacy incidents were made known, Deutsche Telekom commissioned Dr. Gerhard Schäfer, former Presiding Judge at the German Federal Court of Justice (BGH), to write an expert report on data privacy in the spring of 2008. This report was to provide a further external look at Deutsche Telekom’s systems and processes that are to ensure data privacy and data security. The report, which was submitted to the Group Board of Management in December 2009 and also to the Data Privacy Advisory Board in early 2010, contained numerous recommendations on ways to tighten and improve individual processes. Among other things, the recommendations call for further refining of access rights for customer data in call centers [G]. They also pointed out the importance of complying with deadlines for the deletion of data from terminated contracts.

Deutsche Telekom largely completed the implementation of individual operational measures in 2010. A small portion of the measures are still being implemented today. All measures are on the operational level. No cases of abuse like those that became known during the course of the data incidents have been identified.



In March 2010, the German Federal Constitutional Court declared data retention to be unconstitutional. Deutsche Telekom irreversibly deleted the stored data.


Data retention practices discontinued.

On March 2, 2010, the Federal Constitutional Court declared the existing regulations governing data retention [G] from 2008 and 2009 to be unconstitutional. The regulations obliged telecommunications providers, for example, to store the calling party’s number, time and length of the call, other data regarding e-mail and Internet usage, as well as the radio cell in the case of mobile communications. Deutsche Telekom immediately stopped storing and providing information on all data following the ruling. The data stored was deleted irretrievably.



A debate is currently underway in the responsible political committees at German and European level on how to deal in future with the issue of data retention. Deutsche Telekom is advocating a solution that provides a balance between public security and data privacy, but that also reflects the benefits and costs.



Dealing with unauthorized marketing companies.

As discussed in the previous report, unauthorized call centers  in Turkey concluded fixed network agreements with customers for Deutsche Telekom's former Group unit T-Home in 2009. These activities have since been resolved; Deutsche Telekom pressed criminal charges and filed claims under civil law (demand for the return of commissions, contractual penalty, data deletion, etc.). In addition, cooperation with some companies was terminated and warnings were issued. The Turkish call centers were called on to discontinue the unauthorized sale of Deutsche Telekom products. While the criminal proceedings are continuing, the company has successfully resolved the claims under civil law and compensated the material damage caused in the amount of roughly €1.5 million. At the same time, Deutsche Telekom implemented new measures to prevent similar business activities and continues to introduce them.

New legal provisions.

In 2010, lawmakers made important decisions in support of data privacy with a draft bill on employee data privacy and on the amendment to the Telecommunications Act (Telekommunikationsgesetz – TKG) . At the same time, a few changes were made to the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG)  with regard to the disclosure of data to third parties. The Access Impediment Act (Zugangerschwerungsgesetz), which is intended to make it difficult to access child pornography websites, went into force in February 2010. The implementation of this law was suspended on the basis of the federal government's coalition agreement; the Federal Criminal Police Office did not make any revocation lists available for retrieval by the telecommunications companies. Deutsche Telekom subsequently discontinued its measures initiated in early 2010 to make it difficult to access child pornography websites, and removed the infrastructure that had already been put in place.

At the European level, the amendment to the 1995 European Data Privacy Directive has begun.

Details on the changes are provided in the sections on data privacy and data security for consumers, employees and international developments.




Audits and inspections by external and internal bodies.


Internal and external agencies again audited Deutsche Telekom's systems and processes in 2010. Either the supervisory authorities or – usually in connection with certifications – independent external agencies conducted and will continue to conduct external audits and inspections. Deutsche Telekom itself also reviews compliance with legal provisions as well as its own security and data privacy provisions. In doing so, the company continuously maintains a level of protection that is among the highest in the telecommunications industry.

Government audits and inspections.

Group Privacy at Deutsche Telekom is in continuous dialog with the Federal Commissioner for Data Protection and Freedom of Information  and the German Federal Network Agency  regarding current issues related to data privacy as well as the measures taken at the company. Early involvement in critical issues relating to data privacy increases transparency vis-à-vis the regulatory authorities. In 2010, further measures for optimizing the level of data privacy were implemented following intensive coordination with the Federal Commissioner for Data Protection as a result of the Commissioner's consultation and inspection visits in 2008 and 2009. The Commissioner made no further consultation and inspection visits in 2010.

Audits and certification.

In addition to the inspections conducted by the supervisory authorities, Deutsche Telekom also expanded its activities relating to certifications  and audits  in 2010. All in all, Deutsche Telekom's central departments conducted over 450 internal and external audits on the topics of data privacy and data security. Sales also certified more than 100 call centers  or began the certification process. The certification of Deutsche Telekom's exclusive partners, i.e. dealers who sell Telekom products exclusively, was also initiated in 2010.

Deutsche Telekom thus relies on both internal and external expertise in ensuring a high level of data privacy and data security. As confirmation of its high level of security and privacy, Deutsche Telekom also obtained a security certification according to ISO  27001 for its central security management system and a data privacy certification for its billing process in the fixed network consumer segment in 2010 (see pages 35/36).

Provision of information to government agencies and individuals.

Queries addressed to Data Privacy.

The number of inquiries relating to data privacy received by mail, fax or through online channels – either addressed directly to Group Privacy or to service addresses set up specifically for this purpose – increased from 7,460 inquiries in 2009 to 10,808 in 2010. Most of the inquiries received in 2010 came through the special service e-mail address datenschutz@telekom.de. Inquiries are processed by a specially trained team of employees. The reason for this growth in inquiries is the heightened sensitivity to the topic of data privacy among customers and the increasing perception of Deutsche Telekom as an advisor. E-mail has thus become established as a communication channel. Group Privacy and its privacy officers received approximately 911 inquiries, including 190 inquiries that were submitted to the Federal Commissioner for Data Privacy.

Distribution and type of customer inquiries submitted to Group Privacy.

The overwhelming majority of customer inquiries were requests for information under Section 34 of the Federal Data Protection Act [\[G\]](#). According to this law, customers can ask a company to provide information, free of charge, on the stored customer data, the purpose of the storage, the people and bodies to which the customer's data are regularly transmitted (people, companies, agencies, etc.) and, in particular, the origin of the data. These inquiries relate to all data stored on the customer.

Inquiries relating to the Group permission clause (KEK) usually concern the withdrawal of permission to receive advertising or information granted upon conclusion of an agreement. The reason for such inquiries

is, for example, regular receipt of advertising materials, advertising calls or faxes. Customers want to find out whether they have indeed granted such permission or the scope of this permission.

Inquiries relating to directory listings are aimed at correcting or deleting entries in public directories (such as the phone book or directory service). In these cases, Deutsche Telekom provides information within the scope of its legal obligation.

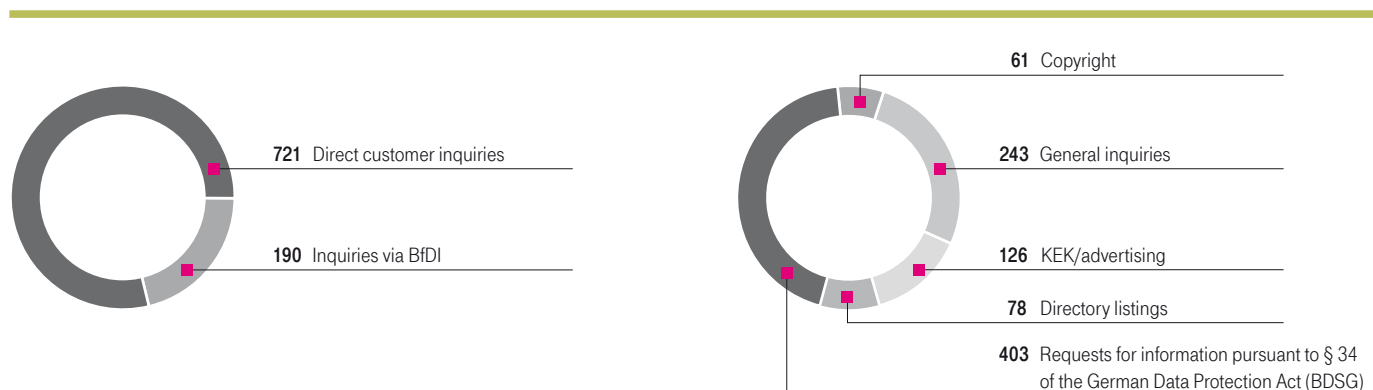
In contrast, inquiries relating to copyrights concern the type of customer data disclosed to a third party, the so-called holder of the right, in a specific instance. Copyright inquiries are submitted by customers who have received warnings of alleged copyright violations from a lawyer (such as claims for illegal use of file sharing sites on the Internet). Or they are submitted by attorneys of rights holders who claim the allegedly impermissible use of copyrighted works (such as music or videos). An inquiry based on copyright violations is frequently followed by requests for information by customers under Section 34 of the Federal Data Protection Act.

Contacting Deutsche Telekom.


Customers who would like to obtain information from Deutsche Telekom on the personal data stored on them can do this through different information channels:

By mail: Group Privacy Officer, Deutsche Telekom AG,
Friedrich-Ebert-Allee 144, 53113 Bonn, Germany.
E-Mail: datenschutz@telekom.de

Distribution and type of customer inquiries submitted to Group Privacy.



Inquiries relating to copyright violations.


In 2010, Deutsche Telekom received temporary orders for the preliminary storage of around 200,000 IP addresses , on average each month. The holders of the rights or their service providers determined these addresses during searches for unlawfully offered copyrighted works. The number of IP addresses mentioned above does not equal the number of actual users who have offered protected works on platforms. Experts believe that a much smaller number of real people are behind the number of requested IP addresses. There are technical reasons for this. Multiple searches for a person's IP address can be carried out while he/she is using a file sharing site. At the same time, a person can have used multiple IP addresses over a certain period of time.

IP addresses.



An IP address (Internet Protocol address) is required for using the Internet. IP addresses allow devices to be addressed logically and uniquely in IP networks such as the Internet. Usually, an IP address is not assigned permanently, since the number of addresses available worldwide for the current IPv4 protocol is less than the number of possible devices. Each time a user dials into the Internet, the Internet access provider therefore assigns a so-called dynamic IP address. Deutsche Telekom stores this combination of user ID and IP address for a period of seven days in order to combat technical attacks on the network infrastructure, spamming or attacks by malware such as Trojan horses or botnets. This is done on the basis of Section 100 (1) TKG and Section 109 TKG.

No reliable figures exist on the development of copyright infringements. With information on 2.28 million IP addresses requested in 2010, however, Deutsche Telekom reported an increase compared to the previous year (1.4. million). The reason for this growth is that more and more holders of rights are using these means to track their rights.

In 2010, Deutsche Telekom accumulated complaints from users who claimed that they were not on the Internet at the relevant point in time. In individual cases, unsecured or poorly secured WLAN connections could have been the cause. Deutsche Telekom has therefore drawn up a data privacy guide for customers which points out this problem. In addition, the equipment operating instructions contain a notice section on encryption and security standards. Furthermore, Deutsche Telekom's latest WLAN routers are provided with an individual network key, and WPA2-PSK encryption  is already activated on delivery. These default settings make the routers particularly secure.

Providing IP information.



Since September 2008, providers such as Deutsche Telekom have been legally obliged to provide, upon request, information from their existing database to owners of copyrights and ancillary copyrights about customers who allegedly have offered the copyright-protected works on file sharing websites. The right to information of the copyright holder stems from the German Copyright Act (Section 101 (2) UrhG). Due to the associated encroachment into telecommunications secrecy, the copyright owner must first apply for judicial permission (Section 101 (9) UrhG). After a copyright infringement has been established, owners of copyrights and ancillary copyrights have seven days to obtain a temporary court order that the IP addresses and their customer assignments established in connection with an infringement be secured. The court checks whether all legal requirements for obtaining information have been met. It also investigates whether the applicant is really the holder of the copyrights or ancillary copyrights, whether the situation is an obvious copyright infringement on a commercial scale, and whether the relevant IP address whose assignment is to be requested from the provider has been determined properly by the copyright owner. If all requirements have been met, a final court decision is made, following which Deutsche Telekom must hand over the backed up data to the owner of the rights or to his/her legal representative. Before doing this, Deutsche Telekom will check whether all necessary decisions and details on provision of information have been obtained. The existing customer data is then provided. Any additional traffic data, communication content or other information referring to such data are not the object of the information provision. After completion of the process, Deutsche Telekom deletes all corresponding data in accordance with legal requirements.

Deutsche Telekom's procedures for assigning and storing the IP addresses, the usage periods and the assignment to customer IDs follow common methods of digital and automated data processing. The user IDs, in particular, prevent mix-ups. Any data processing and database system malfunctions on the part of Deutsche Telekom can be practically ruled out. The data backups needed to provide the information are fully automated without any manual input of IP addresses and dates.

Telecommunications monitoring under Section 109 TKG.

Various German laws at the national and state levels obligate telecommunications companies to allow the security authorities to monitor telecommunications traffic as well as to issue information about traffic and customer data to the security authorities.

The legal basis for telecommunications monitoring is derived from the German Code of Criminal Procedure (Strafprozessordnung), the Article 10 Act (Art. 10 Gesetz), the Customs Investigations Service Act (Zollfahndungsdienstgesetz), the Federal Criminal Police Office Act (Bundeskriminalamtgesetz) and individual state police laws. Depending on the legal basis, telecommunications monitoring must be ordered by a judge or by a comparable neutral institution (such as the head of a top state authority or a federal minister). The calls concerned are then forwarded to the authorities over a secure line. Deutsche Telekom does not have access to the content of the calls or data connections. Legally correct handling of inquiries from security authorities is particularly important for a telecommunications company like Deutsche Telekom because its employees would otherwise quickly run into danger of rendering themselves liable to prosecution due to obstruction of justice (for furnishing allegedly insufficient information) or due to breach of telecommunications secrecy (for furnishing information too "generously").

Deutsche Telekom has four units for providing information to government agencies. For the fixed network/Internet segment it has three regional offices for special government regulations in Frankfurt, Hannover and Berlin. The Münster-based office for mobile communications information for public authorities performs these functions for mobile communications nationwide.

Further development of information provision.

Following the founding of Telekom Deutschland GmbH, it became necessary to check the information provision processes in place at both T-Mobile GmbH and Deutsche Telekom AG (T-Home) for differences and to harmonize them in individual cases. In addition, companies that provide the information also have freedom of action, since the existing legal requirements cannot cover all constellations in daily life. To avoid having to make ad-hoc assessments of legally complex matters, Deutsche Telekom is also revising its practices for providing information to government agencies. The goal of the project is to draw up a reliable guide for providing information to authorized government agencies in 2011. The guide must provide employees with clear rules for their actions in individual situations, even in case of doubt, in order to deal with the conflicting priorities of freedom and security, taking the company's interests into account. At the same time, Deutsche Telekom is committed to promoting a more detailed specification and standardization of the basic legal conditions for providing information at the national level.

Research and development.

Instead with your credit card, pay with your cell phone. Receive an SMS text message when a window is forced open in your home. It is common practice at Deutsche Telekom to fully integrate data privacy and data protection into such products as early as the development stage (see page 33, PSA procedure).

Telekom Laboratories (T-Labs), founded in 2005 together with Technische Universität Berlin, develops innovative products for the company and integrates aspects of data privacy and data security as early as the development phase.

The innovative research and development institute combines practical product and service development with scientific research. A good 300 Telekom experts and scientists in a wide range of disciplines from all over the world work on solutions for the easy, fast and secure communication of tomorrow. In researching and developing future-oriented products and services, T-Labs takes into account aspects of data privacy and data security at an early stage.

A few examples of T-Labs' research work to guarantee data privacy and data security are:

- Developing methods for the early identification of misuse and hacker attacks on a communications network (for example, through computer viruses and worms).
- Minimizing the quantity produced and the use of critical information on the development of procedures that permit customization yet also protect the user's identity.
- Developing an optimized anonymization process that adapts automatically to ensure that usage data collected for network planning or service optimization does not allow any conclusions to be drawn about individual users even when the data volumes are small or different extracts from databases could be combined.
- Researching new methods to facilitate identity management; access data for user accounts falls into the category of sensitive personal data. The increasing number of passwords often causes people to be less vigilant in their use of security mechanisms: weak passwords, notes posted on PC monitors. Identity Management is working on more user-friendly methods that combine ease of use with greater security. For example, identity providers can reduce the number of passwords that need to be memorized, while contactless – or virtual – cards ensure secure transmission of access authorizations.
- Developing user-centric identity management methods. For example, profile information, i.e. information on interests, default settings, usage patterns, etc., can be managed by the users themselves and not by the service provider. Each time they use a service, users therefore can determine whether to reveal any information at all, and if yes, which information – and possibly even a pseudonym under which the information should be revealed.




Furthermore, aspects of data privacy and data security have influenced the development of products and services that are currently in the product launch phase. These aspects were consistently taken into account from conceptualization to product launch:

Mobile Wallet: This new development makes it possible to use a mobile phone for making payments and bundling customer cards with Near Field Communications (NFC) technology, turning the phone into a something like a mobile wallet. Users of the new technology can have their bank and customer data stored on the SIM card that the network operator uses to protect its own services. Since banks and institutions, but not the operator, can view the programs and security mechanisms, and because the selection of a payment service is up to the user, this makes it more difficult to misuse the service, while an anonymous prepaid account ensures privacy.

Home management applications: Houses and apartments of the future will be networked; thus the vacuum cleaner will be turned off when the telephone rings. The alarm system will write a text message when it registers movement in a room. These are no longer future scenarios, but things that are technically feasible today. Standardized operating concepts, confidentiality of data content, user sovereignty over data, transparency and control over access authorizations are only some of the challenges in the field of data privacy for which solutions are being developed. At the same time, the focus is on offering practical, secure and trustworthy solutions for potential users of future home networks.

Outlook – Data privacy and data security in 2011.

Wikileaks revelations, industrial viruses such as stuxnet as well as discussions on what “private” and “public” mean in the Internet age were issues last year and will remain on the agenda in 2011. In 2011, the use of personal data by social networks became a hot topic of discussions on ways to delete such data from the Web. Ideas such as a “digital eraser” or an expiration data for certain content will continue to be discussed in the coming months. In a larger context, the debate extends to topics such as the right to oblivion and the limits to privacy in the Internet age. These discussions will certainly keep cropping up for a long time to come.

Where the technical development of products and applications is concerned, the principle of digital networking will continue to be expanded in 2011 and thus give rise to new questions about data privacy and data security. Cloud or dynamic computing  will provide innovative solutions, and not only for business customers. Private users will also no longer store their data and software on home computers or on their smart phones. They will access the servers of central data centers from anywhere. And while the level of protection in these data centers far exceeds that of an average home computer, such centers could naturally also become the target for attacks. Control of power grids that ensures the economical use of

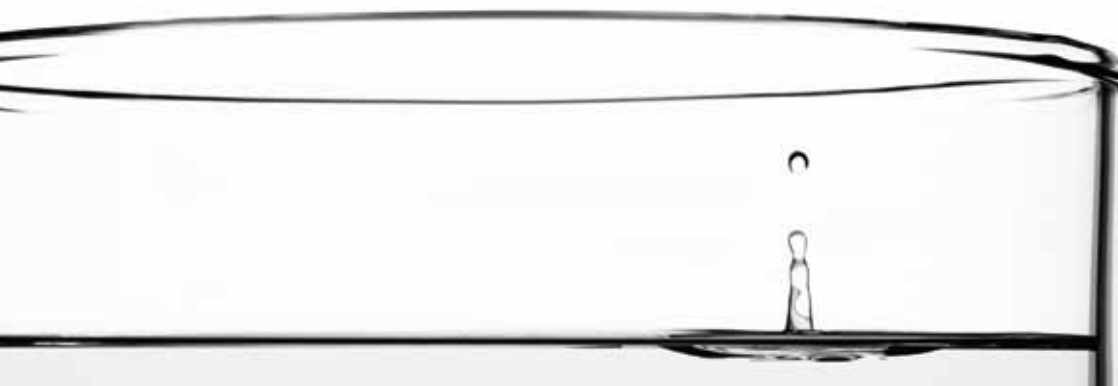
resources will be further improved in the coming years; solutions for home appliances with intelligent communication capabilities will soon be a matter of course. With all these developments, the topics of data privacy and data security will play an ever greater role in the future. Deutsche Telekom takes this increased demand into account. 2011 will see the global rollout of a procedure that is already being practiced in Germany and which requires the integration of data privacy and data security into the development phase of products and services (see page 33, PSA procedure). With this rollout, the Group will establish a standard protection and security standard for its products and services. Deutsche Telekom will provide support for technical innovations in areas such as dynamic computing and networked home environments with increasing focus on data privacy and data security and expand a high level of protection and security as a competitive advantage.

The stuxnet attack on Iranian nuclear facilities in 2010 made it clear that companies and institutions that wish to secure and protect their data and systems must consider a new digital threat in the future. In addition to dealing with technical aspects of security, it will become more important for companies to raise awareness of responsible data use among their managers and employees and to explain how easily negligence can cause damage to the company. At the same time, companies will have to also protect themselves against employees revealing confidential information in order to harm the company. In the wake of the past data scandals, Deutsche Telekom has laid an important foundation for a new, modern corporate culture in which employees and their concerns are taken seriously, but in which transparent rules are also being established and action is taken in case of doubt. The company will expand and strengthen this culture. In terms of technology, Deutsche Telekom will continuously improve systems and processes in 2011 to always remain one step ahead of attackers. In addition, the company will check its training measures and campaigns for data privacy and data security to ensure that they are up to date and adjust them where necessary.

At the legislative level, the signing of the “Red Line Act” , an amendment to the employee data privacy act and an amendment to the EU Data Privacy Directive are planned for 2011, among other things. Deutsche Telekom will get intensively involved in the discussion of legislative changes and implement and apply adopted laws and amendments immediately.

Developments in individual areas.

➡ Data privacy and data security only work if every department does its part.



Consumers.

Legal provisions.

New provisions of the Federal Data Protection Act [\[G\]](#), which regulate the transmission of data requested by credit inquiry agencies, the use of data for the purpose of calculating probability scores, and an expansion of the affected persons' rights to obtain information, went into force on April 1, 2010.

Credit inquiry agencies are companies that collect credit-relevant data on companies or individuals for business purposes in order to provide this data for a charge as needed in assessing the creditworthiness of a data subject. Up to now, the transmission of data to such credit inquiry agencies was not clearly regulated by law. With the new provision in Section 28a BDSG, the lawmakers have now clarified this matter. It describes five specific situations in which, for example, information about a claim against an individual or company may be transmitted to a credit inquiry agency of this type. These changes were also relevant to Deutsche Telekom. Deutsche Telekom also reports uncontested, outstanding receivables to credit inquiry agencies such as SCHUFA, the Fraud Prevention Pool (Bürgerl) and Accumio. Procedures were established to ensure that the necessary notices are given to the customers in accordance with the new Section 28a BDSG and that the necessary periods between the reminder and registration are observed.

In addition, the provision governing the use of data for calculating scoring values was amended in Section 28b BDSG. The conclusion of an agreement is often linked to the customer's ability and willingness to pay (e.g., when a customer asks for a loan or wants to conclude a mobile communications agreement). Companies frequently use a scoring process to rate a person's liquidity.

According to Section 28b BDSG, the use of data for calculating scores is now linked to certain requirements. The data used must be verifiably significant for calculating a future forecast, and score calculation must be based on a scientifically recognized procedure. Scoring based exclusively on address data is not permitted under Section 28b BDSG.

Deutsche Telekom calculates scores as part of credit checks on prospective customers as well as scores for existing customers, i.e., customers whose contractual relationship has lasted more than 5 months. Both scores indicate how likely it is that the existing or prospective customer will fail to meet his/her payment obligations over the next few months. The probability of failure to pay is indicated by scores between one percent (very low) and 99 percent (very high).



Interview with Dr. Claus-Dieter Ulmer,
Chief Privacy Officer
at Deutsche Telekom.



What sets DTAG's data privacy practices apart from those of other companies? What will the trend be in the future?

At Deutsche Telekom, data privacy has taken on a dimension that other companies do not experience in this form, due to the data incidents. The loss of 18 million sets of customer data and, in particular, the spying affair in 2005 and 2006 have unleashed a real shock wave within the company. We have used the momentum generated by this wave for the well-known fundamental changes throughout the company: the establishment of a Board of Management department for Data Privacy, Legal Affairs and Compliance and the reorientation of Group Security are only two examples. The past events have induced us to enhance our privacy practices even more resolutely than we probably would have done had the incidents not taken place. Today, we have achieved a data privacy standard that cannot be taken for granted in the German business community. We have now become the benchmark for other companies in many areas. We are happy to share our experiences and what we have learned from them. After all, we see data privacy as our special responsibility. We meet this responsibility by perceiving data privacy as a service for our customers. We would like to show them how to protect their personal data in everyday situations by providing guides or personal consulting, such as in online chats. We also meet our responsibility by establishing a stronger role for ourselves as a leader in the German business community where data privacy is concerned. In this area, we want to set standards that go far beyond the boundaries of our industry.

Scoring.





Scoring is a mathematical-statistical method that makes it possible to calculate the probability of a certain person demonstrating certain behavior. This probability is indicated by a score. The probability of a customer's payment behavior can thus be calculated in this manner.




To reflect the score provisions, the data subject's right to information under Section 34 BDSG was expanded to meet the transparency requirement. The data subject may request information about the scores that were collected or used within the past six months (within the past 12 months in the case of credit inquiry agencies) as well as information about the type of data used for scoring. The data subject furthermore has a right to receive an explanation, in a generally understandable form, of how the score was reached and what it means. For reasons of transparency, Section 6a BDSG was also expanded and now specifies that the data subject receive an explanation of the main reasons why an automated decision was negative in his/her case.


Deutsche Telekom has made preparations with regard to these additional rights to information. For example, if a customer asks why his/her order was rejected, the general customer service department will refer him/her to a team which was set up specifically for this purpose and which will process these inquiries. These employees now have the additional information needed to explain the main reasons for rejection. This takes into account the right to information, while at the same time only a narrowly defined number of specially trained service employees can access the information, some of which is sensitive.

Further legislative procedures are in progress for implementing the requirements of the directives for the communications sector that went into force at the European level in December 2009. These European requirements must be transposed into German law. This set of directives also includes the so-called ePrivacy Directive (Directive on Privacy and Electronic Communications). It requires that certain adjustments be made to German data privacy laws. The core elements of these required adjustments are:

- Expanding the obligation to provide information about data breaches, specifically for providers of communications services. The European requirements call for immediate notification of the regulatory authority and the data subject in the event that the privacy of personal data was violated, for example due to unauthorized use of the person's data. In addition, the obligation to provide information has also been expanded to internal activities, such as the misappropriation of data.
- Adopting stricter requirements for the data subject's consent to allow personal data to be processed. The context is that the so-called opt-in solution  has been extended to include cookies  in browsers for surfing the Internet or for similar technical solutions which can be used to identify an Internet user. This is primarily aimed at browser providers. The intent is to keep Internet users better informed on how their personal data is handled and to give them greater influence on the use of their data in cookies than is currently provided by German data privacy law. In implementing these requirements, the question arises as to whether the users must be able to accept each cookie individually, or whether it is sufficient for them to select the desired security standard in their web browsers settings, provided they can change these settings at any time.

Deutsche Telekom welcomes these improvements in the protection of personal data and is contributing its ideas to the legislative procedures for implementing the ePrivacy Directive. In the interest of comprehensive protection, however, the company feels that the adjustments should not be limited to suppliers of communications services but be expanded to all sectors. After all, the healthcare industry also handles sensitive personal data which should receive an equal amount of protection. Such a level of protection can be reached through the discussions currently in progress on an amendment to the European privacy directive of 1995 (see page 28, International developments, for details).

Other requirements in the Telecommunications Act  should also be modified. Core elements from a data privacy perspective are:

- Modifying the requirements to enable system maintenance according to the "follow-the-sun principle". For example, a maintenance activity could start in the morning in Germany, continue after business hours in the United States and be completed in India at the end of the workday in the U.S. It will of course be necessary to ensure compliance with data privacy provisions.
- Revising the data privacy provisions for the use of location data in the context of location-based services )

Deutsche Telekom will evaluate the draft bills and support the legislative procedure in order to quickly implement the provision after it has been adopted.

Opt in, opt out.





Opt-in refers to a procedure for using customer data. In this procedure, companies must obtain the customer's consent each time his/her data is used. The companies may use the data only if the specific customer gives his/her explicit consent, for example by e-mail, phone or text message.

With the opt-out solution, companies use the customer data until the particular customer withdraws consent for their use. Customers must be informed of the way in which the data is used in the company's data privacy notices.

Storage and security of customer data.

Deutsche Telekom stores and processes the data of nearly 60 million consumers in the fixed network and mobile communications segments. The Group is conscious of the responsibility it has in handling this highly sensitive data. Protecting this data is a top priority for Deutsche Telekom. In 2010, the company again took steps to further improve the protection of this data.

Group-wide consent clause for using customer data.

Like many other companies, Deutsche Telekom notifies customers of new or improved products and services. The Group uses existing customer data for this purpose based on strict rules. A customer may be contacted only if he/she has given consent to the use of his/her data for advertising and market research purposes. Permission is obtained in the form of the so-called Group-wide consent clause (KEK)  The customer can decide whether and in what form he/she would like to receive advertisements from Deutsche Telekom. This is done in writing by completing an order form, over the telephone or online. Deutsche Telekom's customers can view and change their consent status at any time on the customer portal at www.telekom.de. When Telekom Deutschland GmbH  was founded, old forms of the consent clause were consolidated in a new system and harmonized. Deutsche Telekom presented the methods used for consolidation and harmonization to the supervisory authority, and both were positively acknowledged.

Data stored at Deutsche Telekom.


Deutsche Telekom stores customer data (inventory data) and data generated during the call, so-called traffic data. The traffic data is technically required for setting up and maintaining the respective call. Subsequently, the data is used for billing purposes vis-à-vis the customer or other service providers. The following traffic data is stored and used to this end in the case of telephone lines (fixed network, mobile communications and Internet), where relevant:

- Call number or ID number of the calling and called lines
- Call start/finish
- In the case of mobile telephony, also location ID, SIM card number and IMEI number
- In the case of Internet usage, the local dial-in node
- Billing data:
 - Start/finish of the individual call
 - Connection type
 - Volume of transmitted data
 - Chargeable services used
 - Information on any credit top-up
- Data on incoming call attempts and notifications is used only within the scope of a corresponding service (e.g., voice mailbox and text messaging applications).
- Message content itself is stored only if the customer authorizes this (e.g., voice mailbox and text messaging applications) or if the relevant services require intermediate storage, e.g., for text messages (SMS) or multimedia messages (MMS)


Traffic data is generated with every call since the data is required to set up or maintain the call. During the billing process, the traffic data that is not relevant for billing is removed. This data is then deleted. This affects in particular traffic data generated as part of a flat rate. This data is not included on the itemized bill.

Billing data is stored for up to 80 days after the bill is sent or deleted immediately after the bill is sent, should the customer so wish. Deutsche Telekom stores IP addresses for seven days to combat spam and malicious code (viruses, worms, etc.). Generally, Deutsche Telekom works on the principle of data economy: storing only as much data as necessary. The company is continually developing its systems and processes in order to protect this data.

Ensuring security for customer data through the “External Workforce Management” program.

Deutsche Telekom works with numerous external partners in the areas of IT, call centers , development and sales. These partners access Deutsche Telekom’s internal (IT) systems in order to perform their contractual duties. The Human Resources Board of Management department has set up the “External Workforce Management” program to ensure the overall security of system access for this purpose. The program ensures that the legal risks arising from the use of external staff are recorded, evaluated and reduced. It also ensures that the identity of external service providers is recorded uniquely in the HR systems. In addition to the legal risks, risks also arise from the external partners’ handling of the data of Deutsche Telekom’s customers and the IT system access needed for this purpose. The program largely ensures that internal employees and (external) partners can access only the systems they need for performing their work and cannot, for example, collect any unrelated data. Support processes additionally ensure that all access authorizations remain activated only while the duties are being performed and that these authorizations are deleted immediately once the contract has been finally performed or in the event of organizational changes.

Ensuring customer data security with cIAM – Identity Management.

The IT program Corporate Identity and Account Management (cIAM)  manages digital identities for internal users and workstations at Deutsche Telekom. The purpose is to standardize identity and account management processes and thereby ensure that only those employees who are currently working in or for the company can access systems and applications. When employees leave the company, the identity management system makes it possible to withdraw their access authorizations for connected systems and applications across systems. When employees move to a new position within the company, the identity management program ensures that the roles/authorizations they used are withdrawn automatically.

In the past, accounts and authorizations were assigned and authorizations revoked locally via a variety of processes and parties. The new procedure applies to all Group units and has been approved by the employee representatives. Implementation has started and will be expanded successively to additional systems and applications in the coming years.

Deleting contractual data in internal systems.

Due to legal obligations, the customer’s contractual data must be deleted at the end of the calendar year following termination of the agreement. For customers who have multiple agreements with Deutsche Telekom, this means that the contractual data must be deleted when all business relationships have ceased to exist. An internal control revealed that the system for fixed network customers lacked a standard process by which the customer’s contractual data would be deleted within the legal parameters. In 2010, purging of the contractual data to be deleted was completed and an automated process introduced, according to which the data is deleted automatically in accordance with legal requirements. In the system for mobile customers, the contractual data was deleted in compliance with the law, with the exception of the customer contact data. Since October 2010, this data is being removed from the system continuously. However, the data will not be completely deleted until the end of 2011, due to technical restrictions. A standard process for deleting this data has also been implemented in this system.

Sustainable customer relationships.

Compliance with legal requirements relating to data privacy in dealing with customers is a matter of course at Deutsche Telekom. The Group not only believes that it is important for its own employees to comply with the rules, but it also makes sure, in particular, that external sales partners do so as well.


Compliance.



Compliance means that companies and their employees comply with rules, laws and policies. It is particularly important to Deutsche Telekom that all employees act in keeping with the company’s values and follow internal rules and laws. The Compliance department supports employees by offering services that they can use in their daily work. In addition to a policy database, the department also offers employees training in compliance. Special portals help employees clarify uncertainties about how to behave and report noncompliant conduct.

As a premium service provider, Deutsche Telekom wants to offer its customers a service that goes beyond the minimum legal standards. This applies to data privacy as well as to customer service in general. With a program that is to ensure integrity when dealing with customers, which was established in 2010, Deutsche Telekom is further developing its sales and service practices. The program has been set up to establish standards of legally and ethically irreproachable conduct and need-based consultation in dealing with customers. The goal is to have customers who trust Deutsche Telekom to ensure proper legal and human dealings and remain satisfied over the long term.

Deutsche Telekom has been implementing the following measures since the fall of 2010 (examples):

- Addition of proper conduct and need-based consulting as a core focus of the existing certification concept for sales partners
- Training for field service employees contracted by Deutsche Telekom, training for employees in call centers 
- Additions to the binding Code of Conduct manual for field service employees contracted by Deutsche Telekom
- Rules of conduct for integrity in dealings with customers as a permanent component of the Code of Conduct for all employees



Manuela Mackert,
Chief Compliance Officer
at Deutsche Telekom AG.



Compliance means that companies and their employees comply with laws, policies and rules of conduct. Are there interfaces between compliance and data privacy?

Of course. Compliance and data privacy have many points in common. First of all, any breach of privacy is also a compliance case. Secondly, the employees in our area are naturally involved in confidential matters and investigations. It is therefore essential that they themselves comply with data privacy requirements. We receive a wide range of reports on noncompliance with the law or policies. People will only give tip-offs if they can be sure that that they will remain anonymous if they wish, and that their details will be always treated as confidential. And only by respecting the privacy rights of persons who are involved directly or indirectly does Deutsche Telekom act in full compliance with the law.

Data privacy is therefore fundamental to compliance for two reasons. It ensures that our whistleblowers trust us. And it guarantees that the rights of the people involved are protected.





I would take this one step further: Compliance is only possible at all if data privacy functions properly. Particularly in our area, therefore, data privacy is not optional but rather an absolute must if we want to make sure that our work for the benefit of the Group and its employees remains successful.

Special topics relating to consumers.

In 2010, Deutsche Telekom again further expanded its services. In doing so, the company took into account data privacy and data security requirements from the very beginning. Deutsche Telekom responded immediately to shortcomings in the area of data privacy and data security and took action to remedy the situation.


In addition, structural changes within the company also led to changes in data privacy and data security practices in 2010.

Changes following the founding of T-Deutschland GmbH.

When the former Group units T-Home and T-Mobile were combined into Telekom Deutschland GmbH  on April 1, 2010, this simplified many organizational aspects of customer data privacy practices and also offered enhancements. Among other things, a new organizational structure for risk management in the Sales department was established which guarantees the security of data in Sales and the implementation of compliance  requirements. The new organizational unit also carries out audits  and certifications  of sales partners. It is also responsible for sales and service monitoring.

Even though many privacy challenges arose along the way to establishing an integrated fixed network and mobile communications portfolio, the integration of the two business areas makes many things easier from a privacy perspective.

A quick look at the situation before the merger shows this clearly: Customers who had both a fixed network line and a mobile line from Deutsche Telekom had agreements with two partners: Deutsche Telekom AG (T-Home) and T-Mobile Deutschland GmbH. In terms of data privacy, this meant that the customer data was stored separately. Exchanging customer data between T-Home and T-Mobile was legally permissible only with the consent of the data subject. Thus, it was not possible to contact the customer in matters relating to both lines at the same time, which was often difficult for the customer to understand.

The situation is now much easier: agreements are now only concluded with Telekom Deutschland GmbH, regardless of whether the customer has a fixed network or mobile line. This also means that only one standard database for storing and processing all customer data will exist in the future. Customer consultants can then access all agreements that a customer has entered into with Telekom. The integration measures relating to the founding of Telekom Deutschland GmbH were put in place in close coordination with the supervisory authorities (in particular with the Federal Commissioner for Data Protection ) where questions relating to data privacy were concerned. An important medium-term project is to standardize the different IT landscapes in the fixed network and mobile communi-

cations segments, i.e., the migration and consolidation of data from the old systems in a shared data memory that meets all requirements for privacy-compliant, secure data processing.

Deutsche Telekom is obligated to adapt the mandatory security concept as stipulated in Section 109 TKG when technological and/or organizational changes occur. This concept focuses on protecting telecommunications secrecy and personal data, protecting telecommunications systems against unauthorized access and shielding telecommunications systems from external attacks and disasters. Due to the merger between T-Mobile and T-Home, which resulted in the formation of Telekom Deutschland GmbH, a modified security concept was developed for Telekom Deutschland GmbH on the basis of the existing individual concepts of T-Mobile and T-Home. In October 2010, Deutsche Telekom submitted the security concept to the Federal Network Agency, which is the competent supervisory authority on the German market. The Federal Network Agency had not yet issued an opinion at the time this report went to press.

Twitter – a new way to provide advice to customers.

Telekom offers assistance, even online, as more and more customers want to be able to contact Deutsche Telekom quickly and without a lot of bureaucracy when they have questions. The company made this possible in May 2010 via the online service Twitter, which it now uses to complement its customer consulting service. Since all conversations through Twitter are publicly accessible worldwide, internal rules were defined for using the communication service for customer consulting in order to ensure data privacy on the customer's part. Employees are required to use social networking services only for establishing contact and for general questions that do not relate to the customer's contract. This helps protect the customer's privacy. If the customer asks for a personal consulting session, the employee is required to switch to other communication methods such as e-mail or letters. Customer Service communicates these rules in local training sessions for the employees.

Rules for using Twitter and other social media for advising customers.



1. Social networks and public forums, such as Twitter, Facebook, etc. may only be used for making initial contact with the aim of switching immediately to another protected and non-public communication channel (e-mail, SMS, post, telephone).
2. No customer advice may be given with reference to specific subscriber lines or addresses via social networks or forums. General product advice is, however, permitted.
3. The number of employees charged with advising customers on social networks or forums is to be restricted. These employees must be given special training in using the media and it is recommended that they also be formally obliged to comply with the data privacy provisions governing the use of social networks and forums.
4. Independently of this, the employees must sign a declaration of commitment to data and telecommunications secrecy and must be sensitized accordingly. This must be done before the media is used.
5. The works council must be informed in advance if employees are to provide customer advice using their real name. Employees cannot be forced to do so against their will.
6. All dialog via social networks must be audited regularly following close involvement of the works council to check that communication activities comply with the provisions of points 1 and 2.
7. At the start of each instance of communication, the customer/potential customer must be notified that they should not disclose any personal data via the public network channels. It is recommended that the notification given be agreed with Group Privacy.
8. No employee entitled to advise customers via social networks or forums may request customers or potential customers via social networks to disclose their personal data publicly or identify themselves.
9. If a customer/potential customer discloses their personal data via the public channels of a social network, communication may not be continued there. This information must on no account be confirmed via this public channel.
10. Employees that do not comply with the aforementioned principles will have their authorization to provide customer advice via social networks withdrawn immediately.



The new Internet service of Telekom Customer Consulting is called “Telekom helps”. Employees provide help and advice on the Twitter online service and Facebook.

Fault clearance in mobile communications via Customer Experience Management.

It is Deutsche Telekom’s declared goal to offer its customers the most highly regarded service. With this in mind, Telekom Deutschland GmbH has developed the Customer Experience Management Tool (CEM tool), an application that will make it possible in the future to analyze faults or problems in mobile communications from the customer’s perspective and initiate suitable measures for clearing an incident or problem. The tool is currently in the process of being approved by the Federal Commissioner for Data Protection and Freedom of Information. Following approval, the company plans to further develop the CEM tool so that it can be used in other areas of technology as well.

Use of geodata by Deutsche Telekom.

Services that access geodata [G] are increasingly becoming part of everyday life. At the same time, these OWS services [G] often trigger further innovative developments. Deutsche Telekom uses map material from providers of geospatial data for its services. For example, the Telekom subsidiary Immoscout24 integrates Google Streetview images into its products. Together with phone directory publishers, DeTeMedien links phone book entries with photos showing birdseye and diagonal views of houses on its telefonbuch.de site. The map material used for this purpose is freely accessible on the Internet. The customer has the option of refusing to allow his/her address to be linked to the map material at any time. In 2010, Deutsche Telekom highlighted information on this option to withdraw permission in the interest of transparency and consumer-friendliness. In particular, the company added separate information to the privacy notices at “telefonbuch.de”, “gelbeseiten.de” and “dasoertliche.de”.

Deleting data from T-Shop replacement devices.

Customers can ask their T-Shop for a replacement device when their own mobile phone, for example, is being repaired. One customer complained that the data of a previous user was present on one of these devices. The process of erasing data from mobile devices provided by Telekom Shop Vertriebsgesellschaft (TSG) was subsequently reviewed and audited via spot checks. The result was that the deletion process was well known and well documented. Minor documentation gaps existed only in one shop, while all other shops complied with the process. In the shop that came to Telekom’s attention, the employees had to attend another special training session. Shop audits involving spot checks are carried out on a regular basis.

Erasing data from devices returned for repair.

When a mobile phone is brought to a T-Shop for repair, the shop sends it to the manufacturer. The customer usually receives another repaired device from a replacement pool. There are binding rules for the deletion of data from these devices. The customer agrees to delete personal data from his/her mobile phone before handing it over. Since the customer may not always be able to delete the data due to the technical defect, the manufacturer is also contractually obligated to delete any data that may still be stored on the device. Individual customer complaints have shown that not all manufacturers delete the data consistently even though Deutsche Telekom has clearly defined the applicable data privacy requirements. Deutsche Telekom has also begun to review the entire deletion process for weaknesses independently of these incidents.

Misuse of T-Online IDs.

Several public prosecutors' offices have initiated investigations because in 2009 the IDs of T-Online customers fell into the hands of fraudsters, presumably by dishonest means (e.g. phishing). The perpetrators used the IDs to purchase load keys through the Softwareload and Gamesload portals. These are activation keys that make it possible to download software from the Internet.

The customers affected had no idea why charges for software downloads appeared on their bills. Telekom asked its customers to press charges for fraud. The resulting investigations were supported by Telekom from the very beginning. The Group's internal investigations showed that there is no reason to believe that employees were involved in the incidents. In recent years, there have been repeated cases of fraud based on identity theft or social engineering. Perpetrators try to obtain information such as access data from their victims through social networks. In October 2009, Telekom took technical measures to prevent fraud involving telephone bills. Customers can now select the payment type "phone bill" only over their own line. However, it is not possible to completely eliminate fraudulent purchases, e.g. using credit cards.

Disclosing access data on a social network.

In November 2010, Deutsche Telekom posted an online notice that is visible when logging into T-Online accounts. It notifies customers of a substantial risk of misuse when they disclose their personal access data on a social network. The reason for this notice was a new function on a social network, which gave its users the opportunity to load their address books, such as the T-Online address book, to the network. The service provider compares the data thus obtained with its internal database. In doing so, it can determine who is and who is not (yet) a member.

Deutsche Telekom views such comprehensive disclosure of personal data to be impermissible as it enables third parties to access the customer's personal account at the Telekom Customer Center. This would give them access to functions such as e-mail, online banking and all contractual data. In addition, this behavior is in breach of contract, since the the General Terms and Conditions do not permit the disclosure of personal access data. In addition, linking data in this manner is cause for concern insofar as sensitive personal data of third parties is transmitted without the customer being notified or having given permission. Deutsche Telekom sees this as a violation of legal provisions under federal data privacy laws. The assurances of operators of some social services that they would not use this data for internal purposes do not change this assessment.

Collecting movement data for detecting speeds.

Manufacturers of navigation equipment have an interest in providing precise congestion forecasts, which they offer as additional services. This makes it possible to optimize traffic flow in order to avoid or reduce congestion. To draw up forecasts, the service providers like to use the movement data of mobile phones. For this purpose, mobile communications providers offer data to navigation system manufacturers as a wholesale service. Since this data can, in principle, be traced back to a certain mobile line and thus to a certain person, an anonymization solution must be found which protects the personal data of the mobile user. Data misuse must generally be ruled out, such as taking action when speed limits are exceeded. Two competitors already offer these services, and Deutsche Telekom would also like to provide them.

The ways in which the data must be rendered anonymous were discussed with the Federal Commissioner for Data Protection. The question of how long and in what form information (so-called localization data) that can be used to draw conclusions about the movements of mobile phones should be stored or made available to navigation system operators was also clarified. The solution found was approved by the Federal Commissioner for Data Protection. The product is expected to be launched during the course of 2011.

Dunning procedures of the law firm Seiler.

If a customer fails to respond to warnings by Deutsche Telekom for outstanding invoices, the attorneys with the law firm Seiler handle enforcement of the outstanding customer receivables.

The competent state commissioner for data protection in Baden-Württemberg drew Deutsche Telekom's attention to various practices by the law firm Seiler that, in the agency's view, were objectionable under data privacy laws. These included, for example, the form of the notice to the data subjects in question and the deletion periods for the debtor's data. In a discussion with the state commissioner for data protection, Deutsche Telekom and the commissioner agreed that the Federal Data Protection Act [§ 6](#) also applies to law firms as long as attorney-client privilege is not violated. The aspects criticized by the state commissioner for data protection were clarified. In order to make it easier for the customer to exercise his/her right to information under Section 34 of the Federal Data Protection Act, Telekom Deutschland decided at the suggestion of the supervisory authority that in this matter disclosures by the law firm Seiler do not fall under the attorney-client privilege. The attorney can now disclose information on the collection data on Telekom Deutschland's behalf. The law firm Seiler's notices to the liable parties were also updated.


Business Customers.

Cloud computing and dynamic computing.

The cloud computing market is a market with high growth potential. With a volume of roughly €13 billion worldwide in 2009, various analysts predict an increase to €45 billion, and some even to €150 billion by 2013. Deutsche Telekom has identified the development of this growth market as a core element in its strategy "Fix – Transform – Innovate", which was presented in March 2010. The company plans to meet customer needs with new products and participate in the growth.

Cloud computing offers customers numerous advantages, in particular enormous cost savings. For providers of such solution concepts, cloud computing presents challenges in technical provision and in guaranteeing a high level of security.

Deutsche Telekom offers different cloud computing solutions under the concept of dynamic computing. In its portfolio, the company is currently focusing on the business customer segment. Further information can be found at <http://geschaeftskunden.telekom.de>

T-Systems supplies services of this type both for internal requirements and for Deutsche Telekom's business customers. However, the security of the cloud computing services is a critical factor in success. Security is guaranteed by Group-wide, interdisciplinary cooperation between different departments within Deutsche Telekom. Thus, IT Security develops the technical security requirements. Data Privacy ensures that priority is given to protecting the processed data. T-Systems incorporated Group-wide expertise as early as the phase of developing the dynamic computing services. The company examined the current risks and threat scenarios for the dynamic computing platform down to the last detail and established a comprehensive technical solution. Deutsche Telekom designed and implemented a secure overall cloud architecture in which the individual customer applications can be fully and securely separated from each other. Data Privacy and IT Security are continuously assist with the implementation and further development process within the framework of the Privacy and Security Assessment (PSA)  procedure (see page 33, PSA procedure). This applies not only to the platform itself but also to all applications running on it. Specialists support all migrations from the classic operating environment to the cloud via the PSA process. This ensures that the security documentation (standardized data privacy and security concept) for the application concerned is always up to date.

Cloud computing and dynamic computing.

In cloud computing, information technology infrastructures that were previously provided in a customer's building, are combined into central data centers. Computing capacities as well as data storage, software and programming environments, for example, are offered as services and made available dynamically over a network, adapted to the customer's specific needs. Customers, particularly in the business customer segment, require much less IT infrastructure and can thereby achieve substantial cost savings, among other things. The customer requests a service from a provider, such as network bandwidths, computing and storage resources and adjusts them on demand. The rental price is geared toward the capacities that are actually used.

Cloud computing offers business customers additional security:

- Providing data centrally in a cloud can reduce the number of existing copies of data records, since they are now stored in the cloud rather than individually on each computer
- When data is stored in only one location, more efficient access management can be carried out

Cloud computing also provides consumers with greater security, offering savings potential at the same time:

- The cloud servers where the data is stored are much better protected than most personal PCs and laptops. Most providers (including Deutsche Telekom) prepare backups in order to restore the data in the event that a server fails
- Customers save money for additional storage space on their home PCs and smart phones
- Everyone can easily access their own data from anywhere

As one of the largest suppliers in the industry, Deutsche Telekom has taken an active role in discussions and developments relating to the security of cloud computing [G], for example as part of BITKOM's [G] activities. Recently, the company commented on the draft of the „Minimum Security Requirements of the BSI for Cloud Computing Providers“, together with industry representatives. In addition, Deutsche Telekom believes that it is necessary to set up a high-level security situation center for the industry. The company is also in favor of security certification by the German Federal Office for Information Security (BSI) for security services in the cloud.

De-Mail.

E-mails are the number one medium for written communications. Users around the world send and receive 247 billion electronic messages every day. But e mail reaches its limits when the message content is confidential or if it is necessary to prove it was received at a particular time. It is not always guaranteed that the sender displayed is indeed the actual sender or if a message might have been intercepted or manipulated on its passage through the Internet. This is why there are certain limitations on the suitability of e-mail for legally binding transactions, for example in official and business correspondence.

As part of its high-tech strategy, the German federal government has introduced a bill that will set out both the legal basis and the technological framework for the electronic communications of legally binding documents via De-Mail. The law will be adopted this year. Companies will then be able to get certified as De-Mail providers by the Federal Office for Information Security (BSI). The office will monitor compliance with the strict data privacy provisions.


De-Mail is an enhanced form of e-mail that enables the simple, secure and verifiable exchange of electronic messages between private users, businesses and public authorities. It combines the advantages of e-mail with the reliability of a registered letter. Every sender is known to the De-Mail provider thanks to a personal initial identification. If required, users can receive a qualified signed confirmation that a message has been sent, stating to whom it was sent and when it was delivered to the recipient. The whole range of business and administrative communications, such as offers, contracts, invoices and reminders, can therefore be carried out electronically, conveniently and without a change of media. This substantial saves the cost of printing, envelopes, postage and delivery.

T-Systems has completed numerous projects in which it has acquired extensive experience in connecting companies and public authorities to De Mail and integrating their business processes. For example, in the T-City Friedrichshafen the company has already linked up more than 40 enterprises, chambers of trade and commerce and public authorities via De-Mail. The Ministry of the Interior tested De-Mail in the city for six months up to March 2010. The aim was to create a real-life scenario with as many applications for De-Mail as possible.

De-Mail offers security that goes beyond that of regular e-mail:

- Secure dispatch: De-Mail offers a much higher level of security and allows the dispatch and receipt of a message to be verified. When users want to open a De-Mail account, they must clearly identify themselves personally on a one-time basis.
- Secure data transmission: It is mandatory that data transmissions be secure. The tried-and-tested SSL encryption process [G] known from the Internet (websites with the URL https://) will therefore be used, among other things. The participating servers set up a direct connection and must authenticate themselves to each other.
- Secure delivery: The most important aspect of De-Mail is the secure receipt and dispatch of messages or documents on all levels – similar to today's classic letter. To be certain that the De-Mail [G] is not lost, the sender receives verification by a qualified signature that the message was sent and when it was received in the recipient's mailbox. To make manipulation attempts visible, the messages are also provided with a checksum. The De-Mail provider calculates this checksum from all of the message's content, similar to how one can calculate a much shorter cross total by adding the individual digits of a long number. If a digit is changed later on, the cross total is also changed, indicating a modification. This check is carried out by the receiving provider, in principle, each time a message is transmitted.

Smart energy – from smart meters to smart grids.


Intelligent power grids (smart grids ) are capable of regulating the production of energy on the basis of measured load. Additional local energy producers, such as cogeneration plants, solar power plants or wind turbines, may be added or removed as required. The conventional basic load suppliers (such as coal-fired power plants) can be used more effectively, thus reducing CO2 emissions. Smart grids require the networking of electrical appliances of private households with the relevant electricity supplier and an exchange between the two systems. This makes it possible to identify usage peaks and develop rules with regard to when energy is efficiently provided for appliances. On the whole, it is clear that secured and privacy-compliant data processing and transmission is particularly important here. Manipulating the control cycles between recording energy consumption and controlling energy production would have a far-reaching impact. Likewise, customers must to a large extent maintain the ability to control the data affecting them. Neither approach was a central part of the solution in the traditional power supply models. Deutsche Telekom is therefore investing its entire expertise in securing and designing infrastructures of this type, thus creating important elements for future-oriented power supply.



Measuring power consumption and usage patterns in an energy conscious manner – smart metering makes it possible.

Smart metering.

Smart metering makes it possible to record and process the consumption of electricity, water, heat and gas at specified time intervals. Consumers receive an overview of their consumption and can thus adjust their energy behavior, act quickly and in a timely and energy-conscious manner and thereby conserve valuable resources. There will also be corresponding pricing models in the future.

Technologies such as smart metering  (smart, i.e., networked meter units for electricity, gas, water and heat) are based on networking. To achieve this, power suppliers have been obligated since early 2010 to provide end consumers with monthly, quarterly or semiannual bills, if requested. Since 2010, the legislator has stipulated the installation of smart meters in new and renovated buildings.

With Smart Metering & Home Management (also see <http://www.telekom.de/smartmetering>), Deutsche Telekom offers a modular data communications solution. This solution is aimed at the housing industry, meter operators, utility companies, sales organizations and distribution network operators.


Since these new applications mean that a great deal of personal data is exchanged, guaranteeing a high level of data privacy and data security is particularly important. Data Privacy and IT Security have reviewed the level of security and data privacy in place at the companies involved. During the course of the review, they found out that responsibilities were not described clearly enough in certain contract constellations. This was remedied by drawing up a sample draft agreement for the commissioned data processing of internal and external partners. In addition, all necessary technical measures were taken to guarantee the greatest possible protection. For transmitting the data from the smart meters to the utility companies, a data privacy concept documents who is able to read which data and how this data is processed. The protection and privacy-compliant processing of customer data was confirmed by Data Privacy and IT Security during the course of releasing the data privacy concept.



Special issues relating to business customers.

Recommendations in Das Örtliche.

DeTeMedien and partners in the editing and publishing communities for Das Örtliche, Das Telefonbuch (phone directory) and Gelbe Seiten (Yellow Pages) would like to have customer ratings included with the contact details of a service provider. The function, which is already implemented, was deactivated after the competent regulatory authority intervened.

The regulatory authority criticized the fact that those people to be assessed were not informed about the introduction of the recommendation function and their response options (e.g. opt-out  option, editing of entries). After deactivation of the function Deutsche Telekom advised DeTeMedien on the configuration of this function in compliance with data protection regulations. In multiple talks, the options for implementing the function and for meeting the requirements were discussed with the competent regulatory authority. The details of implementation are currently being prepared. In terms of implementation, the focus is on the content of the preliminary information sent to the party receiving a recommendation. This party must have the opportunity to contradict. This procedure is generally recognized as the opt-out solution.

Employees.

Protecting employee data involves two aspects. First of all, employee data must be protected against unauthorized external and internal data use and processing. Secondly, employee data privacy also covers the requirements and conditions for authorized internal use, such as in investigating criminal acts. A company is obligated to investigate possible misconduct in order to prevent possible violations of third-party rights (e.g., customers, other employees) or to help clear up a matter.

Legal provisions.

In August 2010, the German government passed a draft that provides for changes in employee data privacy rules. The first reading of the bill in Parliament took place in February 2011. The key point of the amendment to the law is to establish clear rules on how a company can investigate employee misconduct and what it is forbidden to do. Personalized, systematic test procedures, known as screenings, will only be allowed to a very limited extent according to the draft. Preventive data comparisons may be carried out only in anonymized or pseudonymized form, i.e., if conclusions about the individual person cannot be drawn or can only be drawn to a limited extent. Following the past espionage incidents, Deutsche Telekom ceased making comparisons of personal data for revealing anticipated or possible personal misconduct even before the draft. The company welcomes the fact that this rigorous procedure is now to be established by law and will require anony-

mization or pseudonymization for such measures. A project group has already been formed for implementing the new provisions within the Deutsche Telekom Group. This team identifies the Group areas, processes and policies that need to be modified on the basis of the new provisions and initiates their implementation.

Agreements and guidelines.

Within the reporting period, Deutsche Telekom has carried out different measures relating to employee data privacy which prevent misuse, protect the personal data of the company's employees and ensure that different interests are reconciled.

- With the “**Group Works Agreement on Preventing Abuses in IT Systems,**” Deutsche Telekom and the works council have agreed on preventive measures that are intended to prevent employees from improperly using IT systems from the very beginning. These measures are primarily technical system restrictions that limit a user's possible activities to the necessary steps from the outset.
- A “**Human Resources Data Privacy Guideline**” guides employees and managers through the complex issue of employee data privacy and informs all employees of their rights and how to assert them. The guideline was published on Telekom's intranet site.

Special topics relating to employee data privacy.

Incorrect workflows in the HR area.

Deutsche Telekom employees can use a computer system to handle their HR affairs, such as timekeeping, viewing target agreements or travel planning. Changing a service within this system resulted in incorrect workflows. As a result, the target agreement proposals of managers were temporarily available for downloading by other employees. The error was remedied immediately upon its discovery. The parties affected received letters of apology.

Unjustified access authorizations in the HR area.

Deutsche Telekom employees who can access customer data or data of employees are given authorizations for this purpose. These authorizations are assigned on the basis of a double-checking principle. This means that employees cannot issue their own authorizations but must receive approval from at least one other person. In Human Resources, one system did not meet the organizational requirements. In isolated cases, employees received authorizations to access data that was not required in the performance of their work, despite the principle of double checking.

This situation became known during the course of a data privacy audit of the department. Deutsche Telekom immediately revoked the impermissible authorizations from the employees involved. At the same time, the principle of double checking in assigning authorizations was redesigned and expanded in this department. The discovered vulnerability was thus eliminated.

Transmitting log information within the scope of commissioned data processing.

To perform their own quality assurance and meet legal requirements for commissioned data processing (Section 11 of the German Federal Data Protection Act), T-Systems business customers need overviews showing the access to their data stocks by the service provider. These overviews have been and are being made available to the customer in various forms on request (online or as documents).

In connection with a review, it was found that most of the overviews had been handed over in non-pseudonymized form, even though it was not absolutely necessary to provide the information with the employees' real names in order to meet the customers' monitoring obligations. Together with the specialist units, a new, standardized reporting procedure is being developed which will be made available to T-Systems as a whole centrally. Until this procedure is introduced, individual solutions will be adopted to ensure a comprehensive aliasing of information.

International developments.

Legal provisions.

Companies were able to express opinion on the planned amendment to the European data privacy directive of 1995 up until January 15, 2011.

Among other things, the amendment is aimed at dealing with the effects of new technologies in data privacy, strengthening the rights of citizens, improving the data privacy situation within the European Union and achieving a more effective means of enforcing the rules. Deutsche Telekom participated in the discussion and welcomes, in particular, the planned harmonization of data privacy requirements and the plan to achieve a high level of protection for data that is transmitted to countries outside the European Union. Deutsche Telekom also welcomes the idea of introducing a data privacy certification at EU level. In addition, Telekom is in favor of, among other things, allowing companies to use customer data for purposes that are not contractually necessary only if the customer concerned has given permission (so-called opt-in solution ). Telekom deliberately takes a position that strengthens customer rights, while many companies within the industry wish a less restrictive approach to the handling of customer data.

Measures for international cooperation.

International cooperation within the Group.

Deutsche Telekom now earns over 50 percent of its revenue outside Germany. It is active as an internationally operating enterprise in various countries in and outside the European Union. Against this background, data privacy is an important international concern for the company, one that must be dealt with at a high level and across national boundaries.

In the relevant countries, different data privacy provisions and laws apply, which in the European Union are largely derived from the European Data Privacy Directive, but which nevertheless vary from one country to another. In countries that are not European Union members, the differences are even greater. Against this background, close international coordination within the Group is important in order to ensure a uniform, high level of data privacy within the company even in the face of non-uniform data privacy requirements.

To achieve this, Deutsche Telekom continuously improves its international cooperation within the Group. Thus, instruments such as standards for data privacy auditing of IT systems or online training courses for international use are being developed.

As early as in the 2009 Data Privacy Report, Telekom announced that it would aim for closer cooperation internationally in 2010. In 2010, the company expanded and introduced initiatives for ensuring international data privacy in the customer's interest.



Deutsche Telekom is continuously improving its international cooperation.

The **International Privacy Circles (IPCs)** form the basis for this. These circles have met once a year for the past several years in each of the global units of Deutsche Telekom, which are combined into three regions. The privacy officers of the national companies in the three regions of Europe/Africa, the Americas and Asia/Pacific meet to share expertise and opinions. The Privacy Circles are also aimed at establishing a standard level of knowledge, for example in international data transfers as well as international developments on both the regulatory and technical levels.

The **International Privacy Task Force** was also formed in late November 2010. In contrast to the International Privacy Circles, the task force examines data privacy issues in small working groups from the perspective of operations in the participating countries. Common solutions, which flow into the Group's international data privacy framework, are developed on the basis of experience and requirements. Among other things, legal requirements for international data transfer within and outside the European Union, developments relating to employee data privacy, procedures for evaluation the data privacy of specialist unit projects and the expansion of the data privacy intranet to form an information and training platform are discussed.

Cooperation outside the Group: Participation in the "Mobile Privacy Initiative".

In addition to its participation in European and international public committees and institutions involved in developing internationally binding data privacy standards, Deutsche Telekom also works on initiatives supported by the industry. Thus, the company supports the "Mobile Privacy Initiative" initiated by the GSM Association (GSMA) [G] and established in January 2011. The GSMA [G] is a global mobile communications association that was founded in 1987 and counts over 800 mobile communications providers and companies as its members. The "Mobile Privacy Initiative" is aimed at obligating leading mobile communications providers, terminal equipment manufacturers and developers of mobile software applications to adopt a common data privacy standard and to provide customers with clear and transparent information about what data is collected and for which purposes. Thus, users of location-based services – i.e., services that access the user's current location – need to be informed about software and asked for the release of this information if this is necessary in order to provide the service. In addition, the scope and use of this data should be described clearly and transparently. This is a first step toward a common framework, particularly where users outside the European Union are concerned, where in many cases privacy laws either differ widely or are non-existent. The "Privacy Principles" published in January 2011 contain the common data privacy standards. These principles form the basis for detailed, product-oriented policies aimed at establishing customer-friendly standards at all levels of product development. The goal for 2011 is to develop these specific policies for data privacy. A first draft of a policy for developers of mobile software applications already exists and is expected to be adopted in 2011. This would be an enormous success, since it would also obligate companies in countries outside the European Union to adopt stricter data privacy requirements.


Special topic relating to international developments.

Everything Everywhere – United Kingdom.

On July 1, 2010, Deutsche Telekom and France Telekom merged their subsidiaries in the United Kingdom to form a joint venture named "EverythingEverywhere". From a data privacy perspective, the central concern was migrating the systems containing personal data. Specifically, this meant complying with the requirements of data privacy laws and the company's internal requirements. Measures for the transfer of operations from a data privacy perspective were also described. The specific implementation of the requirements has begun and will be completed in 2011.

Systems and processes.

With its much-discussed data incidents, 2010 has demonstrated that data is exposed to continuous danger. Absolute data security is not possible. We can only work on making processes and systems as secure as possible and always remain one step ahead of attackers. In this regard, Deutsche Telekom takes on the challenge afresh every day to continuously test its systems and processes in order to protect customer data and to protect its own assets, and it continuously further develops these systems and processes. With certifications  from independent institutes, Deutsche Telekom offers proof that it meets the relevant norms and standards. Experts confirm that the company maintains an exemplary level of security.

In 2010, Deutsche Telekom consolidated and standardized its security and data privacy concepts and rules, standardized and coordinated them intensively, thus further strengthening the Group's level of security. One result of these efforts is the Privacy&Security Assessment (PSA) . It ensures that the security and data privacy requirements are taken into account in the early phase of developing new systems and applications.

Numerous data privacy and data security audits form an integral part of the in-house monitoring system. These audits complete the full set of preventive and reactive measures that are used to protect confidential information and personal data at Deutsche Telekom.



Thomas Tschersich,
head of IT Security
at Deutsche Telekom.




Where does Deutsche Telekom stand today when it comes to data security? And where will it stand in the future?



For many years, we danced a classic two-step when it came to developing new products in the telecommunications and IT industry. First we developed a product, then we made the finished product secure in terms of protecting it against unwanted data extraction – this is inefficient and often leads to compromises in which functionality takes precedence over security. Deutsche Telekom takes a different approach. Years ago, we began integrating security as early as the preliminary planning stage of products and implemented them concurrently with development. We now participate in the entire process up to the finished product, which makes us one of the pioneers in our industry. We see security as a design criterion, and it has long ceased being viewed as an add-on function.

Our goal is to maintain security at a high level in existing products and entire systems, to keep pace with technological development and remain always one step ahead of new criminal ideas. Many external experts confirm that we serve as an example in this area. We plan to resolutely expand this position. However, that's not all. We are also working on establishing a new standard for secure products and thereby further propagate or philosophy of "security by design". Of course, we cannot do this alone. Establishing this type of standard throughout the telecommunications industry will work only if others get on board. We are working on this.

Deutsche Telekom's security management practices.

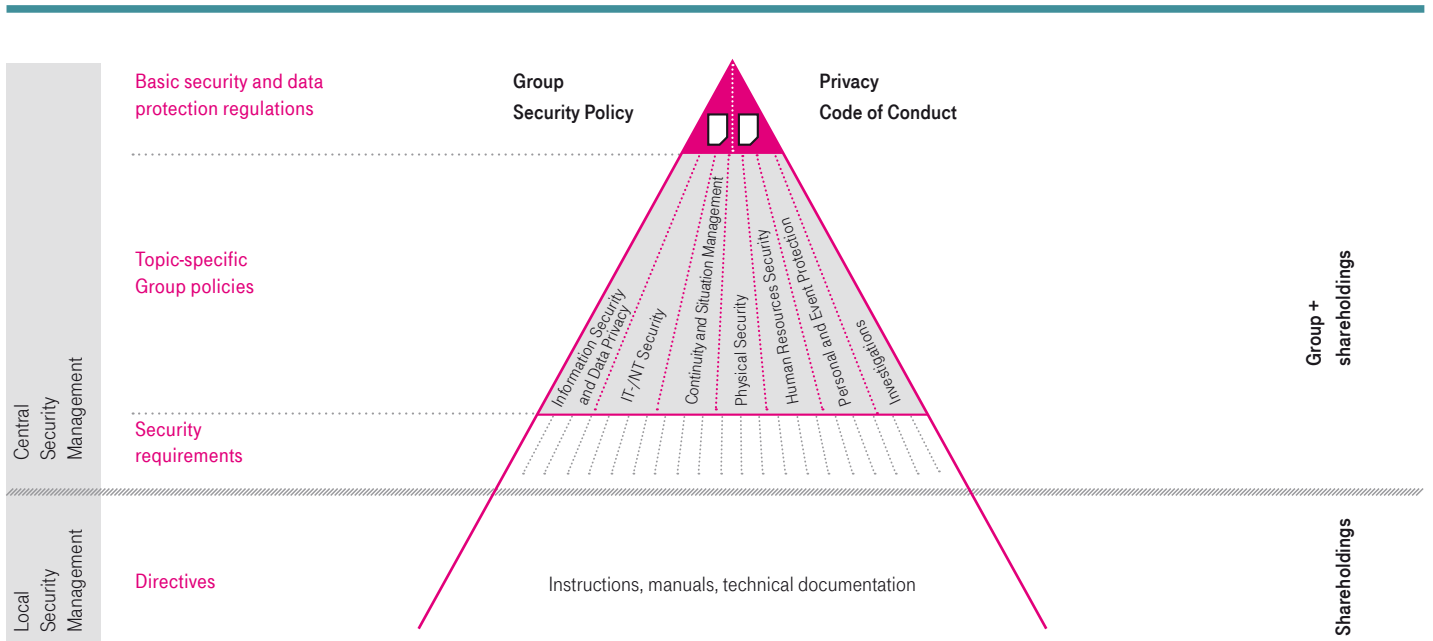
According to Section 91 of the German Stock Corporation Act (Aktien-gesetz), Deutsche Telekom is obligated to take suitable measures to identify developments that could jeopardize the company's existence at an early stage. This obligation includes, in particular, an internal monitoring system. Violations of data privacy and security provisions must be ruled out as far as possible. For this purpose, Deutsche Telekom continuously further develops its Group-wide security management system, among other things. In 2010, it again adapted the system to the latest developments and expanded to other parts of the Group.

Apart from data privacy, a key component of the security management system is Deutsche Telekom's Central Security Management department. The Central Security Management department  consists of the three

organizational units Group Security Policy (GSP), Group Business Security (GBS) and Group Service IT Security (GIS). It governs the interaction between all functions within the Group that are responsible for ensuring security. In December 2010, Central Security Management was certified  according to ISO  27001 (see page 37) and thus complies with the most important international standards.

The security and data privacy management system was continuously refined in 2010. Among other things, a mandatory standardized Group-wide set of rules which harmonizes the security and data privacy regulations was established as its operational basis. This basis for security and data privacy regulations is illustrated in the following diagram:

Regulatory framework for security and data privacy.



At the top of the regulation framework are the two basic documents on security and data privacy within Deutsche Telekom: The Privacy Code of Conduct [G] contains the internal requirements for dealing with personal data (general data privacy provisions), while the Group Security Policy includes the Group's security-relevant principles. The Privacy Code of Conduct and the Group Security Policy also form a kind of "Constitution" for Group-wide data privacy and security practices.

These provisions are further specified by seven additional topic-specific Group policies:

- Information Security and Data Privacy
- IT/NT Security
- Continuity and Situation Management
- Physical Security
- Human Resources Security
- Personal and Event Protection
- Investigations

These Group policies transparently set binding standards that are based on the international standard ISO 27001 in order to guarantee a sufficiently high and consistent level of security and data privacy within the Deutsche Telekom Group (see page 37).

The Central Security Management regulations, which were revised in 2010, are being successively implemented in Germany and in the international holdings. Local regulations supplement and complete them in the individual units. The policies have already entered into force in Deutsche Telekom AG and T-Deutschland GmbH. Implementation in all relevant Group companies is expected by the end of 2011.

Early warning systems.

As the largest supplier of communications services in Germany, Deutsche Telekom is a favorite target of hacker attacks, which continuously present new challenges. The company responds to these challenges with the help of an early warning system aimed at determining information about attackers, identifying new attacks and developing better defense strategies.

In principle, a large pool of data sources and data material available for analysis improves an early warning system. The strict legal standards of telecommunications secrecy and data privacy were taken into account as early as the conceptual design stage. By establishing the early warning system, a picture of the security situation on the Internet was generated, one that is oriented specifically toward the risks and needs of the company. The objective is to protect customers and confidential data of Deutsche Telekom as best as possible against dangers on the Internet with the aid of the information gathered by the company and combining this information with the generally available manufacturer information. Furthermore, this approach makes it possible to identify and implement necessary adjustments to the security mechanisms at an early stage.


Honeypots.

So-called honeypots [G] are a central component of Telekom's early warning system. These are isolated server systems which are accessible from the Internet but which are not connected to Deutsche Telekom's real systems. Honeypots are thus independent of Deutsche Telekom's infrastructure and cannot become a threat even if they are compromised. The honeypot systems are self-learning, which means that they record and analyze unknown attacks and take them into account for detection later on. Deutsche Telekom began building honeypot systems of this type in April 2010. Other providers use comparable systems. For this purpose, Deutsche Telekom maintains intensive dialog, among other things, within the "Antibotnet Initiative" sponsored by the German government, which is aimed at reducing the number of infected consumer computers.

Since the honeypots were set up, they have identified over 500,000 hacker attacks. Deutsche Telekom has used the insight thus gained about the types and methods of attack to prevent successful attacks on its real systems and to notify customers whose computers are part of a botnet and are thus under external control.


Deutsche Telekom continuously improves these and other early warning systems in order to guarantee the best possible protection for its own data and that of its customers. The efforts are successful. Up to now, the honeypot systems have not revealed any vulnerabilities to attack from the Internet in Deutsche Telekom's systems. At the same time, a honeypot enhancement is being tested specifically for analyzing attacks on mobile networks.

Telekom CERT.

Deutsche Telekom's Computer Emergency Response Team (CERT)  operates an internationally oriented management system for security incidents relating to all information and network technologies of the Deutsche Telekom Group. It forms the central point of contact for reporting incidents and establishes mechanisms for the early detection of attacks on internally and externally accessible systems. CERT's main tasks are:

- Vulnerability and Advisory Management – VAM
- Coordination of measures for security-relevant incidents (incident management) or incidents related to customer data
- Internal issuing and evaluation of warnings of newly identified vulnerabilities
- Group-wide early warning and identification of technical attacks on the network infrastructure
- Represents Deutsche Telekom AG on national and international committees (e.g., the global CERT umbrella association FIRST, Forum of Incident Response Teams).

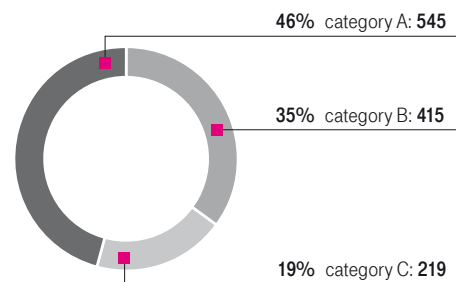
In 2010, the team issued alerts on 1,135 vulnerabilities in software components used within Deutsche Telekom and provided information about them internally. The vulnerabilities range from security gaps in web server technologies to vulnerabilities in operating systems. Where solutions are found as early as the time the vulnerabilities become known, Telekom CERT communicates them as well.

Telekom CERT sees a further serious threat in so-called driveby exploits , in which a user's computer becomes infected simply upon viewing a website. Driveby exploits take advantage of vulnerabilities in web browsers (especially older Internet Explorer versions) and browser add-ons.

Privacy and Security Assessment (PSA).

The Privacy & Security Assessment (PSA) procedure was introduced to Deutsche Telekom Germany in 2010. This procedure replaced the previous approval procedures for data privacy and technical security and integrated them into a joint procedure. In taking this step, the company used experience from individual units which had already used the method. Deutsche Telekom is one of only a few companies worldwide that practices the meshing of data privacy and technical security.

PSA project categories.



The PSA procedure creates a transparent and documented process that efficiently provides a high level of security and data privacy for complex and critical products and services. This takes place as early as the development phase and not only shortly before or after new products and services are launched. Based on a questionnaire, the data privacy and security relevance of a project is determined according to the categories of A, B and C right at the start of the process. The depth of support is then based on this. The extent of the consulting and support provided by the Data Privacy and Data Security units increases with more critical projects (A projects). Standard requirements are used for less critical projects (B projects). The PSA procedure can be used to implement security and data privacy requirements quickly and efficiently. In the end, this standard makes it possible to determine that a project has no relevance for data privacy/security (C projects). Optimum use of resources by everyone involved is thus ensured.

This procedure is currently the only one of its kind within the telecommunications industry. It serves as a model for regulatory authorities and standardization committees.

In 2010, around 1,200 projects were reviewed under the categories A, B and C using this procedure. Nearly 960 projects came under categories A and B and were thus handled according to the PSA procedure. The Group provided support for the development of dynamic computing services. Data Privacy and Data Security also assisted with preparations for converting the telephone network to IP-based telephony.

Such early and continuous integration of data privacy and data security offers Deutsche Telekom's customers a uniformly high level of data privacy in all products and services. In addition to enhancing and optimizing content, the procedure is expected to be also introduced in international Group units in 2011.

Privacy by Design.



Privacy by design means that the protection and careful use of personal data must be taken into account as early as the development stage of new products and services. Companies thus meet the legal requirements of data privacy at the earliest possible stage. In addition, they can make data privacy a differentiation criterion by taking different user needs into account when approving personal data as early as the product development phase. In practice, for example, functions for exchanging sensitive data are developed when designing a smart phone application. It must be possible to decide which specific data is to be exchanged.

Security by Design.

Security by design is a concept that is being used increasingly at conferences and in discussion forums, even though it hasn't yet been established as a definitive term. It means that companies must not only ensure the protection of personal data, but also that this data is processed securely and is protected against unauthorized access. Therefore, a guiding principle of product development must be to take security requirements into account very early on. This avoids expensive improvements later on and maximizes the level of security. The products are then as secure as technically possible and not only designed as securely as necessary.


Privacy and Security by Design.

Privacy and Security by Design. In the future, we can expect a procedure that takes both aspects into account to become a standard procedure.

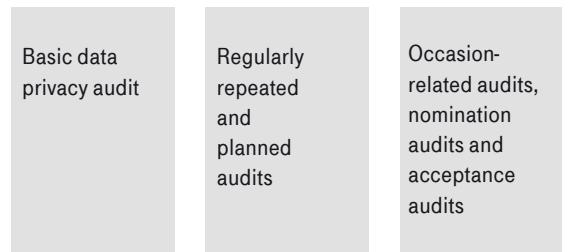
Audits and certifications.

Regular audits and certifications relating to data privacy and data security take place with the Deutsche Telekom Group. For this purpose, Deutsche Telekom uses a system of audits and certifications by external agencies and internal units. The company thus serves as a model within the telecommunications industry: certifications for company units are still the exception within the telecommunications sector.

Categories for audits.

Deutsche Telekom's audits  for internal control and monitoring of how data privacy and data security requirements are implemented fall into three categories:

Deutsche Telekom's audit categories.



The basic data privacy audit is carried out at national as well as international level. It checks whether Group Privacy requirements have been observed. The second category covers audits of systems such as IT and products. The audit also checks whether Deutsche Telekom's organizational structure and internal processes meet the latest data privacy and security requirements. The third category covers special audits occasioned by incidents or suspicions and acceptance audits for approving prioritized projects. This means that before a project such as a market launch of a new product is begun in actuality, an audit is performed to check whether it meets all required and necessary data privacy and security requirements. As part of nomination audit, new sales partners are audited before business relationships are entered into. Existing sales partners are audited through a regularly repeated audit.

Audits performed.

In 2010, the Internal Auditing, Group Privacy and Central Security Management departments alone performed around 450 audits on data privacy and data security. A large portion of the data privacy and security audits were for IT and network technology. These audits are aimed at securing the information and network technologies used within the Group. For example, the implementation of the authorization, data privacy and security concepts are examined throughout the Group in order to identify any gaps. Such gaps can arise due to security deficiencies in software solutions, which are identified and remedied together with industry partners.

Audit.



An audit is a general examination procedure that is used, for example, to evaluate systems, processes, organizations and locations for compliance with requirements and policies.

To obtain a certificate, the company is tested in an audit conducted by external auditors to see whether its internal systems and processes meet the requirements for receiving the certificate. Once the certificate has been obtained, these audits must be repeated at regular intervals (every one to three years).


In addition to audits performed by external parties, companies often perform various internal audits as well. They use these audits to check compliance with their own internal requirements and policies.

The audits also focus on checking whether technical and organizational measures and processes relating to data security and data privacy have been observed. The remaining audits go to guaranteeing general security such as personal and physical security measures. This includes audits to check compliance with fire safety requirements or access regulations.

The results of these audits help ensure a high level of data privacy and security by either verifying the effectiveness of the internal systems and processes or identifying and helping to correct any vulnerabilities at an early point.

Sales audits.




In 2010, Deutsche Telekom also continued systematic certification of the sales partners of Telekom's German business sales organization by using independent external auditors. This certification covered, among other things, data privacy, IT security and quality management. The external sales partner audits contribute to the Group-wide strategic objective of "Integrity and Respect in Contact with Customers". (see page 19)

In 2010, 37 call centers , which handle customer calls according to Deutsche Telekom's requirements within the sales organization, were successfully certified by TÜV-Rheinland. In October 2010, the company began certifying around 70 call centers whose operation is commissioned by Deutsche Telekom Customer Service. At the same time, audits of around 350 exclusive trade partners were initiated. These certifications are expected to be completed in 2011.

In addition, Deutsche Telekom rigorously pursued non-compliant conduct by sales partners and employees that was reported by customers and employees and took action against such misconduct.

Standard privacy audits.

Deutsche Telekom regularly audits important processes, systems and departments under its so-called TOP audits. In 2010, these were:

1. **Audit  of data retention by T-Home/T-Mobile:** After the German Federal Constitutional Court revoked the rules for data retention  in March 2010, an audit was performed to check whether all data had been properly deleted according to the Constitutional Court's requirements. The audit confirmed that the data had been irreversibly deleted. Now that the data has been deleted and data retention  is no longer practiced, this audit will no longer be necessary in the future.
2. **Audit of the investigation process:** This examined whether internal investigations within Deutsche Telekom are carried out in compliance with data protection regulations. The audit confirmed that the investigations were in compliance with data protection regulations.
3. Another **audit** was performed to check the system for **customer management in mobile communications**. The corresponding customer management system for fixed networks will also be audited in 2011. Over the medium term, both systems will be merged as a result of the founding of T-Deutschland GmbH and will therefore be audited as a single system in the future.
4. The **SAP HR audit** checked the collection and processing of employee data, i.e., compliance with the agreed access authorizations.
5. **Audit of the data warehouse:** In 2010, compliance with the data privacy requirements of the data warehouse for mobile communications was checked. The corresponding system for the fixed network will be audited in 2011. As in other systems that do not exist separately for fixed networks and mobile communications, both systems will be successively merged over the medium term as a result of the founding of T-Deutschland GmbH and will therefore be audited as single systems in the future.

Identified vulnerabilities were and will be eliminated by the specialist units and the implementation of the measures checked by Group Privacy.

The following central internal and external audits took place in 2010:

Results of the 2010 national and international basic data privacy audits.

The annual basic data privacy audit allows Deutsche Telekom to measure the general level of data privacy within the Group and identify possible structural vulnerabilities. The basic data privacy audit surveys employees and has been conducted at Deutsche Telekom since 1997, with the audit going international in 2006. In 2010, the form and content of the audit was fundamentally revised over previous years. While executives and team leaders used to be surveyed, the focus is now on a direct survey of a representative sample of 65,000 employees in Germany and 20,000 employees abroad (around 40 percent of the workforce in all). This provides a better target group-specific analysis of the results as well as better measure development based on these results.

At the international level, both employees and the local data protection officers are surveyed by asking them to provide information on their own level of data privacy within their organizations. The self-assessments are checked by local audits in the form of sampling. In 2010, the self-assessments of several national companies (T-Mobile USA, T-Mobile Netherlands and T-Systems USA) were thus audited separately, and a reasonable level of data privacy was determined. In the first half of 2011, additional local audits will be carried out at national companies.

The survey dealt with topics such as data privacy awareness, training intensity and benefits, knowledge of how to use tools such as e-mail encryption and ways to destroy files as well as data privacy processes. One result of this survey was that 75 percent of the respondents in Germany and 63 percent of the respondents in the international companies rated Telekom's level of data privacy as "very high" or "high". On a personal level, 87 percent of employees in Germany and 80 percent of employees in the international companies find the topic of data privacy to be "very important" or "important".


Although the results were overwhelmingly positive, Deutsche Telekom continuously makes an effort to sustainably develop and strengthen the data privacy level. Thus, Group Privacy will continue to expand, in particular, its training concept and portfolio in Germany in 2011.

Audits in locations outside Germany.

T-Systems, the business customers arm of Deutsche Telekom, offers international IT services for Deutsche Telekom itself as well as for business customers. In 2010, several of these international locations (such as Brazil, Spain and Hungary) were audited to ensure a reasonable level of data privacy. These audits are referred to as point of production audits (PoP audits).

The Privacy Code of Conduct audits (PcoC audits) were used to check compliance with rules laid down in the Privacy Code of Conduct (see www.telekom.com/datenschutz) for ensuring a reasonable data privacy level within the entire Deutsche Telekom Group. These audits were performed at T-Mobile USA, T-Systems North America, T-Mobile Netherlands and Telekom Croatia.

Certifications received.

Audits are an important component of achieving a sufficient level of data privacy. Many other control mechanisms ensure that data privacy and data security measures have been implemented within Deutsche Telekom. In addition to organizational control under the German Accounting Law Modernization Act (Bilanzrechtsmodernisierungsgesetz (BilMoG))  this includes the processes for advising on, auditing and approving data privacy and security concepts, external audits by regulatory authorities and processing notifications and complaints by customers and employees on data privacy problems. To this are added certifications based on recognized standards.


Various parts and units of Deutsche Telekom have undergone diverse certification procedures and thus meet recognized high standards:

Certification by TÜViT of the accounting process for consumers.

Certification.

A certification is a procedure that is carried out by external, independent agencies such as TÜV and DEKRA. They are used to verify compliance with certain requirements for products and services and their production processes, including trade relations, people and systems. Certification procedures are particularly objective and thus especially time-consuming as well as associated with great expense, due to the amount of work involved. Certifications are carried out on the basis of national and international standards.

After the first part of the accounting process for consumers in the fixed network (traffic data processing) was audited and certified in June 2009, TÜV IT also confirmed the two remaining parts in September 2010. The second part involved certifying the presentation of invoices on paper and online

information systems, while part three concerned the provision of billing information for financial reporting and other supporting documents. As a result, Deutsche Telekom's entire billing process for consumers in the fixed network has been certified. TÜViT granted the company the data privacy certificate "Trusted Site Privacy". An audit under the Trusted Site Privacy criteria involves both an assessment of data privacy and an analysis of IT security. For this purpose, different IT systems and interfaces were audited and security tests carried out over a period of two years. The recommended requirements were implemented. All requirements for customer data privacy have thus been met. Deutsche Telekom is the first, and so far the only, telecommunications company to have its entire accounting process audited and certified by independent TÜViT experts. The process involves collecting and processing all data generated for over 27 million customers who conduct daily telephone calls over the fixed network. A similar certification  is expected to be carried out for the mobile communications segment as well.

Certification of Telekom Shops.


The Telekom Shops successfully completed the certification of their privacy- and security-relevant processes in 2010 and have thus earned the right to use the DEKRA seal "Data Privacy and Data Security According to the Federal Data Security Act" for the second year in a row. DEKRA attested that the Telekom Shops had increased their level of data privacy and enhanced employees awareness and expertise, confirming in its final report that customer data privacy is extremely important to and in place for employees in the sales territory.

ISO 27001 certification.



The international standard for information security is described in ISO/IEC 27001. This standard specifies the requirements for the production, introduction, operation, monitoring, maintenance and improvement of a documented information security management system, taking into account the risks within the entire organization. ISO 27001 certificates are awarded by accredited certification institutes. The certification covers document management, continuous improvements to the management system, the management of values within the organization, HR security, physical security, operation/communications management, access control, procurement, development and maintenance of IT systems, handling of information security incidents, securing of business operations (continuity), compliance with requirements. The certification is independent of the type of organization and can thus be applied, for example, to trading companies, as well as non-profit and government organizations.

Certifications according to international standards.

In 2010, Deutsche Telekom received a certification under the international standard ISO  27001 standard for its central security management system and parts of T-Deutschland GmbH. T-Systems also continued the process of certifying its German organization and 17 national companies in 2010. This goal is to obtain the umbrella certificate for the introduction of an information security management system at T-Systems. The company also performed 160 ISO 27001 audits worldwide alone this year.



Deutsche Telekom has its shops audited and certified by independent experts.

Internal and external communications.

Handling personal data is a matter of trust: customers' trust in the company to which they entrust their personal data. But it also means that Deutsche Telekom must trust the employees who handle the sensitive data. Trust in both directions requires communication in both directions. Deutsche Telekom therefore believes in providing its customers with transparent information and offers its employees security in handling personal data. For this purpose, Deutsche Telekom uses a variety of communications tools and channels, both external and internal ones.

Customer-facing communications.

Deutsche Telekom views data privacy and data security as a customer service: It is the company's duty to provide customers and interested parties with information about the dangers involved in using the Internet as well as ways to protect themselves. Deutsche Telekom also provides information on how it handles stored customer data. Deutsche Telekom uses different media for this information and is continuously expanding its communications system.

In 2010, the company used press releases and online notices to draw attention to European Privacy Day, which has taken place since 2005. On the occasion of Privacy Day 2011, which took place on January 28, Deutsche Telekom expanded its activities. Prior to the event, it published a survey on how Germans use the Internet (www.telekom.com/datenschutz or www.studie-life.de) and distributed guides containing tips on ways to safely surf the Internet in the pedestrian zones of major German cities. On Privacy Day itself, the company organized an online chat session with internal and external experts on all questions relating to data privacy in products and services. Around 180 interested parties took advantage of this offer. In the future, Deutsche Telekom plans to further expand its activities for European Privacy Day and, to this end, work together even more intensively with organizations and other companies. At the same time, the company plans to participate more actively in discussions as part of the public debate surrounding data privacy and data security.

In 2010, Deutsche Telekom 2010 addressed the public with the following additional measures:

- A new edition of the guide titled "Data Privacy at Home – How To's" provides interesting tips on how to prevent Internet crime and abuse. The brochure is available in the T-Shops and can be downloaded from www.telekom.com/datenschutz
- Deutsche Telekom educates users in radio broadcasts on issues such as secure WLAN encryption and secure online shopping
- At www.telekom.com/datenschutz, Deutsche Telekom continuously provides the latest news relating to data privacy. The company also provides tips on using the Internet safely and explains changes to laws that affect data privacy
- In addition to presentations at CeBIT and the International Consumer Electronics Fair in Berlin, the Chief Privacy Officer offered personal advice to customers in selected T-Shops in Germany
- In presentations in schools, privacy officers educate children and young people on the sensible and responsible use of the Internet. A list of services can be downloaded from the website www.telekom.com/datenschutz.

Employee-facing communications.

Employees comply with data privacy and data security when they are aware of the topics and react confidently even in difficult situations. Communication is the key to enabling employees to act accordingly.

Whatever applies to employees is naturally also obligatory for the Group's top management. Data privacy and data protection are more effective when managers are more intensively involved in these areas from the very beginning. In a process that was redesigned in cooperation with Human Resources, data privacy awareness within Deutsche Telekom is being raised among all newly hired top managers. The Chief Privacy Officer informs and educates executives and managers about the special importance of data privacy when they join the company. Regular management training on the topic ensures that the managers remain up to date.

In 2010, the focus was on introducing a decentralized data privacy organization as well as on cooperation with the data privacy coordinators within Deutsche Telekom. The data privacy coordinators assist with the introduction and implementation of Group-wide data privacy requirements. They receive local support from the so-called "data privacy bridge heads", who

are appointed by the Management Board and who implement the company's privacy-specific requirements in operations. The data privacy coordinators meet regularly to discuss current topics and share their experiences. These meetings are aimed at supporting the bridge heads in implementing and coordinating the Group Privacy requirements.

The data privacy bridge heads, who have been in place within the company since 2009, as have the data privacy coordinators, held monthly meetings in 2010 to share experience and information.

To give employees the opportunity to learn about data privacy locally in person, the Chief Privacy Officer visited ten locations in Germany and answered questions over a telephone hotline.

A further web-based learning tool was added to the already extensive range of data privacy training opportunities. In addition, advanced training measures, such as a workshop on the newly introduced PSA procedure [G], was also offered. Furthermore, employee awareness of security-compliant behavior was raised in regular training sessions.

Deutsche Telekom checks training services and content at regular intervals in internal audits. Thus, the data privacy training opportunities for employees were analyzed in 2010. It turned out that the scope and content of the measures could be rated as positive.

The data privacy website, which was redesigned both nationally and internationally, went online in September 2010.



Passwords and access data should remain secret.
Deutsche Telekom provides information about secure data
on the occasion of European Privacy Day.

Deutsche Telekom's Data Privacy Advisory Board.

➡ Examining a topic from different points of view leads to success.



Tasks and functions.

Deutsche Telekom's Data Privacy Advisory Board is an independent committee that advises the Management Board and facilitates constructive discussions with leading data privacy experts and leaders in politics, education, industry and independent organizations on topics relevant to data privacy. The Data Privacy Advisory Board was formed in February 2009 and contributes an external, independent and socially varied perspective to Deutsche Telekom's internal data privacy and security organization.

The Data Privacy Advisory Board covers a broad range of topics. It deals with business models and processes on handling customer and employee data as well as IT security and the appropriateness of corresponding measures. It also deals with issues relating to international data privacy and the implications of new legal provisions. Its duties include evaluating data privacy and data security measures as well as developing proposals and recommendations for the Board of Management and Supervisory Board in the context of the "digital" society.

Structure.

Deutsche Telekom appoints the members of the Data Privacy Advisory Board to two-year terms. Leading data privacy experts as well as representatives of different professional groups are appointed in order to guarantee qualified external critical consideration of data privacy and data security matters. In 2010, the members included:


- Wolfgang Bosbach, Member of the German Parliament, lawyer and Chairman of the German Parliament's Committee on Internal Affairs
- Dr. Michael Bürsch, former Member of the German Parliament, member of the "Center for Corporate Citizenship Germany" (CCCD)
- Peter Franck, Member of the Management Board of Chaos Computer (CCC)
- Prof. Dr. Hansjörg Geiger, Honorary Professor of Constitutional Law at the Johann Wolfgang Goethe University in Frankfurt am Main, and State Secretary of the Federal Ministry of Justice from 1998 to 2005, President of the German Federal Office for the Protection of the Constitution and the German Federal Intelligence Service
- Prof. Peter Gola, President of the German Association for Data Protection and Data Security (GDD)

- Bernd H. Harder, lawyer and member of the Executive Board of BITKOM e.V., lecturer at the Stuttgart Media University and the Munich Technical University (TMU)
- Gisela Piltz, Member of the German Parliament, Deputy Parliamentary Group Leader of the FDP parliamentary group
- Dr. Gerhard Schäfer, Presiding Judge at the Federal Court of Justice (BGH), retired
- Lothar Schröder, Chairman of the Data Privacy Advisory Board, Member of the ver.di National Executive Board and Deputy Chairman of the Supervisory Board of Deutsche Telekom AG, member of the Enquete Commission on the "Internet and Digital Society"
- Silke Stokar, former Member of the German Parliament, former spokesperson on internal affairs for B90/Die Grünen parliamentary group
- Dr. Peter Wedde, Professor of Labor Law and Law in the Information Society at the University of Applied Sciences, Frankfurt a.M.

Examples of the Data Privacy Advisory Board's work in 2010.

Since 2009, the Data Privacy Advisory Board has become established not only as an important advisory committee, but it also helps Deutsche Telekom take on a leadership role where data privacy and security are concerned. In 2010, the committee evaluated its own work in order to review its independent role as an advisory board. In this context, the members gave a positive rating, for example, to the way information is exchanged with Deutsche Telekom in the Data Privacy Advisory Board meetings as well as how seriously Deutsche Telekom takes the committee's recommendations.

The Data Privacy Advisory Board can address data privacy and data security issues on its own initiative. It is called upon to raise issues independently and to process corresponding proposals and recommendations for Telekom's Board of Management.

This high degree of freedom enabled the Data Privacy Advisory Board to expand the focus of its work on dealing with "processing topics" to include future-oriented aspects of data privacy and data security. While the primary concerns in 2009 were on reorganizing Group Security and reorienting data privacy practices, in 2010 the focus shifted increasingly to issues such as cloud computing  and web neutrality, which underscore Deutsche Telekom's role as a trendsetter for companies in the telecommunications industry and in the digital society acting in accordance with data protection regulations.



Lothar Schröder,
Chairman of the Data Privacy Advisory
Board, member of the ver.di National
Executive Board and Deputy Chairman of the
Supervisory Board of Deutsche Telekom AG.



**Why does Deutsche Telekom need a data privacy advisory board?
Why don't other companies have one?**

Indeed, Deutsche Telekom is not the only one that needs a data privacy advisory board – other companies do as well! The advantages of such a committee are obvious. A company can take advantage of external expertise from a variety of fields that cannot be covered by internal staff. The diverse membership of the Advisory Board offers Deutsche Telekom the opportunity to bring its work on data privacy and security to bear in different segments of society through the disseminators on the Advisory Board.

A Data Privacy Advisory Board requires a relationship of mutual trust. This is particularly clear where Deutsche Telekom is concerned. Since 2009, we have seen proof that the company has consistently improved its data privacy practices, and it takes data privacy and security very seriously. Our trust in Deutsche Telekom has grown steadily over the course of the Advisory Board's work. At the same time, we are aware that the company demonstrates enormous trust in us by allowing us to examine its structures and measures in such a sensitive area. I think that both the Advisory Board and the company itself will continue to intensify cooperation in the future and also deepen the range of functions performed by a data privacy advisory board. These are valuable experiences that other companies should emulate.

In a total of five sessions, the Data Privacy Advisory Board discussed a wide range of topics in 2010. Thus, it dealt with Deutsche Telekom's misuse detection systems, the expert report by Dr. Schäfer and risk management measures in Sales and Service. It discussed a data privacy foundation, the draft of the employee data privacy law and offered advice on the effectiveness of access control procedures in customer data systems as well as the security level of sales partner portals. A further area of advice in 2010 was the topic of "web neutrality" which is being intensively discussed in public. The Data Privacy Advisory Board's primary concern here was the privacy-relevant implications of possible "rights of way" for defined data.

The Data Privacy Advisory Board also discussed aspects of cloud computing [G](#) and Telekom's "Entertain" IP TV, which are relevant for data privacy and data security. It communicated corresponding positions and recommendations in these areas to Deutsche Telekom's Board of Management.

External experts have maintained a critical view of the requirements of data privacy and IT security as well as their implementation at Deutsche Telekom. The Management Board of Deutsche Telekom will continue to engage in constructive dialog with the Data Privacy Advisory Board.

Guide on the secure handling of data.

 Armed with the right knowledge, users can better protect their data.



We are living in the age of digitalization – we are performing our private banking transactions online, making purchases over the Internet and increasingly maintaining our social contacts on the web. User behavior has also changed the face of crime. Spying on access data or hacking private WLAN connections are the modern equivalents of stealing purses and breaking and entering. Everyone knows how to secure their house and purses in just a few steps. We need to develop the same routine when using the Internet.

By observing the following tips you can protect yourself against Internet crime and prevent misuse. Should you have any questions on the topic of data protection in general or at Telekom, you can send an e-mail to privacy@telekom.de.

PC security and basic protection.

Observe the following tips so that your private data also remain private and secure on a PC.

Always be aware of how sensitive the data is.

With confidential information you should not use a public PC, because you do not know whether it is adequately protected against viruses, worms, Trojans and external attacks.

Make sure nobody can overlook your PC. Pay attention to who can see your screen if you are entering sensitive data such as users names and passwords.

Always keep your system up-to-date.

Software providers are continually enhancing their products and thus closing any security gaps which emerge. Therefore always keep your software and anti-virus software in particular up-to-date to protect yourself from attacks.

Ensure you have high security settings.

To protect your data, install an anti-virus program and an anti-spyware program. It is also important to set up your personal firewall. Using the configuration you can protect yourself from attacks from the Internet. Also use the virus scanner supplied by your e-mail provider to get the highest possible security standard.

Check downloads and e-mail attachments.

It is common to spread viruses via file attachments. For this reason only open trustworthy attachments from people you actually know. The same applies for software downloads: If the provider or site does not seem trustworthy to you, you should not download anything.

Secure your PC with a password.

To protect your PC, and therefore your data, from being accessed by third parties you should always lock it using a password. Make sure that the password is a very secure one. After entering the correct password the screen is activated again and you can continue working. It is recommended that the screen and keyboard lock is activated with the screen saver five minutes after the last user entry. On a private PC, the activation time is of course freely selectable. The lock can also be activated immediately if required. In a Windows operating system this is done by pressing the keys Ctrl + Alt + Delete and then selecting the option "Lock computer".

Deactivate wireless interfaces.

To protect your private PC from external attacks, deactivate any wireless interfaces you do not currently need - after all, when you leave the room you also switch off the light. So why not switch off the WLAN transmitter on the router when you are not on the Internet? Most models now have a button on the back. The same also applies for your cell phone, for example with the Bluetooth interface, in order to protect it from viruses, worms and Trojans on the one hand, and on the other hand ensure that unauthorized persons cannot access your personal data such as the address book, calendar or your images. Configure your wireless accesses on the devices you use. This too will make it difficult for third parties to gain access (page 48).

Data backup.

To be on the safe side, you should regularly make a back-up copy of important data in particular, for example on CD-ROM/DVD or on an external hard drive.

Creating a secure password.

You won't get very far on the Internet without a password. And the better the password is, the more secure the data concealed behind it is protected.

Online banking, reading e-mails or writing a contribution in an anglers' forum – anyone using Web 2.0 will sooner or later always reach a point at which they are asked for a login name and password. The login name generally does not cause any problems. However, by about the fifth password it's difficult to stay on top of things. Even more so, because a secure password is unfortunately the opposite of a memorable one. So, how do I create a secure password that I can remember? Here you can learn how to exasperate hackers and protect your data.

How do I create a secure password?

The golden rule for creating a secure password is this: It should not be recognizable to anybody else as a meaningful word. There is a simple trick to creating a password like this: Think of a sentence which is easy for you to remember. From this sentence, use only the initial letters of each word and replace the individual letters with numbers and special characters. An example of a sentence would be: "We both like eating pizza with salami." The initial letters give the combination "Wblepws". Now the numbers and special characters come into play. Here you can let your imagination run wild. In our example sentence we replace the "l" with a "2" and add a "!" at the end. Our secure password then becomes "W2lepws!". This password comprises 8 characters. This is the lower limit recommended by experts for a secure password. As a rule, the longer and more complex the password the better.

The reason for this is that hackers use programs to systematically try out all the possible password combinations. With each additional character, the number of possible passwords and thus the necessary runs that this type of computer program would need to crack your password therefore also increases.



A complex password protects personal data – and makes life difficult for online swindlers.

Create a password for each access.

An additional important precautionary measure is to use different passwords for different accesses wherever possible. This is because every now and again data thieves manage to spy on entire customer files, including all the access data. A password which falls into the hands of thieves in this way is no longer secure. The hackers will also try this password if they want to gain access fraudulently. A secure password is therefore always one which you only use for one access. This should always apply to your access to online banking.

Keep your passwords safe.

You should also only keep your passwords in secure locations to which only you have access. The best place for this is of course your head. The worst place is your browser. You should therefore ignore the “auto-complete function” for important passwords in particular and never save them on the hard disk or note them down on a piece of paper near the PC. Change your passwords regularly. You should change your passwords at regular intervals to increase protection against data theft. We recommend that you do this at least every three months.

When do I need a secure password?

The problem with secure passwords is this: They are extremely difficult to remember. Whether it's your wife's name or grandma's birthday – any memory aid makes a password insecure. However, it may be that you do not always need a password which is 100% secure. For the anglers' forum mentioned above for example, you do not necessarily need to be as careful as for online banking.

Therefore have a good think before you choose a password:

- Is it protecting personal or business-related information (e. g., e-mails, contacts, etc.)?
- Can financial transactions be performed if access is gained (such as with online banking or online auction houses)?
- Have you saved important data like your credit card number or bank details in the corresponding access

If the answer to these questions is “yes” then you should definitely choose a password which is secure as possible. If not, it may be that a less secure password is adequate. Even in this case you should of course make sure that you do not make things too easy for any hackers.

WLAN security.

More and more people are using wireless networks (Wireless Local Area Networks or WLAN) at home or on public PCs to access the Internet.

They are practical because they mean that you can access the Internet from anywhere. However, they also pose security risks. In general it can be said that any wireless connection offers less security than a network connection over a cable. With the wireless connection, the data is transmitted to the recipient by radio and can be intercepted.

The personal effort in creating a secure personal environment is not only important for protecting yourself against attacks, but avoiding negligence minimizes liability.

A private WLAN should be protected by the usage of passwords. If a third party gains unauthorized access to the non-secured WLAN and performs illegal activities, depending on the country legislation, you as the owner of the WLAN, may be forced by an injured party to cease and desist and to reimburse any associated costs of legal proceedings. It is therefore important that you encrypt your data so that your private e-mails, user names and passwords do not fall into the wrong hands. You can find important information on how to configure the security parameters of the router in its user manual.

You can protect your home against data theft by following these points:

Secure your WLAN router.

This is the most important precautionary measure since the WLAN router establishes the connection between your computer and your Internet access. Before you start operating your WLAN you should change a few basic settings: First you need to manually change the SSID, which refers to the network name, and give it a personal name. Here it is best to select an imaginary name which does not allow it to be traced back to you personally or your Internet provider. To increase security you should prevent the SSID from being displayed so that the name of your router cannot be found on the network. Since you know the name of your router you will of course be able to find it.



Surf the web any time and anywhere.
An encrypted WLAN router is the first
step toward doing this safely.

Set up encryption.

An additional protection measure is to encrypt your WLAN. In most WLAN systems this is done via WPA2-PSK – PSK (Pre-Shared Key), i. e., the previously agreed key. Here a “key” (password) is needed to access the network when a connection is established. It is important that you select a secure password here. You will find more information about creating passwords under “Creating a secure password”.

Set up a filter against data thieves.

To increase the security of your data you can set up a MAC address filter. The MAC address is a number with which every network card and thus every Internet-enabled computer can be identified. If you only allow the MAC addresses you need, thirdparty computers have no chance. How do I find the MAC address? Example in Windows: Go to the start menu and select “Control panel”. Then click on the “System” icon and, under “Hardware”, select “Device Manager”. Here you will find the item “Network Adapters”. Normally you will find two entries here – one usually has “Wireless” added on to the name. Double-clicking on this entry brings up various menus: The MAC address can be found here under “Extended”.

Deactivate your WLAN.

You should deactivate your WLAN when you are not using it. By doing this you are not only protecting yourself from data thieves but also saving electricity.

Security Information of the Federal Office for Information Security.

The Federal Office for Information Security recommends having no wireless installation of all settings on your WLAN Router but via cable.

Especially when using publicly accessible Hot Spots you should consider the following recommendations to protect your data in the best way.

Deactivate your network approval.

If you use HotSpots the file and directory approval on your laptop or mobile device should be deactivated. As a rule you can deactivate this approval in the network settings of your operating system. You should never be logged in with a user account which has administrator rights.

Activate your firewall.

Before you dial into an external WLAN, activate your firewall. The firewall monitors the data traffic from and to your computer and thus helps to prevent attacks by harmful software.

Do not establish automatic connection.

Do not establish any connection with the HotSpot if you do not know who is responsible for operating the access. You should also not allow any automatic connection with wireless networks and always manually select which network you wish to connect to.

Look out for fake HotSpots.

In order to access confidential data, criminals set up their own wireless networks which are very similar to the home page of the real HotSpot, for example, of T-Mobile. When connecting to the fake HotSpot you are asked to enter information such as your credit card number, supposedly to open a new HotSpot account. This manipulation technology is based on the phishing and pharming technology which is explained under "Secure online banking and protection against phishing attacks".

Secure online banking and protection against phishing attacks.

More and more people are banking over the Internet. This banking facility can be accessed any time of the day or night and is easy to use from home.

As convenient as online banking from home may be, it poses risks due to the processing of sensitive data. Data such as PIN and TAN numbers, which enable access to an account, repeatedly fall into the hands of fraudsters due to carelessness. This very often happens due to phishing attacks, which have high potential for risks and damage. Phishing is a combination of the terms "password" and "fishing" and refers to attempting to acquire passwords as well as PIN and TAN numbers. Through fake e-mails and websites with which the customer is asked to give his account details along with passwords, criminals can access sensitive data. In most cases a link takes the user to the fake website of banks and other companies which look very similar to the original.

Pay attention to the following points so that you can protect yourself against these attacks:

Look out for phishing e-mails.

- In most cases the forged e-mail is addressed to a general, nonpersonalized subject, for example "Dear customer of XY bank".
- Phishing e-mails demand immediately and necessary action which may also use threats ("If you do not update your data immediately it will be lost...").
- Always look at the full sender's address of the e-mail. If the address does not clearly relate to your bank it is best to check once again directly and make sure.
- Your bank will never ask you to provide confidential data such as a PIN and TAN in a form within an e-mail. Neither will your bank ever ask you for sensitive data over the phone. If are unsure, call the number of your bank you are familiar with directly and make sure..
- Phishing e-mails are in many cases written in poor language. For languages with special characters in many cases it becomes obvious. For example, in German, umlauts such as ä, ö, ü are missing. This is because these messages are translated from other languages quickly and simply by computer programs. But often, even emails written in english, disclose spelling or grammar mistakes.
- The most secure thing to do is to never go to a website via an e-mail link. Always call up the site directly from your browser. Make sure the address of the site is written correctly.



Social networks are a permanent fixture of everyday life. But even here, not all information is intended for everyone.

Watch out for phishing websites.

- Always look for the security certificate which is shown by the lock icon at the bottom right-hand corner of your browser. If this is not displayed then the site is not secure.
- If it is a secure connection, the abbreviation "https://" is displayed in the browser's address bar. This encryption procedure prevents data from being read or manipulated during the time you are working on it. In rare cases this can also be faked. To be on the safe side, always enter the address of your bank yourself in the address bar of your browser and do not follow a link.
- On the login page your bank will never ask for TAN codes. If this is the case, please contact your bank immediately.

General precautionary measures for online banking.

- Always keep your personal data such as passwords, PIN and TAN in a secure location and never save these on your PC, including under a password manager. If this data is saved on the PC it could be read out.
- Select a secure password and keep it safe. See the tips on creating a secure password. For online banking you should always use a special password which you do not use for any other purpose. The password should be changed regularly to increase security.
- Banking transactions should only be performed from your own private PC or a mobile device in private. Make sure that you log out at the end of the session and empty the cache on your PC.
- It is also important that you always use current anti-virus software and perform security updates to close any security gaps.
- Check your account transactions regularly. Contact your bank immediately if you see anything suspicious or if any discrepancies arise. If you notice anything suspicious or unusual, block your access to online banking. You can do this by instructing your bank over the phone or directly via a relevant function in the online banking window.

If something seems to be unusual or suspicious, block your access to your online bank account. You can either do this via a phone call to your bank or directly online via the respective window on your online banking website.



Deutsche Telekom offers its customers help and advice on the subject of data privacy. The guide is available in the Telekom Shop or online.

Behavior in the social network.

With Web 2.0 social networks have found their way into our day-to-day lives.

These days everyone can send and receive information around the world and thus members of social networks such as Xing, Facebook, MySpace, etc. naturally disclose private data. Contrary to what is often incorrectly assumed, the Internet is not a legal vacuum. However, not everyone complies with the applicable data protection provisions, to the provision on the right to one's own image or to copyright laws. This poses privacy risks which many users are not aware of. For this reason it is important to comply with certain practices in social networks.

First of all, read the General Terms and Conditions and data protection notices of the platform operators thoroughly. These generally tell you how the operators deal with your personal data.

Creating your own profile.

- First and foremost, where possible do not disclose any personal data such as e-mail addresses, telephone numbers, Messenger data, photos etc. This is because anyone who gives away a large amount of information about themselves is making it easy for other people to send them phishing messages or unwanted advertising, for example.
- In chats and discussion forums, instead of your own name you can also specify a nickname, even if the operator of this site asks you to use your real name. But if you do want to use your own name, you should at least shorten your surname to the initial.
- You can restrict access to your own profile using the settings. It is most secure to only allow friends to have access.

Profile pictures.

- Even if it seems normal amongst young network users to show a picture of themselves on the Internet using photos, images which are too revealing violate privacy protection regulations. For this reason you should carefully consider which photos of yourself you display on the Internet. Photos in beachwear or underwear are generally taboo. Most people would not publicize their private life to people they don't know in their day-to-day lives, would they? Always think what you really want to reveal about yourself.



Photo albums.

- The function of uploading photos to online photo albums is popular and frequently used. So as not to take any risks here either, you should make sure that only immediate friends have access to these albums.
- As a rule you should only upload photos to which you also have rights.
- Photos which you have uploaded to the Internet often remain saved in the cache for a long time, even if you have deleted the images or the entire photo album.

Privacy.

- You should know about and use where necessary all the settings provided by a social network for protecting your privacy. If you want to protect your privacy on various social networks you can consult the website www.klicksafe.de.

Adding friends.

- We often receive a friend request from somebody we do not know. Before you accept the invitation or send it to anybody else you should check thoroughly who this person is.
- Personal data should only be made accessible to genuine friends.
- Since you would not want to be shown in disadvantageous images or read private comments about yourself on the message boards of these sites, you should also respect the privacy of friends and relatives and only place images of them on the Internet after consultation.

Since every “friend” can see the data released for friends, you should always give careful consideration to who you accept as a friend

Making arrangements on the Internet.

- Social networks are often used to arrange to meet friends or discuss other rendezvous. Private information such as arrangements to meet or “I’m home alone tonight” should however under no circumstances be posted on message boards. This type of information should only be exchanged privately, via e-mail or Messenger or over ICQ, Skype, etc.

Report and ignore function.

- People, content or groups which breach the Code of Conduct of networks should always be reported. You can either use the report button on your profile page to do this or you can contact your local police station.
- Users who harass you can be blocked from accessing your page using the ignore function. They can then also no longer send any messages. You should also report these people to your provider.

Security for children on the Internet.

Nowadays exposure to the Internet during childhood almost goes without saying. It is hardly surprising that parents worry about the safety of their children when they use the Internet.


There are however ways to rule out any concerns. Make your child aware of how to use the Internet correctly:

- Discover the Internet together so that your child learns how to use it correctly from the start. You should also regularly ask him about his recent experiences on the Internet and/or take a look at the screen if your child is sitting at the PC.

Look for trustworthy web sites regarding child protection and find out together with your child which sites children can surf without having to worry about being confronted with unsuitable content. The Deutsche Telekom, for example, is promoting in Germany child-friendly offers on the Internet and creating a secure area to surf the Internet with the search engine www.fragfinn.de.

- Agree on rules for Internet usage and find out about protective devices associated with this. There are special filters which can be installed on the computer and which automatically block pornographic sites as well as those which glorify violence or are associated to political extremists.
- Your child should never pass on personal data - no details about age, where he lives or meeting places. Even when creating an e-mail address or a name for chat rooms your child should only use nicknames.
- Discuss the risks of meeting people. Your child should only meet people they have got to know over the Internet after consulting you. Children cannot tell whether this person has good intentions.
- Discuss the extent to which content is truthful with your children.
- Encourage your child to have good netiquette, i. e., to behave appropriately. This is particularly important if your child contacts friends on the Internet.
- Use filter programs so that your child only has restricted access to the Internet and only visits sites appropriate for their age.
- You can find further comprehensive information on internet security on the website www.klicksafe.de. Under the mandate of the European Commission this website wants to bring forward the media competency related to the usage of the internet.

Appendix.

 When it comes to data privacy and data security, nothing should be left up to chance. Good organization and the right measures point the way to success.



Special data privacy and data security measures since 2008.

Particularly since the data incidents and the spying affair of the past, Deutsche Telekom has developed measures intended to help prevent such incidents in the future. The measures are both organizational and technical in nature and they affect all levels of the Group. One of DTAG's principles is to provide transparent and candid information about all aspects of data security and privacy. In addition, the company uses its expertise to provide assistance to customers and interested parties in how to handle personal data on the Internet.

Measures taken by Deutsche Telekom.

- October 2008: Formation of the Board of Management department for Privacy, Legal Affairs and Compliance, the first DAX 30 corporation to do so. Other DAX 30 corporations have since followed suit.
- 10-point program of immediate measures (March 2009)
- Realignment of Group Security and control structures
- Double-check principle
- Spring 2009: Publication of the first Data Privacy Report, the first DAX 30 Group to do so. Objective: Open, transparent communication on data incidents and data privacy measures.
- Publication of a data privacy report on www.telekom.com/datenschutz containing information on all recent events.
- February 2009: Formation of a Data Privacy Advisory Board with leading data privacy experts from politics, academia, industry and independent organizations
- Mid-2010: Introduction of a standard security and data privacy procedure with standardized documents for the German Group companies

Improved data privacy.

- Shutdown of non-secure systems
- Introduction of system restrictions for outgoing customer calls made by call centers in order to prevent mass data retrieval. Employees can access only the current data record of a customer.
- Narrower definitions of areas of responsibility within customer support, reduced access to customer data. As a rule, access is limited to data needed for the work at hand (need-to-know principle)
- Increase in general controls and administrator controls by internal Group Privacy
- Systematic logging of data access
- Tracking of access to particularly sensitive databases using log files
- Heightened requirements for user IDs and passwords
- Implementation of a variety of security measures in individual IT systems to prevent unauthorized use
- Training of all employees on data privacy issues and regular obligation to maintain data and telecommunications secrecy.

Transparency/certificates.

- Auditing and certification of systems, processes and sales partners through independent experts, the first telecommunications company to do so.

Raising public awareness.

- Free data privacy brochure available at www.telekom.com/datenschutz
- Regular radio broadcasts with tips on safer ways to surf the web, etc.
- Regular chat sessions on data privacy and data security
- Consulting on data privacy via Datenschutz@telekom.de
- Support for initiatives such as fragFINN e.V., Making Germany safe on the Net , Teachtoday
- Extensive information for customers whose computer systems have been infected with malware



Organization of Group Privacy.

Group Privacy, under the management of the Group Data Privacy Officer, provides the national companies with direct support on data privacy issues and works toward establishing an appropriate level of data privacy throughout the Deutsche Telekom Group. The Chief Privacy Officer performs the role of statutory data privacy officer, defines the Group's strategic alignment in data privacy matters and represents the Group in all data privacy matters both internally and externally.

Group Privacy consisted of four departments in 2008. An additional department (Privacy Audit and Technical Know-How Management) was set up in 2009 in response to the data privacy incidents.

Data privacy interfaces and data privacy coordinators are installed as on-site data privacy contacts for legal entities, departments and other organizational units. At international shareholdings, this function is assumed by data protection officers appointed for this purpose. Both data privacy coordinators and data protection officers are in constant contact with Group Privacy.

The individual departments:

1. Privacy Requirements, Policies.

The Privacy Requirements, Policies department is responsible for fundamental data privacy issues. In order to ensure legally sound and uniform action, data privacy guidelines and policies that apply throughout the Group are prepared and processes developed within Group Privacy. Alongside internal and external data privacy communication and the coordination of international data protection organizations in the Group, the team's tasks also include the management of interdisciplinary projects and developments related to data privacy.

2. Consumer Privacy.

The Consumer Privacy department advises and supports the Group and its strategic business areas on customer data privacy issues; in particular during the introduction of business models and processes in terms of legal options and organizational requirements for using customer data as well as ensuring compliance with technical requirements governing IT-based customer data processing.

3. Employees and Stakeholders Privacy.

The Employees and Stakeholders Privacy department advises and supports the Group and its strategic business areas on employee data privacy issues and on dealing with personal data of third parties that are not telecommunications customers (e.g., shareholders, suppliers). Its tasks also include advising works councils in the Group, in particular the Group Works Council, on data privacy matters and representing Group companies vis-à-vis the regulatory authorities on employee data privacy issues at operating level.

4. Business Customers Privacy, Products.

The Business Customers Privacy and Products department provides data privacy services for selected affiliated companies of the Group, supports internal projects and sales activities in business customer projects, and assists in the development of Group products in line with data privacy regulations.

5. Privacy Audit and Technical Know-How Management.

This department develops data privacy-specific auditing principles and processes and manages the implementation of these within the Group. It carries out its own audits and manages audits related to data privacy in the Group. It draws up action plans based on auditing and monitors the implementation of these. In addition, it is the internal expert body for data privacy in complex technical issues. The department is currently being expanded.

Organization of Group Data Security.

Group IT Security is responsible for developing and implementing Group security requirements in the ICT field and is thus an integral part of the organization for ensuring data security. In order to live up to this responsibility, Group IT Security has established the following four action areas:

Security requirements.

Definition, preparation and publication of Group-wide security strategies, standards, requirements and processes.

Process integration.

Integration of security aspects into relevant projects.

Implementation of measures.

Advice on and coordination of security acceptance measures and audits for verifying compliance and monitoring of current vulnerabilities. Also works on and provides advice for projects.

Technology.

Market monitoring and evaluation of relevant technologies with responsibility for new security components and achievement of savings potential.

Organization.

Group IT Security is divided into two departments which are responsible for the security of production infrastructure and security in IT services and applications. A unit for order control, interface management and reporting was also set up.

This structure clearly defines interfaces to other Group units, which provides efficient support to the Chief Information Officer and Chief Technical Officer units. The Production Infrastructure Security and Technology departments (Chief Technical Officer organization) work closely together. Issues relating to information security in the Chief Information Officer unit are clarified primarily with the IT Services and Applications Security department.

The specific duties of the Production Infrastructure Security and IT Services and Applications Security departments are handled by specialized teams. Most of these duties are strategic and conceptual in nature – operational implementation is then handled by the the operational departments concerned.

IT Services and Applications Security.

The IT Services and Applications Security department is responsible for ensuring the security of IT services and applications, from customer portals to booking systems.

The IT Applications Security team is also responsible for the security of Deutsche Telekom's internal applications, with a special focus on mission-critical applications.

The Portal Systems Security team is responsible for the security of Deutsche Telekom's portals, with a primary focus on customer portals and portals accessible to external partners. Examples of public portals with mass impact are T-Online.de and the portals of the Load family.

Rounding out the department is the Office and Communications Services team, which focuses on developing and implementing strategies and concepts for the security of office communications networks, services and infrastructures.

Production Infrastructure Security.

The Production Infrastructure Security department designs security measures for Deutsche Telekom technology needed for handling value creation processes. The department is divided into three teams based on the architecture of the Next Generation Network Security Framework:

Access and transport network security is ensured by establishing technical security measures. This involves access platforms for the fixed and mobile networks, aggregation systems and wide area networks (WANs) as well as network-related projects and services for consumers and business customers.



A further team ensures the security of all network services and data center, management and monitoring infrastructures operated by the Group. In addition to handling project inquiries, the Network Service and Data Center Security team also directly initiates projects driven by current security issues. Examples include cloud and dynamic computing.

The Devices and Services Security group is responsible for the security of terminal equipment as well as systems and applications that provide services for Deutsche Telekom's external customers. For example, a major challenge at present are social communities, in which many external partners do not apply Deutsche Telekom's high security requirements and use individual systems.

The fourth component of the Production Infrastructure Security department is the Computer Emergency Response Team. This team operates an internationally oriented security incident management system within the Group's technical security operations and establishes mechanisms for the early detection of attacks on externally accessible IT systems. Its other activities include vulnerability management and discussion of newly identified vulnerabilities with the global emergency teams of other companies.

Glossary.

Audits.

Examination and review procedures that assess whether and to what extent requirements and policies have been met. Penetration tests, which are highly specialized technical reviews, are a special type of audit.

Call center

A company or departments of a service provider that offer operator-supported voice services. A large number of operators handle inbound calls via a hotline and/or outbound calls as part of a direct marketing campaign.

Census verdict

The census verdict is a landmark decision by the German Federal Constitutional Court on December 15, 1983, in which the basic right to information self-determination was established as part of the general right to privacy and human dignity. The verdict is considered a milestone in data privacy rights. It was motivated by a census taken in the Federal Republic of Germany that had been planned for April to May 1983 and was finally carried out in a modified form in 1987 on the basis of the verdict.

Central Security Management

Central Security Management coordinates the interaction of all functions within the Group that are responsible for ensuring security.

Certifications

Certifications are procedures that are used to verify compliance with specific standards for products or services and their respective manufacturing processes.

Cloud computing/dynamic computing

Cloud computing primarily refers to the approach by which abstracted IT infrastructures (e.g., computing capacities, data storage, network capacities or software) are dynamically adjusted to user demand and provided over a network. Data processing by the applications is thus moved to a "cloud" as far as the user is concerned.

Compliance

Compliance means the adherence to codes of conduct and the fulfillment of laws, standards and internal guidelines. The goal is to avoid tangible and intangible damage to the company and its employees.

Cookies

Small files that a web server stores in a web browser so that the information can be retrieved at a later time. Examples of ways in which cookies are used are the shopping carts of online shopping sites and the personalization of websites.

Data retention

Data retention refers to the obligation of telecommunications service providers to record electronic communications data without there being an initial suspicion of wrongdoing or a specific danger. The purpose is to provide better prevention and tracking of serious criminal acts.

Data warehouse

A data warehouse is a central database within a company that contains data from different sources. For example, it is used to combine customer data from multiple systems.

De-Mail

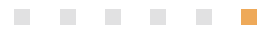
Services on an electronic communications platform that are intended to ensure secure, confidential and trackable business transactions for everyone on the Internet. Interested parties can register for the service at <https://www.de-mail.t-online.de>.

Driveby exploits

These take advantage of vulnerabilities in web browsers (especially older Microsoft Internet Explorer versions) and browser add-ons so that a computer system can become infected simply by visiting an infected website.

Federal Data Protection Act (BDSG)

In conjunction with the data protection laws of the German states and other industry-specific regulations, the German Federal Data Protection Act governs the handling of personal data that is processed in IT systems or manually.



Federal Network Agency (BNetzA)

The Federal Network Agency is an independent federal authority for electricity, gas, telecommunications, posts and railways under the Ministry of Economic Affairs and Technology, based in Bonn. Since July 13, 2005, the Regulatory Authority for Telecommunications and Posts, which came out of the Federal Ministry of Posts and Telecommunications (BMPT) and the Federal Office for Posts and Telecommunications (BAPT), has been renamed the Federal Network Agency. It regulates the telecommunications market, among other things.

Geodata

Geodata refers to digital information to which a physical location in space is assigned. For example, photos can contain a geographic assignment that clearly assigns them to the precise location where the image was created.

Geodata services

Geodata services are web services that make geodata accessible in structured form. Geodata services can integrate geodata into a wide range of network-based geographic applications that display the data in interactive maps or further process the data. Examples of geodata services are Google Streetview and Microsoft Bing.

Group permission clause (KEK)

With the Group permission clause, customers authorize Deutsche Telekom to compile their existing data from T-Home and T-Mobile. The permission includes not only the customer's permission to disclose the contractual data, but also permission to use the data for customer consultation, advertising and market research. Inquiries relating to the Group permission clause usually concern the withdrawal of permission to receive advertising or information granted upon conclusion of an agreement.

Honeypots

Honeypots are isolated server systems that are accessible from the Internet and which simulate vulnerabilities.

International Standards Organization (ISO)

The International Standards Organization develops international standards in many industries. Exceptions are the electric and electronics industry, for which the International Electrotechnical Commission (IEC) is responsible, and the telecommunications industry, for which the International Telecommunications Union (ITU) is responsible. Together, these three organizations form the World Standards Cooperation (WSC).

IP address

The address in computer networks based on the Internet protocol (IP). It is assigned to devices that are connected to the network and in this way makes the devices addressable and thus reachable.

Location-based services (LBS)

Location-based services provide users with location-specific information via a mobile device. To do this, the services must access the location data of the user concerned.

Near Field Communications (NFC)

A transmission standard for contactless exchange of data over short distances. NFC can be used on terminals as a key for accessing content and for services, for example for cashless payments, paperless ticketing, online streaming or downloading.

Opt-in solution

Companies can use customer data only if the customer involved grants permission to do so.

Opt-out solutions

Companies use customer data until the customer objects to such use. Customers must be informed of the way in which the data is used in the company's data privacy notes.

Privacy Code of Conduct

The Privacy Code of Conduct (PCoC) is a Group-wide data privacy guideline of Deutsche Telekom, implemented in 2004 and based on European legal provisions. It contains standardized internal requirements regarding the handling of personal data in the Deutsche Telekom Group.

Red Line Act

This planned law is intended to prevent particularly serious infringements of privacy rights by impermissible publication in teledata. It is intended to prevent personal profiles from being prepared on the basis of personal data gathered from the web. Examples are location data that a cell phone transmits by GPS signal or web services with face recognition function. It should also not be possible to view search requests since these could allow conclusions to be drawn about the person performing the search.

Request for information

Customers can ask a non-governmental body to provide information, free of charge, on the stored customer data, the purpose of the storage, the people and agencies to which the customer's data are regularly transmitted and the origin of the data.

Smart grids

Intelligent power grids (smart grids) are capable of regulating the production of energy on the basis of measured load. They allow additional local energy producers, such as cogeneration plants, solar power plants or wind turbines, to be added or removed as needed.

Smart metering

The service consists of the reading, processing, presentation, and billing of power and energy consumption, and other meters in industry and homes. Smart metering reduces costs considerably and allows access to a mass-marketable service. In particular, it gives energy providers, meter operators, and the housing sector the opportunity to offer their customers innovative products and services, as it delivers consumption data virtually in real time.

Social media

Social media refers to the wide range of digital media and technologies that enable users to interact with each other and organize media content individually or in communities. Examples include Twitter, Facebook, Xing, and LinkedIn.

Telekom Deutschland GmbH

The previously independent business units for fixed network (T-Home) and mobile communications (T-Mobile) in Germany were consolidated into Telekom Deutschland GmbH on April 1, 2010.

Traffic data

As defined in the German Telecommunications Act, traffic data is data collected, processed or used in the provision of a telecommunications service.

WPA2-PSK

An encryption method for wireless networks.



Abbreviations.

BDSG	Federal Data Protection Act (Bundesdatenschutzgesetz)
BfDI	German Federal Commissioner for Data Protection and Freedom of Information
BITKOM	German Association for Information Technology, Telecommunications and New Media (Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V.)
ciAM	Corporate Identity Account Management – manages digital identities for users and workstations within Deutsche Telekom
CEM tool	Customer Experience Management Tool
DRC	Data Privacy, Legal Affairs and Compliance Board of Management department
GBS	Group Business Security
GIS	Group IT Security
GPR	Group Privacy
GSMA	Global System for Mobile Communications Association (formerly Groupe Speciale Mobile Association)
GSP	Group Security Policy
IPC	International Privacy Circles
KEK	Group permission clause
PSA	Privacy and Security Assessment
T-Labs	Telekom Laboratories
TKG	Telecommunications Act (Telekommunikationsgesetz)
TSG	Telekom Shop Gesellschaft



Imprint.

Deutsche Telekom AG
Corporate Communications
Postfach 2000, 53105 Bonn, Germany
Phone +49 (0) 228 181 4949
Fax +49 (0) 228 181 94004

www.telekom.com

Concept:
Deutsche Telekom AG and
HGB Hamburger Geschäftsberichte GmbH & Co. KG, Hamburg

Design and production:
HGB Hamburger Geschäftsberichte GmbH & Co. KG, Hamburg

Photographs:
Deutsche Telekom AG, Getty Images, Wolfram Scheible

Reproduction:
PX2@Medien GmbH & Co. KG, Hamburg

Printing:
Broermann Druck + Medien GmbH, Troisdorf

KNr. 642 100 151 (German)
KNr. 642 100 152 (English)

Contact.

Datenschutz Deutsche Telekom AG
datenschutz@telekom.de
www.telekom.com/datenschutz



Deutsche Telekom AG
Friedrich-Ebert-Allee 140
D-53113 Bonn
Germany

www.telekom.com