Report Data Privacy and Data Security 2011.

Life is for sharing.

Report Data Privacy
and Data Security 2011.

About this report.

The report on Data Privacy and Data Security at Deutsche Telekom looks back at a four-year history and a broad basis of further development. With the current report, Deutsche Telekom remains faithful to our principle of revealing how data privacy and data security are implemented within the Company to our customers, supervisory authorities and committees, politics, shareholders and employees. At the same time, the Group provides information about the primary structures and processes utilizing the data with which we have been entrusted. Last but not least, the Company states our position in the political and legal discussions on current data privacy issues and participates in the political and technical debates on data security matters.

The familiar structure of the report has been kept: the management report contains an overview of special events in data privacy and data security in 2011, both within and outside the Deutsche Telekom Group. In the same section, the Company also extends a view to the future of both topics. The section on data privacy in detail examines developments and events in data privacy and data security for specific target groups. Deutsche Telekom makes our in-depth expertise on safer surfing in the Internet available to customers and interested parties in a wide variety of formats. This service commitment is also reflected in the current report: interested readers will find the latest version of the guide here.

With our open information policies and active participation in the debate on data privacy and data security, Deutsche Telekom will continue to embed and advance these subjects in the public awareness, as well as in the political realm and the expert communities.

Contents.

Foreword by the Board of Management.

Dr. Manfred Balz

Dear Readers,

When something is important to us, we want to make sure it is in safe hands: we only entrust our children to reliable childcare providers. We handle our financial transactions with banks we believe we can trust. And our data? We prefer to entrust it in companies where we are certain it is well protected.

More than 170 million customers place this trust in Deutsche Telekom. We are aware of the great responsibility this entails: we work diligently every day to ensure that your data is protected against unauthorized access and openly communicate how we handle your data. Nature has developed sophisticated protective mechanisms with which species ensure their survival. We have to deploy the best processes and systems to protect what you entrust to us. We have accomplished a great deal toward achieving this goal. All the same, we must maintain our diligence as we look ahead.

> “Nature has developed sophisticated protective mechanisms with which species ensure their survival. We have to deploy the best processes and systems to protect what you entrust to us.”

Data privacy is increasingly being negotiated on the international stage, with the aim of setting cross-country standards. As an international company, we welcome this development. Another form of internationalization is also attracting our attention, however: cyber-attacks are increasing worldwide, with attackers routing their malicious coding through servers all over the world in just seconds, rendering them unidentifiable. We have to be vigilant and know the attack patterns in order to defend against them. We have to develop security solutions and exchange information with companies and politics to this end. We also have to get involved in political debates on data privacy and share our experiences. And above all: we must continue to clearly communicate what we do with the data entrusted to us – and what we don’t do! Our Data Privacy Advisory Board, consisting of independent experts, helps us interact with society and politics – in our common interest.

Deutsche Telekom has pursued a path of analysis, interchange and transparent communication of results for many years now. So far very effectively. The future will show us the destination of this path in the long term. But one thing is certain: we will continue to follow it and are pleased to have your company.

I hope you find the report enjoyable reading.

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

Management report.

Curling up into a ball may be an effective strategy for hedgehogs, but modern companies rely on open communication to build trust.

2.1. Overview of data privacy and data securityin 2011.

The year 2010 gave new impetus to data privacy and data security: a broad public debated for weeks over how personal data must be defined in the Internet age and how personal data can be protected adequately. This discussion continued into the year 2011, gaining momentum at the same time: questions about state monitoring and the necessity to analyze massive amounts of data were a repeated subject of debate. In Germany, this subject dominated the media for weeks after the announcement that cellular phone stations had been analyzed during a demonstration in Dresden. Kindled by the discovery of a neo-Nazi terrorist cell in Saxony and fomented through campaigns by various groups, the subject of mass data retention was the center of many controversial public debates. At the same time, American Internet services were subject to critical examination as a result of new functions on Facebook and new terms of use for Google products.

Data security – and especially “cybersecurity” – received unprecedented public attention in 2011: millions of hacked customer accounts at Sony and hacking incidents at FBI websites perpetrated by “Anonymous” demonstrated the scope and quality of Internet-based attacks to a wide audience. The constant threat posed by the Internet was also underscored by the announcement of successful investigation by the FBI, carried out under the code name “Operation Ghost Click”: after five years of work, the FBI arrested cybercriminals in Estonia who had infected millions of computers around the world with the “DNSChanger” virus. This criminal energy did not spare Deutsche Telekom customers, either: of the four million infected computers worldwide in early 2012, 16,500 belonged to Deutsche Telekom customers. These customers were identified and notified. Together with the German Federal Office for Information Security (BSI) and the Federal Criminal Police Office (BKA), Deutsche Telekom provided the public with an online quick test that showed whether a given computer was infected. At the time this report went to press, on April 2, 2012, the website had been visited more than 20 million times. Some 80,000 visitors received a warning message stating that their computers were infected. This statistic may be inaccurate, however, because some media published a direct link to this warning message.

2.2. Special events in 2011.

Deutsche Telekom participation in initiatives for data privacy and data security.

In 2011, Deutsche Telekom continued to pursue its activities in the environmental and political spheres. In addition to delivering opinions on domestic and international legislative procedures, it was involved in associations and pan-company initiatives aimed at promoting the topics of data privacy and data security in business 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. At the national level, together with companies from the telecommunications and information technology sectors and the Bitkom industry association, Deutsche Telekom founded the registered society for self-regulation in the information economy , called „Selbstregulierung in der Informationswirtschaft e.V.” The society will develop self-regulatory approaches in future, such as the data privacy codex for geodata services Ⓖ. In an initial step, the association will set up a central information and objection website for geodata services and a telephone advisory service during the course of 2012. The foundation was occasioned by public debates and information requirements that arose from services such as Google Street View.

Another field of activity at Deutsche Telekom was cooperation in developing a voluntary commitment by the online advertising sector, under the umbrella of the German advertising association Zentralverband der deutschen Werbewirtschaft (ZAW) and the Bundesverband Digitale Wirtschaft (BVDW), the organization that represents the interests of companies in the field of interactive marketing, digital content and interactive added value. The aim of this voluntary commitment is to improve the transparency of online behavioral advertising for consumers and to create an institutional framework through the founding of an online advertising council.

At the same time, Deutsche Telekom is an active participant in political processes intended to improve data privacy and data security. In particular, Deutsche Telekom participated in the German IT summit for this purpose. It also participated in discussions regarding the establishment and charter of the planned Privacy Foundation and ensured its support for the facility.

A further commitment of Deutsche Telekom was its participation in the "Security promoter group" of the Research Union Ⓖ of the German federal government. This advisory committee supports the work of the German government with suggestions for more effective protection of communications networks. In particular, this involves areas of research aimed at strengthening the level of privacy and data protection through new technological approaches.

Assessment of Group-internal data privacy.

A study to assess Deutsche Telekom's Group-internal data privacy organization took place on the company's own initiative. This study was carried out by an external auditor. Its subjects were the monitoring processes and structures that cover not only the relevant legal requirements, but also more extensive internal regulations. In the final result, the auditors confirmed that Deutsche Telekom demonstrably implements the required and voluntary controls and that the high level of data privacy targeted by Deutsche Telekom is actually achieved.

Data privacy solution for anonymous Internet surfing with IPv6 addresses.

In November 2011, Deutsche Telekom became the first telecommunications company to introduce a solution for anonymous surfing with the new Internet standard IPv6. Through a three-tier procedure, the two different components of the new IP addresses that will come into effect in 2012 can be effectively obscured. IP addresses that are allocated during Internet use are a prerequisite for surfing the Internet with a given device (such as PC, laptop or smartphone). The developed data privacy solution lets users decide for themselves how anonymous they wish to surf the Internet and conceal their identities. As a result, Deutsche Telekom goes beyond current German laws governing informational self-determination. The product launch is planned for 2012. During the transition period, both the existing IPv4 and the new IPv6 standards will be supported (see page 24).

Individual compensation payments for victims of the "spying affair".

The so-called "spying affair" at Deutsche Telekom was tried before the courts in 2010. The main criminal trial at the Bonn regional court ended with a conviction of the former Group Security department head: as the main defendant, he was sentenced 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 in late November 2010. The ruling had not yet become enforceable at the time this report went to press in early April, 2012.

As a result of the spying affair, Deutsche Telekom donated some 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 (see Report – Data privacy and data security in 2010). Over the course of the year 2011, Deutsche Telekom also reached agreements on individual compensation payments for journalists and others (such as family members) who had been spied on.

2.3. New legal provisions.

The legislature took further important steps in 2011 toward the improved protection of data. At the German and European level, there were changes and amendments to laws governing telecommunications service providers such as Deutsche Telekom. These include the Telecommunications Act, which includes improved provisions for consumer protection and data privacy, and is intended to reinforce confidence in the telecommunications market. In particular, this includes strengthening consumers' legal rights in the handling of their sensitive customer data. The Employee Data Protection Act is primarily intended to limit preventive screening of employee misconduct and is to be integrated in the German Data Protection Act. At the European level, the planned EU Data Protection Regulation aims to harmonize data protection rules, to give consumers a uniform level of consumer protection within the EU. The legislature continued to pursue these amendments in 2011; they are slated to take effect in the course of 2012 and in 2013/2014.

As a leading provider of telecommunications products and services, Deutsche Telekom contributed to the three legislative procedures from an early stage. The goal is to give customers the maximum possible legal certainty and protection in the use of their personal data and information. With the rapid implementation of current and future legislative changes, Deutsche Telekom does its part to ensure compliant data privacy in a world of connected life and work. The sections under “Developments in individual areas” describe the legal changes in data privacy and data security in detail.

2.4. Audits and inspections by external and internal bodies.

Internal and external bodies audited the systems and processes at Deutsche Telekom once again in 2011. External audits and inspections take place either through public supervisory authorities or within the framework of certifications, the latter usually through external bodies. As part of its due diligence, Deutsche Telekom and the Board of Management department for Data Privacy, Legal Affairs and Compliance carries out an additional, internal inspection function: the company internally verifies compliance with legal regulations and its own security and data protection rules. In doing so, the company continuously maintains a level of protection that is among the highest in the telecommunications industry. At the same time, the insights gained in the process are directed toward the further reinforcement of data privacy and data security. With these measures, Deutsche Telekom aims to take the leading position in the 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, as well as the German Federal Network Agency Ⓖ, regarding current issues related to data privacy as well as the measures taken at the company. In addition to its legal notification and reporting requirements, Deutsche Telekom involves the supervisory authorities in critical data protection issues at an early stage, to promote transparency and cooperation. In February 2011, the German Federal Commissioner for Data Protection and Freedom of Information paid a consulting and inspection visit to Congstar GmbH, a subsidiary Ⓖ of Telekom Deutschland GmbH. Its objective was to inspect the collection and processing of customer data.

A high level of data privacy and data security requires audits and inspections from external and internal bodies.

Audits and certification.

Deutsche Telekom also continued to develop and expand its certification and audit activities Ⓖ in 2011. In addition to inspections by state supervisory authorities, the central departments carried out 220 audits on data privacy and data security. To maintain a continuously high level of data privacy at the point of sale, the company carried out repeated inspections of its Telekom Shops to verify compliance with data privacy requirements. The data privacy and data security-relevant processes at the Telekom Shops were once again audited successfully by DEKRA Certification GmbH in 2011. Like in the previous year, Deutsche Telekom’ certification under the international ISO/IEC 27001 Ⓖ standard was confirmed for its security management system and departments of Telekom Deutschland GmbH, which was founded in 2010. Group subsidiary T-Systems also continued the process of certifying its German organization and 19 national companies in 2011. The goal of this process is to obtain the umbrella certificate for the introduction of a Group-wide information security management system. In addition, 188 ISO/IEC 27001 audits were carried out at Deutsche Telekom alone in 2011.

2.5. Provision of information to public authorities and individuals.

Queries addressed to Data Privacy.

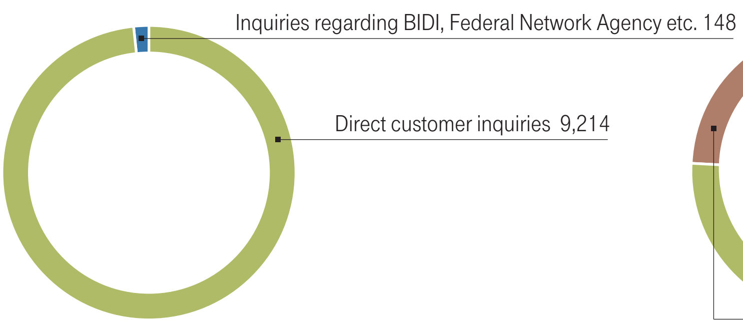
Queries involving data privacy declined in the year 2011. Whereas Deutsche Telekom received 10,808 queries in the year 2010, through regular mail, fax or online channels – either directly to Group Data Privacy or specifically configured service addresses – the number of queries received in 2011 declined to 9,362. Most of the inquiries received in 2011 came through the special service e-mail address datenschutz@telekom.de. Around one-eighth of all queries were sent directly to the Group Privacy Officer. Of these, 148 were sent by the German Federal Commissioner for Data Protection and Freedom of Information and others by the Federal Network Agency.

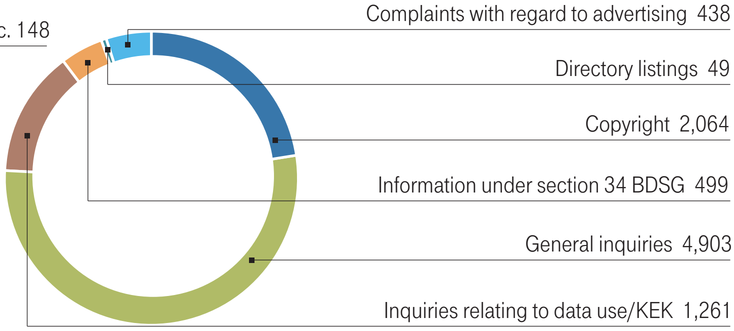
The largest number of queries, 2,003 in the previous year, involved warnings of alleged copyright violations. This inquiries concern the type of customer data disclosed to a third party, the so-called holder of the right, in a specific instance. Copyright inquiries are submitted primarily by customers 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 by their legal representatives. Inquiries involving copyright violations are often followed by requests for information under section 34 of the Federal Data Protection Act (BDSG), since the affected customers request an explanation of the forwarding of their data and the underlying legal basis (see page 15 for more information).

Another part of the inquiries involved requests for information in accordance with section 34 BDSG, which were submitted to Deutsche Telekom for no specific reason. 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 and, in particular, the origin of the data. These inquiries relate to all data stored on the customer.

Inquiries relating to the Group-wide consent 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.

Distribution and type of customer inquiries submitted to Group Privacy





Total inquiries* 9,362
* Internal inquiries not included

Another reason why customers contact Deutsche Telekom is to obtain advice on security questions (PC protection, viruses, worms, spam, phishing etc.) and dealing with personal data in social media. Deutsche Telekom makes a contribution toward security in the Internet through practical tips and targeted assistance and increases customer awareness for data privacy and data security issues (see page 57).

Contacting Deutsche Telekom.

Customers who would like to receive information about their personal data stored by Deutsche Telekom are invited to use the following information channels:

Mail: Group Data Privacy Officer
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany

E-mail: datenschutz@telekom.de

Queries addressed to Employee Data Privacy.

Employees can contact Deutsche Telekom with technical questions involving their projects, as well as personal questions dealing with their employment at Deutsche Telekom. During the year under review, 2011, the company processed 2,179 inquiries and submissions. These were received by regular mail, fax, phone and online communication. While some two-thirds of the inquiries involved technical questions, 682 transactions concerned data processing for specific employment relationships. Frequently asked questions included how personal data is passed on to external service providers in performance records, which data privacy rights have to be observed in substitution rules for access to e-mail and calendar applications and how documents are handled for electronic personnel files. Other questions asked in 2011 included data privacy-compliant procedures for employee surveys and the handling of vacation lists.

Queries to the Deutsche Telekom CERT.

The Cyber Emergency Response Team (CERT) at Deutsche Telekom bears international responsibility for crisis management and incident management involving cyber-activities within the Deutsche Telekom Group. In addition, the CERT is the main point of contact for inquiries and security notifications from external persons and organizations. Internet service providers, law-enforcement agencies and authorities and the security community contact the CERT to make them aware of security incidents and threads that could affect Deutsche Telekom AG and its customers. Examples of this include information about the distribution of illegal content in the Internet or the creation of phishing websites. 681 messages were received in 2011 through the official CERT gateway – CERT@-telekom.de. 109 of these messages were so serious that they were classified as cyber incidents and handled by the CERT.

Contact with the Deutsche Telekom CERT.

Persons outside Deutsche Telekom can contact the CERT to report security incidents that threaten Deutsche Telekom or through which Deutsche Telekom services threaten third parties. The following contact e-mail address can be used: **cert@telekom.de**

IP addresses.
An IP address (Internet Protocol address) is required to use 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 dynamic IP address. This principle will be retained upon introduction of the new IPv6 standard (see page 24). 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) and section 109 Telecommunications Act (TKG).

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.

Inquiries relating to copyright violations.

In the year 2011, Deutsche Telekom received temporary orders for the preliminary storage of around 100,000 IP addresses per month on average. The holders of the rights or their service providers determined these addresses during searches for copyrighted works being offered over the Internet.

No reliable figures exist on the development of copyright infringements. However, with 1.23 million temporarily saved IP addresses in the year 2011, Deutsche Telekom recorded a decline of some 50 percent compared to the previous year. There are no meaningful empirical investigations as to the cause of this decline. Two likely reasons, however, are that customers receive general information about this topic when concluding contracts and that instructions for use – of WLAN routers, for example – contain a section with information on encryption and security standards. Another possible reason could be the increased use of legal platforms. Overall, customers have been made more aware of the issues involved in file sharing and the related wave of lawsuits from copyright owners and their service providers.

Complaints to Deutsche Telekom from users whose data were passed on to third parties also declined in 2011. There are no clear reasons for this drop. However, one reason could be the advisory brochure for customer data privacy developed by Deutsche Telekom, which indicates data privacy and security measures for user devices.

Telecommunications monitoring under section 110 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 (Bundeskriminalamtsgesetz) 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 public authorities. 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.

2.5.8. Further development of information provision.

The founding of Telekom Deutschland GmbH in the year 2010 made it necessary to identify differences in the provision of information between T-Mobile GmbH on one side and Deutsche Telekom AG (T-Home) on the other side and to harmonize the procedures 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 has revised its practices for providing information to public authorities in 2011. The goal of the project was and remains to draw up a reliable guide for providing information to authorized public authorities. The project was carried out over the course of 2011; its results were presented to the Data Privacy Advisory Board at Deutsche Telekom in February 2012. The Data Privacy Advisory Board confirmed that the practices for providing information to public authorities are based on clearly identifiable legal foundations and are very structured and documented. Independently of this, Deutsche Telekom remains committed to promoting a more detailed specification and standardization of the basic legal conditions for providing information at the national level.

2.6. Research and development.

Deutsche Telekom does not rely exclusively on in-house skills in the development of innovative products and solutions. Instead, it teams up with scientific institutions to gain insights from new perspectives, which are an important component of the company’s innovation strategy. In this process, both internal developers and scientists consider aspects of data privacy and data security at the feasibility study stage – even before the development phase of a service or product begins.

An important facility for research and development is the Telekom Innovation Laboratories (T-Labs), which was founded together with Technische Universität Berlin (TU) () in 2005.

Data privacy and data protection for consumers and business customers enjoy high priority in the research work of T-Labs. Here are just a few examples from the year 2011 and the first weeks of the year 2012:

- At CeBIT 2012, Deutsche Telekom launched the third version of simko (short for “secure mobile communication”), a new standard for secure mobile working scenarios. simko an extremely secure smartphone on one hand, and on the other hand is a unique model for ensuring data protection and safeguarding telephone conversations against tapping and eavesdropping. Mails, contacts, appointments, SMS texts, photos, voice recordings and telephone calls are completely encrypted and stay within the customer's infrastructure. Working together, T-Systems and Telekom Innovation Laboratories have developed a secure software architecture for smartphones – a kind of "Fort Knox" for data protection in telephones. So-called micro kernels enable the creation of two secure "worlds" in a single device: one is an open public realm; the other is a high-security realm for business matters. Thanks to encryption, the information on the smartphone is safeguarded even if the device is lost or stolen. This structure also makes it possible to expand the existing simko solution to include tablets and notebooks.

- SmartSenior: intelligent assistant systems for senior citizens help older people to lead independent, carefree lives at home for as long as possible. T-Labs is heading the SmartSenior project of the German Federal Ministry of Education and Research. Its goal is to develop an integrated overall concept comprising health, security, services and communication solutions with standardized and intuitive user interfaces. The digital communication and data processing of the assistant system is to be protected, for example, to enable the secure exchange of healthcare data with a home care service. Deutsche Telekom prepared a major field test in 2011, as part of the development phase, to guarantee data privacy and data security for test users. In addition, the developers worked with the privacy officers of the involved partners to develop the processes to ensure privacy-compliant test operations in 2012.

- Identification of irregularities in datasets: as part of a research project, Deutsche Telekom examined data using methods from the machine learning and artificial intelligence areas. Objectives of the project include early recognition of server failures and detection of misuse in Internet portals. The test data required for these scenarios need a high degree of anonymization. Data Telekom guaranteed this in close cooperation with the data owners and Group Data Privacy.

- Data storage in cloud solutions: companies and consumers can now order software on demand from the Internet. In these cloud solutions, data is stored physically on servers that can be anywhere in the world. As a result, business customer data, product data and billing data are often subject to different jurisdictions and inspection by the authorities. As part of a research project, Deutsche Telekom is continuously developing and enhancing technologies and solutions to satisfy the increasingly demanding privacy requirements of companies and consumers.

- SIM authentication: in another research project, Deutsche Telekom is developing and testing the use of SIM cards for the secure authentication of Internet services. It aims to give users more secure, easier to use access to their e-mailboxes, for example, through a smartphone. As a result, password entry could be replaced by use of a short PIN. At the same time, the cell phone numbers could be anonymized, making it impossible to send advertising texts or calls to the number saved by the Internet service.

- In addition to research in T-Labs, Deutsche Telekom works together with public and private scientific organizations, research institutions, universities and companies. It supports the chair of "Mobile Business & Multilateral Security" (www.m-chair.net) at Goethe-Universität Frankfurt am Main, which deals with data privacy issues in next-generation mobile communications within the framework of various European projects:

- The PICOS project examined how users can protect their privacy while using social networks with mobile devices such as smartphones. To date, users only have limited possibilities to restrict access to personal data and content on a situation-specific basis. The project aims to give them tools to determine for themselves, in every situation, which location and context information they want to reveal. This includes partial identities, which enable users to act under different pseudonyms. The concepts developed in the PICOS project were implemented in two mobile applications and evaluated by users.

- The PrimeLife project develops concepts and technologies for the privacy-friendly design of identity management systems. Among other things, the endowed chair has developed a method for the economical assessment of functions for protecting privacy. To date, the monetization of customer information that companies gain from their communication services was part of many telecommunications providers' business models. But which competitive advantages do companies gain from giving their customers privacy-friendly functions? One example is a concept for identity management that goes beyond mere compliance with legal requirements, instead focusing on the privacy needs of users.

2.7. Outlook for data privacy and data security in 2012.

In the past months and years, Deutsche Telekom has established a name for itself, and not only in data privacy. The company's experts are also welcome guests at national and international cybersecurity symposia, as well as respected partners to business, politics and public authorities. In particular, the concept of privacy and security by design – the integration of security and data privacy during the development of processes and products – was very well received in 2011. Likewise, Deutsche Telekom's early-warning systems to identify attack patterns from the Internet, which were developed in 2010 and enhanced in 2011, were met with keen interest. New technical developments and enhancements by Deutsche Telekom for the early warning and identification of cyberattacks can also be expected in 2012: 50,000 to 60,000 new viruses, Trojan horses and worms that infect user devices as malware appear around the world every day. In future, this high number will require security technologies and systems that enable valid identification in real time.

Deutsche Telekom will continue to expand its early-warning systems in 2012, such as its honeypot systems (see page 40), to identify attack patterns and new trends in cyberattacks. The company is pursuing a policy of making its technology available to other companies and organizations and consolidating the respective results for the online protection of customers. To this end, Deutsche Telekom will increase the number of its mobile honeypots in 2012, which make the company the first telecommunications provider in Europe with the ability to analyze network-based attacks on smartphones.

Thanks to sophisticated early-warning systems, Deutsche Telekom can identify attack patterns from the Internet. It will continue to expand these systems in future.

A lack of information regarding potential security vulnerabilities remain a root cause of successful cyber-attacks on companies and customers in 2012. Deutsche Telekom already relies on intensive cooperation with public and private organizations to learn from attacks. In future, this cooperation could lead to the publishing of security standards for technical experts and the online community. With this approach, Deutsche Telekom seeks critical discussion with the Internet community, inviting critics and experts to work together to develop better security standards and protection concepts.

In cooperation with other providers and equipment manufacturers, Deutsche Telekom will support the joint efforts of the industry in 2012 to place the information and data itself at the center of the protective measures, and not only the devices. In future, data security in the Internet should also be contained in the information itself – comparable to today's digital rights management of working documents. To this end, Deutsche Telekom is conducting talks with several different manufacturers to help develop solution approaches for the next generation of products.

In light of the high threat level from Internet-based attacks and increasing public awareness of cyber risks, providers and manufacturers can no longer afford to develop their products without the latest protection technologies or publish them without sufficient security tests. Deutsche Telekom will continue to develop its PSA (Privacy and Security Assessment, see page 41) process, which was rolled out internationally in 2011. This process integrates the requirements for technical security and data privacy in product and system development from the very first development step. More than 2,000 projects currently go through the PSA process each year, increasingly making it a model among experts. In addition, Deutsche Telekom will continue to encourage its partners and suppliers to firmly embed technical security and data privacy as design criteria for products and services. Digital security tests should become mandatory prior to market launch. This will help increase the level of protection in products and services for all providers and manufacturers, to protect customers against cybercrime and Internet threats.

Aside from the establishment and further expansion of technical security measures, Deutsche Telekom is continuing its broad spectrum in data privacy in 2012. Employees and users must be sensitized to the risks to ensure safe, self-confident interaction with the online world. To this end, the company has started a project to introduce children and young people, as well as their legal guardians, to the opportunities and risks associated with the Internet at an early stage.

Security and data privacy in the cloud will also be one of the most important topics at Deutsche Telekom. Cloud solutions are already an integral component of many company IT models. More and more private users no longer want to store their data and software on home computers or on their smartphones, either. At the same time, they insist – justifiably – on the high data privacy and security standards of Deutsche Telekom. The company hopes to achieve comprehensive security standards through the development of standardized certification methods for cloud services. To do so, it will actively support the initiatives by the Bitkom electronics industry association and the Federal Office for Information Security in Germany in 2012, as well as fight for the establishment of independent security certifications for cloud services.

Several major developments are expected in the legislative area in 2012: Deutsche Telekom is focusing on the implementation of new legal regulations, such as the Telecommunications Act Ⓖ. It is also preparing intensively for the expected amendments to employee data protection and continues to make constructive contributions to the debates.

At the same time, the first draft of standard rules on data protection for Europe, the EU Data Protection Regulation, was presented at the start of 2012. This approach to harmonization will deliver many positive aspects and impetus for business, as well as the citizens of Europe. Deutsche Telekom will continue to support this approach and seek a dialog with representatives of the European Parliament, to present the regulatory demands it has identified through the course of its business operations.

In the healthcare area, special attention will be paid to support for the new business models at Deutsche Telekom. This includes examination of the applicable legislative framework, such as the German criminal code, which forbids the dissemination of patient data under penalty of law. Such regulations have to be reexamined in light of the current security and protection mechanisms of possible business processes and IT processing. All the same, the measure of all things is and remains the high demands on the integrity and protection of patient data.

Developments in individual areas.

Those who conceal themselves well avoid discovery.
When it comes to data privacy and data security,
Deutsche Telekom has nothing to hide.

3.1. Consumers.

Legal provisions.

Following agreement by the Bundesrat and Bundestag Mediation Committee regarding the amendment of the Telecommunications Act, the new law is slated to take effect in the second quarter of 2012. Among the changes to the Telecommunications Act, new consumer protection regulations prohibit operators from charging callers for time spent on hold with toll numbers. The treatment of location-based services Ⓖ) services is regulated in section 98 Telecommunications Act. Service providers are not allowed to process location data or forward it to providers of additional services without prior consent by the user.

Moreover, additional information requirements have been introduced in section 98 Telecommunications Act, with the aim of better protecting sensitive data and thus strengthening consumers' legal standing. Among other things, this includes a requirement to display a message to the user whenever he is being localized through his mobile device. These changes will result in more transparency and legal certainty for consumers.

In the framework of implementing European directives, the reporting requirements of telecommunications providers have been extended for privacy incidents. section 109a Telecommunications Act requires immediate notification of violations of privacy if they result in serious repercussions for consumers. These extended notification requirements of privacy violations will result in greater transparency for data security and data privacy. In comparison to the existing reporting requirements, under which the telecommunications companies only had to notify affected parties when data was improperly transferred to third parties, they now also have to report when data is improperly deleted or modified by the provider internally. Deutsche Telekom began voluntary reporting of data incidents long before this legal requirement came into effect, as the first company in Germany. As such, it sees itself well-prepared to deal with the new reporting requirements. Deutsche Telekom considers the solution for improving consumer and privacy protection to be very positive. Also worth mentioning is the elimination of section 92 Telecommunications Act, which regulated the requirements for transferring personal data to non-public

Dr. Claus-Dieter Ulmer
Group Data Privacy Officer,
Deutsche Telekom

Data privacy is an issue around the world, but usually only at the individual country level. Don't we need an all-encompassing view of data privacy? Do we need to rethink national barriers?

The question as to how we can establish globally valid, reliable data privacy standards in the face of individual country regulation is currently being debated vehemently. Reaching a positive result is essential to the success of the entire Internet and IT sectors worldwide. Business models cannot stop at country borders. Yet right now, differing data privacy laws can have that very result. A strict, transparent, reliable global standard would enable entirely new approaches, while at the same time represent a confidence-building measure for customers. Customers have to be certain that their personal information is in good hands around the world. Only then will they begin to really use the new business models.

In particular, the European Union took a major step toward a harmonized right to privacy in 2011 and 2012, with their planned amendment to the EU Data Protection Directive. At least within Europe. This harmonization was long overdue, both to provide transparency for customers and to ensure a level playing field for companies. In the next step, approaches such as the planned regulation must set a precedent worldwide. In harmony with business, consumers and privacy protection.

bodies within the EU. This elimination will simplify the transfer of telecommunications data, which was previously subject to particularly severe restrictions that went far beyond the general protection level of the Federal Data Protection Act. In one example, the name and address of a subscriber could not previously be passed on to an international subsidiary for processing there. Once the amended law comes into effect, international data transfers will now be uniformly subject to the rules of the Federal Data Protection Act for all industry sectors. As a result, telecommunications data can be processed abroad in accordance with general data protection regulations – a solution that Deutsche Telekom strongly favored. It gives the telecommunications industry the opportunity to operate in international business transactions on an equal footing.

Storage and security of customer data.

Each year, Deutsche Telekom stores and processes the data of nearly 60 million consumers in the fixed and mobile networks. The data is stored to enable the technical provision and billing of services; its use is described in the Group's data privacy notices. The national legislatures define the retention periods.

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.

Storage of radio cells.

Deutsche Telekom stores the radio cell where a mobile phone is currently located. This is done for technical reasons, for it allows mobile phones to be reached more quickly and more easily. As soon as a mobile phone changes cells, the old location is overwritten. As a result of this storage practice, it is not possible to reconstruct movement profiles of mobile phones after the fact. Likewise, it is not possible to past research locations of cell phones if no communication processes took place. In contrast, if the phone was used to communicate, the cell at the time of the process becomes part of the traffic data and is saved for 30 days. This data can be provided subsequently within this period.

Data storage.

Data stored at Deutsche Telekom. Deutsche Telekom stores customer data (master data) and data generated during the call (traffic data). The traffic data is technically required to set up and maintain the respective call. Subsequently, the data is used for billing 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:

- Phone number or identification of the calling and called line
- Service used
- Call start/finish
- In the case of mobile telephony, the location code, SIM card number and mobile device 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

Traffic data – retention periods at a glance:
Deutsche Telekom stores the traffic data that is required to establish and maintain connections, and for billing purposes, for 30 days. The company is working on shortening this retention period for data that is not needed for billing purposes. A minimum retention period is still needed for this information, however, to maintain technical operations and for troubleshooting. Billing data is stored for up to 80 days, provided the customer does not request immediate deletion after bills are sent. Deutsche Telekom deletes IP addresses that are stored as connection data during Internet surfing after seven days. Data that is required for billing with service providers is stored for six months, for invoicing purposes, and only in anonymized form.

Group-wide consent clause for using customer data.

Like many other companies, Deutsche Telekom notifies its customers of new and improved products and services. The Group uses existing customer data, such as name, phone number and currently used products 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 defined writing when an order form is signed, by phone with a subsequent confirmation letter or online. Customers also have the option of revoking a granted consent, if they decide they no longer want to receive such information. Deutsche Telekom's customers can view and change their consent status at any time on the customer service portal at www.telekom.de.

Data privacy solution for anonymous Internet surfing with IPv6.

In November 2011, Deutsche Telekom became the first telecommunications company to introduce a solution for anonymous surfing with the new Internet standard IPv6. Through a three-tier procedure, the two different components of the new IP addresses that will come into effect in 2012 can be effectively obscured for third parties. IP addresses that are allocated during Internet use are a prerequisite for surfing the Internet with a given device (such as PC, laptop or smartphone). The developed data privacy solution lets users decide for themselves how anonymous they wish to surf the Internet and conceal their identities. As a result, Deutsche Telekom does more than required by current laws. In Deutsche Telekom's opinion, this anonymization is necessary because the new IPv6 standard will provide more than enough IP addresses to supply a unique IP address to every user and every device worldwide. From a technical perspective, every user and device could keep its address permanently, enabling clear identification through this permanent address. As a result, it would be theoretically possible to create detailed movement and user profiles, which Deutsche Telekom's solution is intended to prevent.

The new IPv6 addresses consist of two parts (network prefix and interface identifier), each with a length of 64 bits. The protection model consists of three tiers: the first two tiers affect the network prefix assigned by Deutsche Telekom. As a result, in the first tier, all devices that are connected to an Internet access router provided by Deutsche Telekom (Speedport) are regularly assigned new, randomly selected network prefixes. This function is configured by default. Secondly, Deutsche Telekom will implement a "privacy button" in the configuration pages of the routers it supplies. Users can be assigned a completely new IPv6 prefix with a click of the mouse. This reassignment can take place manually or automatically at a specified time. Thirdly, on most modern devices, the device part of the IP address will automatically be obscured using random logic. Deutsche Telekom will inform its customers about the options for anonymized surfing. The product launch is planned for 2012. During the transition period, both the existing IPv4 and the new IPv6 standards will be supported.

Deutsche Telekom presented this solution to a trade audience at Dafta, a privacy conference, in Cologne in November 2011, as well as at an IPv6 symposium hosted by the German Federal Commissioner for Data Protection and Freedom of Information, Peter Schaar, also in November. The responses from both the experts and the German Federal Commissioner for Data Protection were positive.

Security of telephony in the GSM network.

At a security conference hosted by the Chaos Computer Club in Finowfurt, Brandenburg, in August 2011, cryptography specialist Karsten Nohl presented the technical possibility of decrypting protected data traffic in GSM networks, the global standard, under certain circumstances. His hacking attempts attracted broad media interest and involved mobile communications providers who use the GPRS standard to send data to the GSM network. Deutsche Telekom follows such experimental designs with great interest. Deutsche Telekom networks are highly resistant to eavesdropping. Criminal energy is required to overcome the existing security systems. Accordingly, the probability that a customer's data communication could be tapped or intercepted is low, representing more a theoretical possibility than an everyday scenario.
The security of the worldwide GSM cellular standard is not just the concern of individual manufacturers or network operators – it must be ensured industry-wide. For this reason, Deutsche Telekom is active within the global organizations GSMA (Global System for Mobile Communications Association) and 3GPP (3rd

Generation Partnership Project, a global standardization committee for mobile communications) that work to enhance security standards.

The company is continually improving its security systems – in line with technical progress – and raising the standards of current and future systems. Among other projects, Deutsche Telekom is working on the comprehensive implementation of the A5/3 encryption algorithm in its GSM, networks which meets even higher security standards. This algorithm is derived from UMTS networks. Nevertheless, the forced, network-side activation of this new encryption algorithm is not possible without further steps, because older mobile phones would be rendered in inoperable due to technical incompatibility.

For particularly high-security applications, Deutsche Telekom offers the simko solution, which features highly effective encryption between two devices.

Security and data privacy for users of the Telekom Cloud.

As a leading provider of cloud solutions, which let consumers, companies and public authorities order computing and storage capacity over the Internet – from the IT cloud – at the touch of a button, Deutsche Telekom introduced the Telekom Cloud for consumers in 2011. It is part of the “Cloud Store”, in which Deutsche Telekom also offers solutions for SME companies and corporate customers, in addition to consumers.

Wherever the Internet and thus the services provided online by Deutsche Telekom are available, customers can use their files and applications. And that holds true across all devices: PC, notebook, tablet PC, smartphone or TV – with the Telekom Cloud, users are no longer tied to technical platforms. For example, consumers can store their photos, music, e-mails and videos in the virtual media center, and access their encrypted data via the Internet. Users have access to a storage capacity of 25 gigabytes available from the cloud. The Deutsche Telekom broadband network ensures that the services are available.

As the data is stored only on servers in Germany, it is subject to the strict German data privacy provisions. Deutsche Telekom’s data centers meet the latest protection requirements, guaranteeing a high level of security and data privacy. All data stored in the Media Center is permanently protected from loss because the content is stored not only on the user’s devices, but also on Deutsche Telekom’s servers. The Deutsche Telekom Media Center was audited and certified for data privacy and security by TÜV Saarland in 2011. Fee-based Telekom Cloud services are settled through Telekom bills. So it is not necessary to state any credit card details. This, as well, improves data privacy and security.

All Telekom Cloud services undergo the PSA (Privacy and Security Assessment, see page 41) process during their development stage. This guarantees that requirements for technical security and data privacy are fixed components of product and system development. This included the advance implementation of product-specific security requirements, such as encrypted data interchange with the cloud, along with security reviews in the form of penetration tests Ⓖ and verification of compliance with statutory requirements and company policies. Cloud services offer a wide range of options for combining the Telekom Cloud with individual products from partner companies. To this end, Deutsche Telekom continued to enhance its guidelines in 2011 to guarantee a uniform level of data privacy and security for collaboration partners and service providers as well.

GSM.
GSM (Global System for Mobile Communications) is a standard for full digital cellular networks used primarily for telephony, as well as for short messages (SMS or texting). The aim of GSM was to give subscribers a pan-European mobile telephone system that offered voice services that were compatible with ISDN and conventional analog phone networks. It was introduced in Germany in 1992 and is now the most widely used mobile communications standard in the world. The standard has undergone several subsequent enhancements with faster data transmission speeds, including HSCSD, GPRS and EDGE. The GSMA industrial association represents some 800 mobile communications providers worldwide and has taken on the task of further enhancing GSM mobile communications and developing pan-network standards jointly.

Privacy-friendly “two-click solution” for Like buttons.

Recommendations of websites over social networks are becoming increasingly popular. Users of social networks such as Facebook can click the Like button to point out interesting pages to their Facebook friends. In general, these buttons transmit visitor data even if they are not currently logged on to the social network. Deutsche Telekom has developed a privacy-friendly solution to stop website visitors from sending their personal data to the networking platforms involuntarily. The telecommunications company offers users a modified Like button on its own websites. The Telekom solution is based on a two-click solution that has already been acknowledged by experts and many privacy advocates. This two-click solution only transmits data when users approve: the button does not send any data to third parties automatically. Users have to click the Like button once to grant their approval for technical communication with the social network servers. The button is then active and establishes a connection. The second click then activates the actual Like function.

Checking data deletion during device repairs.

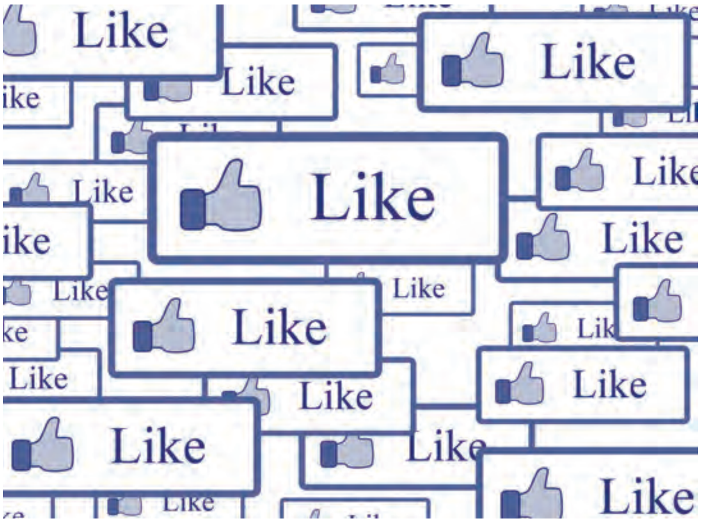
When customers send in devices (such as smartphones) for repair in Germany, they immediately receive a functional device from Deutsche Telekom’s replacement pool. Deutsche Telekom sends the defective device to the manufacturer or repair shop to be fixed. In this process, the customer is obliged to delete all personal data from his mobile phone before he turns it in to a T-Shop or sends it by post. Likewise, the manufacturers and repair services are contractually obligated to delete any data that may still be on the device. Deutsche Telekom investigated the entire deletion process, as announced in the 2010 reporting year. This investigation showed that the privacy-compliant deletion of all customer data is part of the standard process for repairs to which all manufacturers and repair services are contractually obliged: after it is repaired, every device is subject to a final inspection and subsequent additional check to verify that the device does not contain any customer data. The investigation also resulted in revised master contracts for manufacturers and repair services to standardize the models and compliance with data privacy requirements throughout the Group. If customers forget to delete their data from a device before turning it in for repair, the multi-step deletion and check concept at Deutsche Telekom guarantees compliance with data privacy requirements: of 500,000 exchange transactions in the year 2011, there were only ten documented customer reports of insufficient deletion.

Installation of the Carrier IQ software by smartphone vendors.

In late 2011, business and daily press in Germany increasingly reported on the “Carrier IQ” software, which is installed on smartphones from various vendors as part of the production process. This software is used for quality assurance by manufacturers and network operators. It can record various device data when defined events occur. The application can be adapted to the specific needs of the various manufacturers and network operators, a feature that many data privacy experts criticize. Deutsche Telekom does not use the Carrier IQ software, nor does it record any data with it.

Inspection of the security concept at Telekom Deutschland GmbH.

Before implementing technological and/or organizational changes, Deutsche Telekom is required to modify the security concept that is generally required under section 109 Telecommunications Act accordingly. 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. 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 agency confirmed the operability of the security concept in March 2011. In the third and fourth quarters of the same year, the supervisory authority also audited the implementation at selected sites. During the audits, only one recommendation was made – to install a privacy shield at one building – and was immediately implemented by Deutsche Telekom.



When the Like button from a social network is clicked, visitor data is transmitted. Under the “two-click solution”, this data is only sent with the user’s consent.

Deactivation of mass storage devices and external communication channels.

At the call centers that carry out customer service on behalf of Deutsche Telekom, the employees have workplace computers with USB ports. These ports are blocked by default at the call centers, to prevent data from being stored on external USB storage media and thus the unauthorized distribution of customer data. During an audit, Deutsche Telekom discovered that the USB port block was inactive on less than one percent of the devices used in customer service. The company eliminated this issue immediately. In addition, to further improve security at its agent call centers, Deutsche Telekom has blocked the option for sending e-mail to external addresses and visits to websites that are not essential to performing their duties (also see page 44).

Regulation of data access by Telekom Shop partners.

In Germany, sales and distribution for Deutsche Telekom are carried out by subsidiary Telekom Shop Gesellschaft mbH and its partners, among others. This sales business takes place based on strict data privacy agreements (agreement for commissioned data processing in accordance with section 11 of the Federal Data Protection Act) exclusively on the retail premises. The Telekom Shop partners have access to a central customer database, to assist Deutsche Telekom customers with contract and product inquiries. This access to customer data is clearly regulated and only permitted for the support of customers on the retail premises. There were indications in 2011 that the customer database had access rates by a very few sales partners that differed from normal use, which triggered internal audit procedures. The audit results showed that the database was not only used for the agreed-upon customer support, but also to check commissions, an option not provided for by the contract. Written warnings could only be issued in incidents for which timely investigation results were available. According to the findings to date, no misuse of the improperly accessed customer data occurred. Deutsche Telekom has streamlined its internal investigation process to respond to any unauthorized database accesses with written warnings more quickly in future. A letter has been sent to all sales partners reminding them of the valid data privacy regulations.

Management of performance records in telephone sales.

Following a tip from a regional works council member, Deutsche Telekom subjected the recording of individual performance records in telephone sales to a privacy audit. In individual call centers Ⓖ, team leaders recorded and processed personal data to document the achievement of revenue targets and sales figures by individual team members. They stored this information outside of protected IT applications, in an Excel file on their workplace computers. In addition, employees used an Excel file to document the progress of individual sales talks for their team leaders, to prove their contribution to the department’s revenue target. Deutsche Telekom has agreed with the specialist departments and co-determination committees to supply the operationally necessary performance figures to authorized user groups through an IT program called “KPI Viewer”. This program features role-based access to the key figures, so employees can only see the data that is relevant for their tasks. Access to person-specific performance KPIs is not possible. Deutsche Telekom has included these rules for managing performance records in call centers in a general works agreement, to ensure legal and privacy compliance throughout the company. Defined security mechanisms and procedures will apply during the transition phase to document where and how the KPIs are electronically recorded and viewed. All affected areas have been requested to destroy any existing printed lists immediately and delete electronic versions irrevocably. Implementation of the KPI Viewer program is to be completed by the end of 2012.

Unauthorized server access at ImmobilienScout24.

Unknown parties obtained unauthorized external access to one of the company servers at real estate portal operator ImmobilienScout24. Access was gained to the address and contact information, customer numbers and names of both commercial and private vendors. The data itself was largely already available on the ImmobilienScout24 website as it is the standard information included in the contact field for real estate advertisements. Data was also taken from contact forms, such as catalog requests or inquiries. No passwords, bank details or other financial data were taken. ImmobilienScout24, a subsidiary of Deutsche Telekom, blocked the unauthorized access path immediately and has since restored the security of the server attacked. Vendors and users have been notified. The company has filed charges against an unknown party with the public prosecutor's office in Berlin.

Technical malfunction in the T-Online customer portal.

In September 2011, Deutsche Telekom discovered irregularities in interfaces to IT systems that support the operations of the T-Online customer portal on the Internet. A customer complained that he could see other customers' data when viewing his order in the password-protected area of the portal. The corresponding functions of the customer center were deactivated temporarily as a precaution. The cause of the malfunction was found to be a data error in a software release that theoretically could have resulted in the incorrect display of 300 customer data records. The malfunction was corrected within just a few hours, in close collaboration with Group Data Privacy. During the maintenance work, customers could contact the phone support hotline. According to present knowledge, before the customer portal was deactivated, ten customers were shown incorrect customer data; no misuse of the billing data is known. Deutsche Telekom sent the affected customers a written notification of the incident.

Cloud computing has long become a part of modern IT infrastructure. It offers a wide range of benefits to both consumers and business customers.

Incorrect documents sent to an attorney's office.

Between April 14, 2011 and May 10, 2011, six e-mail messages with documents from three customers who are claiming damages against Telekom Deutschland GmbH in court were sent to an incorrect e-mail address, due to human error. The e-mail attachments contained copies of the disputed bills, mobile phone contracts and account statements. The invoices contained address, customer number and bank data. When the error was discovered, the Company immediately asked the incorrect recipient to delete any e-mail messages that were not intended for him personally. Deutsche Telekom notified the affected customers about the incident and contacted them to ask whether they would like a new customer number.

3.2. Business customers.

Certification as a service provider for De-Mail.

In the second quarter of 2012, Deutsche Telekom launched its De-Mail Ⓖ service, following its certification as a De-Mail provider by the Federal Office for Information Security. De-Mail is a service for the simple, secure, documented exchange of electronic messages. Within the certification framework, an external auditor reviewed the business units of Deutsche Telekom that are responsible for compliance with data privacy and for the registration and identity verification of persons who want to use De-Mail. For the technical security of De-Mail, the Federal Office for Information Security reviewed Deutsche Telekom's IT systems and granted the accreditation. In addition to the external certification, Deutsche Telekom also conducted a successful internal audit of the De-Mail product. The objective here was to subject the peripheral systems that communicate with the official De-Mail system to a rigorous examination with regard to the Group's internal data privacy regulations.

De-Mail combines the advantages of e-mail with the reliability of a letter. 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 known from the Internet (websites with the URL https://) will therefore be used, among other things.

- 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 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 calculating the checksum of a long number by adding its individual digits. If a digit is changed later on, the checksum is also changed, indicating a modification. This check is carried out by the receiving provider, in principle, each time a message is transmitted.

Cloud Computing.

Cloud computing Ⓖ has become an indispensable part of modern IT infrastructures and offers numerous benefits to users. For business customers, the tremendous cost savings are the primary consideration. In addition, companies can make their cost structures more flexible and scale their IT on demand to deal with fluctuating loads. Providers of cloud products face special challenges, especially technical delivery and guaranteeing security. Deutsche Telekom set up a Cloud Store in 2011, in which it consolidates its offers for consumers, SMEs and corporate customers. All cloud offers are subject to strict security requirements.

At Deutsche Telekom, security and data privacy are guaranteed through the comprehensive collaboration of several departments within the Group. Group-wide expertise was already incorporated in the development of dynamic computing services. As a result, the IT Security area developed the technical security requirements. The Data Privacy area ensured that priority was given to protecting the processed and saved data, in the framework of the Privacy and Security Assessment (PSA, see page 41) process.

In cloud computing, all data and applications are stored at the data center. The security of this data depends on the respective cloud provider. Deutsche Telekom's data centers are security certified. T-Systems – the operator of the data centers – began offering cloud services to corporate customers in 2005. The Telekom subsidiary operates 90 high-security data centers worldwide. In particular, the data centers in Germany are subject to the strict German privacy laws, as well as EU regulations. Thanks to the high security standards for the data centers, T-Systems also fends off hacker attacks, along with viruses and Trojan horses.

Constant maintenance and automatic updates keep the security precautions up to date at all times.

If the customer requests it, the service provider can also encrypt the data for transport through the network. Another important factor is the availability of the cloud services. If one data center fails due to a local disaster or targeted attack, a "twin" can take over for it. In this twin-core approach for business customers, every data center has a complete mirror. Deutsche Telekom also has failsafe measures in place within the individual data centers, through redundancies to protect against the failure of individual systems.

As a vendor of cloud-based business models, Deutsche Telekom has been actively involved in political debates on security and data privacy in the cloud. Various company representatives have participated in working groups at both the national and European level, for example, with the European Commission and in the framework of the IT summit process. Deutsche Telekom has defined the following goals for its activities within the organizational and political spheres:

- Increase the transparency of privacy and security-relevant regulations for users
- Ensure high investment requirements in security
- Define benchmarks, such as data privacy and security certifications or seals of approval for cloud based solutions

Smart metering/smart grids.

More and more electricity customers are becoming electricity producers. The installed capacity of local photovoltaic systems now corresponds to that of 25 nuclear power plants – with one difference: the sun and clouds control these 25 nuclear power plants, destabilizing the electricity grid. For its performance fluctuates significantly. Digital meters show us what is going on in the electricity grid. They are the foundation for a smart grid that controls itself. But the transmitted consumption data is sensitive. Firstly, it allows conclusions to be drawn about the customer, and secondly, there is a risk of manipulation of the entire electricity grid. As a result, it is particularly important to guarantee a high level of data privacy and data security here.

Smart metering shows what is going on in the power grid – and is the foundation for smart grids.

Deutsche Telekom tested the use of smart metering in its T-City Friedrichshafen "model city" between 2007 and 2012 and further improved the security of the system based on the results. It decided, for example, to split billing relevant data from control signals for the connected home. Instead, there are two infrastructures: an ultra-secure communication box, which transmits all the consumption data from the house, and a home management box, which delivers information to the house.

Likewise, Deutsche Telekom attaches great importance to secure billing: the company transmits monthly figures to the energy provider for this purpose. The reading frequency corresponds exactly to the contract between the energy supplier and the consumer. If the consumer orders reading every 15 minutes, for example, then this exact reading interval is implemented. Telekom has implemented threefold protection against manipulation. Values are stored in encrypted form and transmitted through a secure transport channel. Moreover, neither the meters nor any other components can be reached through the Internet. As such, Deutsche Telekom offers an infrastructure for secure data transfer.

The legislature has also responded and commissioned the Federal Office for Information Security to elaborate a general protection profile and a technical guideline for smart metering. The final version of this guideline is expected in July 2012. They will regulate the intelligent metering, reading and transfer of electricity consumption by households. At the present time, however, this guideline only focuses on the control unit in the customer's household.

Deutsche Telekom sees a need for action here: smart metering requires an end-to-end consideration of the full systems, processes, usage scenarios and market roles, in the background of smart electricity grids. With its years of experience as a network operator, it has offered its services as a dialog partner in achieving this consideration and made specific proposals for ensuring a high level of security for smart metering Ⓖ and smart grids Ⓖ.

Privacy guidelines in the healthcare sector.

The healthcare sector is subject to numerous privacy provisions. Some are aimed at protecting personal social, patient and treatment data, while others guarantee the compliant use of medicines, cures and treatment methods. With its products and services for the healthcare sector, Deutsche Telekom is taking a leading role. This ambition goes hand in hand with a responsibility to provide healthcare facilities – such as hospitals and clinics – with privacy-compliant solutions at all times and to advise them as to how to best protect their patients' data. In this light, guidelines for dealing with sensitive healthcare and social data were developed for the hospital segment in 2011. There are plans to supplement the guidelines with examples of best practice approaches. The guidelines are intended for customers, sales and sales project managers. They aim to provide sensitization, orientation and information about the privacy requirements in the e-health area and emphasize the Group's privacy capabilities and competencies in the solution business. Among other things, the document discusses the privacy requirements, as well as the further development of specific solution approaches and procedures for implementing outsourcing projects and commissioned data processing. The inclusion of external service providers, in particular, confronts hospitals with complex privacy demands. The guidelines can also serve as a template for other business areas.

Smart metering.
Smart metering is a major component of smart electricity grids and provides utilities with information as to when, where and how much electricity is fed into the grid locally and how much customers use. Since 2010, the legislator has stipulated the installation of smart meters in new and renovated buildings.

With its metering services, Deutsche Telekom offers a data communications solution with a modular structure. This solution is aimed at the housing industry, meter operators, utility companies, sales organizations and distribution network operators. Business customers can integrate their smart meters with this communications solution, gaining access to an infrastructure for reading and transporting the data. Consumers also benefit from smart meters: customers can track exactly how much electricity they use – broken down by hour, day, week, month or year as desired. They enable comparisons with past values, as well as future interactive offers such as consumption forecasts, rate optimization and notification services that send messages when defined values are exceeded. Smart metering is used for electricity, as well as for gas, water and thermal energy.

3.3. Employees.

Employee data protection regulates how the data of employees and civil servants is handled, regardless of whether processing is automated or not. The rules for employee data protection specify the framework for legally allowed processing of employee data: they include the prerequisites for processing this data by the employer as well as protection of employee data against unauthorized internal and external use. In addition to the framework for authorized usage by the company in the course of establishing or maintaining an employment relationship, employee data protection also regulates the use of employee data in the detection of criminal offenses. The electronically connected workplace, in particular, results in complex requirements of the individual protective interests of the legislature, employees, customers and the company as employer.

The German government submitted a draft law on the protection of employee data in 2010. The first parliamentary reading of the Employee Data Protection Act took place in February 2011, during the year under review. Further consultation and passage of the law are expected in 2012. Deutsche Telekom supports this legislative initiative because it provides for more legal certainty.

Investigations against employees.
Deutsche Telekom has established strict investigation principles for employee data that go beyond the legal requirements. Only under a very strict set of conditions may personal data be evaluated for the purpose of performance or quality control, or for the detection and prosecution of misconduct by employees. Before any investigation of employee data is authorized, Deutsche Telekom assesses whether the grounds for initial suspicion of criminal activity are given. These investigation principles enjoy general legal recognition, incorporate recent court rulings and give employees and executives the security of action.

Personal privacy of employees has been enhanced significantly in comparison to the current legal situation. At the same time, the employer retains the necessary powers to continue to combat business misconduct, corruption and data theft. All the same, standardization down to the smallest detail through the legislature offers the potential for overregulation. Therefore, matters should proceed with all due foresight. Fundamentally, current laws already permit sufficient scope for creating a data privacy-friendly corporate culture and collaborative partnership within the company.

Agreements, standardization and organizational workflows.

Deutsche Telekom implemented various measures in the course of 2011 to balance the interests of employees and employer in employee data protection. In addition to the protection of personal data, the prevention of misuse of employee data was a primary focus.

- In future, Telekom Deutschland will standardize the technical office equipment of some 130,000 employees in Germany. The goal is to modernize the workplaces with standardized hardware and software at 1,750 sites and boost productivity. The foundation is a standardized IT infrastructure with uniform basic equipment for all employees. Deutsche Telekom reached a milestone in this project in 2011: the user data of all employees has been consolidated from several different system in a privacy-compliant manner. A user and authorization management system ensures that access privileges are managed centrally on a need-to-know principle. This role-based rights administration makes sure that employees only have access to the specific data they need to carry out their duties. Improvements have also been implemented for employees. Among others, this includes:

    - Transparency in user identity and access privileges: an intranet portal shows employees, in a protected area, which information is stored for their user IDs. This includes access authorizations for IT applications, organizational area, office address and phone number.

    - Protection when printing confidential documents: printing and scanning at a central print terminal is possible from any workplace. With the implementation of the new technology, the printout will not be made until the employee activates it on the printer with a chip card. As a result, no confidential printouts – such as customer or HR data – can remain in the printer tray unsupervised, and employees can decide for themselves when they wish to pick up their documents.

- Data privacy when working in the Telekom Social network: Deutsche Telekom employees have access to an internal social network. This social media platform provides users with various functions for virtual collaboration, such as discussion forums, document repositories, messaging and the creation of virtual working groups. To perform these functions, personal data is collected and processed, divided into required and voluntary information. Deutsche Telekom has specified that the required information be kept to a minimum and that each employee can decide for themselves which additional data they wish to specified and exchange through the social network. The first time they use the Telekom Social Network, each employee is only granted basic user rights. They can delete their accounts, removing the personal reference to their submitted content. Privacy information is provided to ensure transparency in the use of content and data on the social media platform. Group Data Privacy has drawn up a model contract for all German and international subsidiaries to guarantee the legally and privacy compliant use of the Telekom Social Network for all their employees.

- Data privacy in auditing: Deutsche Telekom has organized the remit of the auditing function throughout the Group. To this end, these corporate functions from the individual Group companies have been consolidated centrally. Within the framework of this transfer of functions, Deutsche Telekom developed a model contract to ensure the privacy-compliant use of employee data in the course of auditing activities.

- Data privacy in corporate integration management: Deutsche Telekom has expanded on the privacy-compliant exchange of information between those involved in corporate integration management. In light of the need for information on the part of the employee representatives, it became necessary to regulate the extent to which they have access to data on employees who are entitled to reintegration after health-related absences: if an employee is incapable of working for more than six week at a time, or incapacitated repeatedly, the employer must check whether the employee will benefit from such measures. The employee must be notified of the workplace design, while employee representatives are also entitled to receive information. With these regulations, Deutsche Telekom has balanced its privacy protection obligations to employees with the information needs of the employee representatives.

Informational visits by the privacy supervision authorities regarding electronic personnel files.

While the German Federal Commissioner for Data Protection and Freedom of Information is responsible for privacy issues involving civil servants at Deutsche Telekom, the privacy of employees is supervised by the State Data Protection Commissioner of North Rhine-Westphalia, among others. In the 2011 period under review, Deutsche Telekom presented the Group's new personnel file guidelines to both supervisory authorities: effective December 1, 2011, HR documents are managed exclusively as electronic personnel files.

The commissioners gained an impression on several current topics:

- The qualified electronic signature (QES) of documents in the electronic personnel file is being implemented in a current project in accordance with the requirements of the Federal Ministry of Finance. The QES serves to ensure the legal effectiveness and validity of electronic documents. To this end, the deletion and retention periods of nearly 2.4 million documents in the electronic personnel files of civil servants are being checked. The review was based on specific demands from the supervisory authorities to ensure the privacy-compliant disposal of the civil servants' printed files.

- The physical deletion in the software systems for personnel administration will not be completed until early 2013 in some cases, which the supervisory authorities judged to be critical. The duration of the process is due to technical reasons related to the version of the SAP software used. The Federal Commissioner for Data Protection has been notified. The supervisory authority and Deutsche Telekom are working together to reach a faster solution. The implementation of the data deletion has already been ordered in other software systems. Both supervisory authorities emphasized the excellent, constructive cooperation.

Unauthorized evaluations in the personnel administration software.

The data privacy concept Ⓖ of the personnel administration software used at Deutsche Telekom defines permissible evaluations and the users authorized to carry them out. A Group works agreement regulates which users are authorized to query which personnel data. A routine check revealed that newly installed software functions resulted in unauthorized evaluation options. In response, Deutsche Telekom developed authorization concepts and modified the evaluation prompts to comply with the data protection concept of the software and the Group's regulations.

Incorrect e-mail sent in the fleet management area.

Deutsche Telekom provides a number of employees with company vehicles, in exchange for a portion of their salary, which is managed through Group subsidiary DeTeFleetServices GmbH. A technical system error occurred during the annual automatic sending of electronic invoices: the e-mail messages contained the recipient name from the previous send process. As a result, billing information was inadvertently sent to the wrong recipients. The error was identified and eliminated immediately. The affected parties received a letter of apology with information about the error and its correction.

Legally compliant regulations for data processing by procurement software.

The eBest (Electronic Buying and E-Commerce System Telekom) purchasing application is part of Deutsche Telekom's procurement system. After several functional enhancements were implemented, a routine review of the data protection concept of the software was carried out. During the review, it was discovered that several Group companies use eBest, but that no contractual basis existed for this cross-organizational processing of data. For example, this data involved order information, such as employee name and delivery address, that was exchanged between Group companies for the purpose order processing via the procurement system. Deutsche Telekom closed this gap by elaborating the missing contracts and revising the data privacy and security concept for eBest.

3.4. International developments.

Legal provisions.

- **Amendment of the EU EU Data Protection Directive**
  The EU Commission has revised the European Data Protection Directive and submitted a draft to the European Council and the European Parliament. It is intended to define the legal framework for the protection of personal data in the EU and come into force as a regulation. As a regulation, in contrast to the existing directive, it will take effect immediately, because it does not need to be implemented in national law by the EU member states. The consequence would be a uniform, harmonized set of rules governing privacy protection in Europe, which would make it easier for companies to conduct international business in a privacy-compliant manner and also strengthen consumer protection.

  The EU Regulation is based in parts on existing regulations that have been part of German data privacy legislation since 2009. In particular, the new rules include the uniform responsibility of a single supervisory authority for a corporate group, the applicability of the Regulation to companies headquartered outside of the EU and the introduction of privacy officers at companies throughout the EU. Another new rule would free companies from having to appoint a privacy officer for each legal unit, and instead only require the naming of a single group privacy officer. Uniform rules for notifying parties affected by breaches of security in personal data or its misuse (data breach notification) Ⓖ are also planned. This last item is already covered by a section of German data privacy legislation and has been implemented by Deutsche Telekom.

Deutsche Telekom sees the planned amendments as a necessary harmonization of data protection regulations in Europe and welcomes the improved protection for affected parties. At the same time, Deutsche Telekom sees a need to act up on a number of rules that are still inexact, for which the EU Commission reserves the right to introduce regulatory statutes. For example, the Commission plans to promote privacy certification, but provides no information about standards or processes. At this juncture, Deutsche Telekom calls for the involvement of businesses to enable practical implementation. Following completion of consultations in the Parliament and European Council, the new EU Data Protection Regulation is likely to come into force in 2013.

International privacy committees.
The international privacy circles (IPCs, now: International Privacy Leadership Teams) 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 teams also aim to establish 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. It examines privacy issues in small working groups, from the operational perspective of 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.

- **Other new legal regulations and initiatives.**

New rules were not limited to the EU level. Russia revised its data protection law, particularly with regard to the international transfer of data. Similar to the European Union regulations, transfers to a third country were only possible if that country was determined to have an adequate level of privacy protection. The amendment clarified how this determination is made. Privacy laws were also revised in some EU member states, such as Hungary. The changes have far-reaching consequences for multinational corporations. For example, the subcontracting of data processing is still not allowed. Binding group regulations – such as the Privacy Code of Conduct Ⓖ at Deutsche Telekom – are not recognized and the transmission of personal data from Hungary to abroad continues to be forbidden without express consent.

The confirmation of these strict rules also has consequences for Deutsche Telekom, because it means the Hungarian subsidiary cannot use international Group infrastructure, such as for uniform privacy training courses. The law also deviates from the EU Data Protection Directive in that data processed in Hungary is always subject to Hungarian privacy laws, even if the data was collected abroad. This can result in conflicts with legal requirements in the country of origin.

Measures for international cooperation.

The annual International Privacy Circle (IPC, in future meetings of the International Privacy Leadership Team) and the International Data Protection Day took place from June 28-29, 2011.
In contrast to past events, this IPC was not held on a regional basis, but was instead centralized at the Deutsche Telekom Group's Headquarters in Bonn. As a result, all privacy offers of the international business units had the opportunity to meet one another personally and exchange experiences for the first time. The

Circle is a central forum where information and opinions can be exchanged on privacy-related topics, such as requirements for international commissioned data processing, internal verification systems and results of the international basic data privacy audits. The event was rounded out by International Data Protection Day, which examined strategic topics, in contrast to the workshop-oriented Privacy Circle.

In late 2010, Deutsche Telekom prioritized topics within the framework of the International Privacy Task Force: these topics, the rollout of the international Privacy and Security Assessment (PSA), international privacy training courses and international commissioned data processing, were developed and implemented over the course of the year. In the commissioned data processing area, new templates were produced for various project constellations, to support the user departments more efficiently. The international training courses will be translated into the respective languages incrementally in future, in cooperation with the national companies. The international intranet was completely reworked within the framework of a joint relaunch project by the Data Privacy, Legal Affairs and Compliance Board of Management department. As a result, information, newsletters and documents are now available in a standard, clear design.

Audit of international data privacy.

In August and September 2011, the Group audit department examined the international data privacy strategy at the Deutsche Telekom Group. In the process, the implementation of the Privacy Code of Conduct, the international Governance & Cooperation Model and the corresponding requirements and processes were examined at the international business units. In the end result, the successful implementation of the Privacy Code of Conduct at over 90 percent of the international business units and the rollout of the governance model were judged positively. The further development of the Governance & Cooperation Model and the full implementation of the Privacy Code of Conduct were recommended for the coming years.

A catalog of measures has been developed to fulfill these recommendations and its implementation will be pursued over the course of 2012. For example, the duties of the respective privacy officers at a national business unit and the associated implementation process will be portrayed in a simplified process overview in future. This will optimize the transition when a new privacy officer is appointed and streamline the familiarization phase. At the same time, a schedule and information flow between the business units and Group Headquarters has been defined, to optimize the possibilities for Group Data Privacy to render support during the transition. In addition, functional management of the local data privacy structure is to be expanded by Group Data Privacy and the existing interactions between Group Headquarters and the business units reinforced. The existing coordination processes from the Governance & Cooperation Model will serve as a basis.

The international data protection intranet, which provides documents, information and training courses on international data privacy and which was completely reworked in 2011, will continue to be expanded. A recommendation was also made to add more training courses and white papers to the platform for the business units. As the central online communications medium, the intranet will increasingly provide basic information such as the international data privacy strategy and related contents. The successfully launched data privacy and privacy incident reporting system will continue to be developed as a consolidated reporting system. The path taken toward international data privacy in past years has been judged positively. This path is to be enhanced continuously and adapted to new requirements.

International standard for tracking.

Initiated by the Federal Trade Commission in the U.S., a broad debate was launched at the international level on tracking mechanisms on the Internet and the lack of user options to evade such tracking. A working group was installed at the level of the World Wide Web Consortium (W3C), a committee for standardizing technologies in the web. This group aims to define an international standard that leaves it up to users to allow or disallow tracking. Deutsche Telekom sees an urgent need for action here. This applies particularly to mechanisms such as the EU directive on cookies and proposals for amending the Telemedia Act. Deutsche Telekom will continue to participate actively in this debate, with

Deutsche Telekom is continuously improving its international cooperation.

the aim of ensuring that national and European data privacy requirements are met.

Audits in locations outside Germany.

T-Systems is Deutsche Telekom' s business customers arm. It offers IT services in Germany and internationally. In the year 2011, several international T-Systems sites were audited to ensure an appropriate level of data privacy, including Brazil, Malaysia and South Africa. These audits are referred to as point of production (PoP) audits. The audits discovered a varying level of compliance; a number of corrective measures were defined and their implementation tracked. In addition, re-audits were carried out to verify implementation of measures agreed from previous audits.

Privacy Code of Conduct (PCoC) audits examine compliance with the Privacy Code of Conduct within the Group. The results of the international basic data privacy audit were also considered. Audits were held at T-Mobile Poland, Telekom Croatia, Magyar Telekom (Hungary), T-Mobile Czech Republic and affiliated companies of OTE in Greece and Romtelecom in Romania, among others. The results were also heterogeneous here. In addition to the definition of corrective measures, units whose structure is still being established were lent support by Deutsche Telekom for personnel-related and organizational matters. Appropriate re-audits were also defined.

Enhancement of data privacy at Hrvatski Telekom.

During a visit by Deutsche Telekom's Group Privacy Officer to the CEO of Hrvatski Telekom in October 2011, the data privacy strategy of the Group's Croatian subsidiary was elaborated in more detail. In addition, adoption of the data protection requirements from the Governance Model was agreed upon, the implementation of measures from past audits was discussed and the implementation of the PSA process explained. The parties also agreed to supplement the data privacy organization at Hrvatski Telekom with additional staff, to make collaboration with the internal IT department more efficient for project work.

Everything Everywhere.

On July 1, 2010, Deutsche Telekom and France Telekom merged their subsidiaries in the United Kingdom to form a joint venture named “Everything Everywhere”. 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 corresponding measures and decisions involved in complying with system-side privacy protection during the system migration were supported in 2011. Deadlines were defined to enable a privacy-compliant transition.

Attack on home gateways at Slovak Telekom and Romtelecom.

Massive attacks on the home gateways (DSL routers) of many consumers in February 2011 caused a significant disruption of Internet access business at Slovak Telekom and Romtelecom. The hackers used an unsecured administration access option in the devices installed by the affected national companies to manipulate DNS settings (Domain Name Service, used to resolve Internet

Thomas Tschersich
Head of IT Security,
Deutsche Telekom AG

A new credo in cybersecurity is "analysis over prevention". Isn't that a paradox?
This thought may seem paradox indeed, at first. But the paradox is resolved when one takes a differentiated view: putting one before the other does not mean omitting the latter. Of course, both factors – prevention and analysis – are crucial to effective cybersecurity. But at a time in which digital threats are constantly increasing and new attacks and patterns are emerging daily, our focus must shift. We have to be aware that we can't simply erect a fixed, virtual fence around our infrastructure.

To understand how to counter the threats, we have to find out their nature. And that's where the analysis comes into play, with the results serving as the basis for further preventive measures.

In recent months, Deutsche Telekom has continued to expand its early warning and analysis systems, such as honeypots and the CERT. At the same time, it is following a strategy of integrating security and data privacy from the very first development steps of projects and digital security tests prior to the market launch of products. But all this is always just a snapshot. We know: the right balance between analysis and prevention is the direction we want and have to take.

names). As a result, some of the affected consumers' Internet traffic was rerouted to other destinations, in an attempt to distribute malware (to establish a botnet, for example, to carry out distributed denial-of-service attacks Ⓖ) and obtain access data to services (phishing attacks).

Individual infrastructure components of both national companies were subject to heavy loads as a result of the attacks, which meant that customers whose home gateways were not attacked directly were also affected. Affected devices were identified through remote maintenance and the manipulated configuration settings were corrected. The vulnerability was also eliminated. Deutsche Telekom supported Slovak Telekom and Romtelecom in their actions.

3.5. Systems and processes.

The year 2011 was a year of wide-ranging public and political debates on the topics of data privacy and data security (see page 10). Deutsche Telekom considers the broad societal and political awareness of these topics to be entirely productive for the constructive further development of existing and planned national and international privacy and security concepts. The Company places great store on openness in this debate, however: it must always be clear that the absolute security of data is not possible. As such, the goal can only be to design systems and processes to be as safe as possible, necessary and desired.

Deutsche Telekom reached important milestones in this area in 2011. It continued to expand its early warning systems, which it uses to identify new attack patterns from the Internet, evaluate them, and utilize them to improve internal systems (see page 40). At the same time, it continued to advance a process that has been deployed Group-wide to integrate and consider data privacy and data security in the development of products and services from the very start (see page 41). In addition, the Company continued to demonstrate compliance with relevant standards in 2011, through certification by independent institutes. Experts confirm that the company maintains an exemplary level of security. Numerous data privacy and data security audits comprise a central component 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.

Deutsche Telekom’s security management practices.

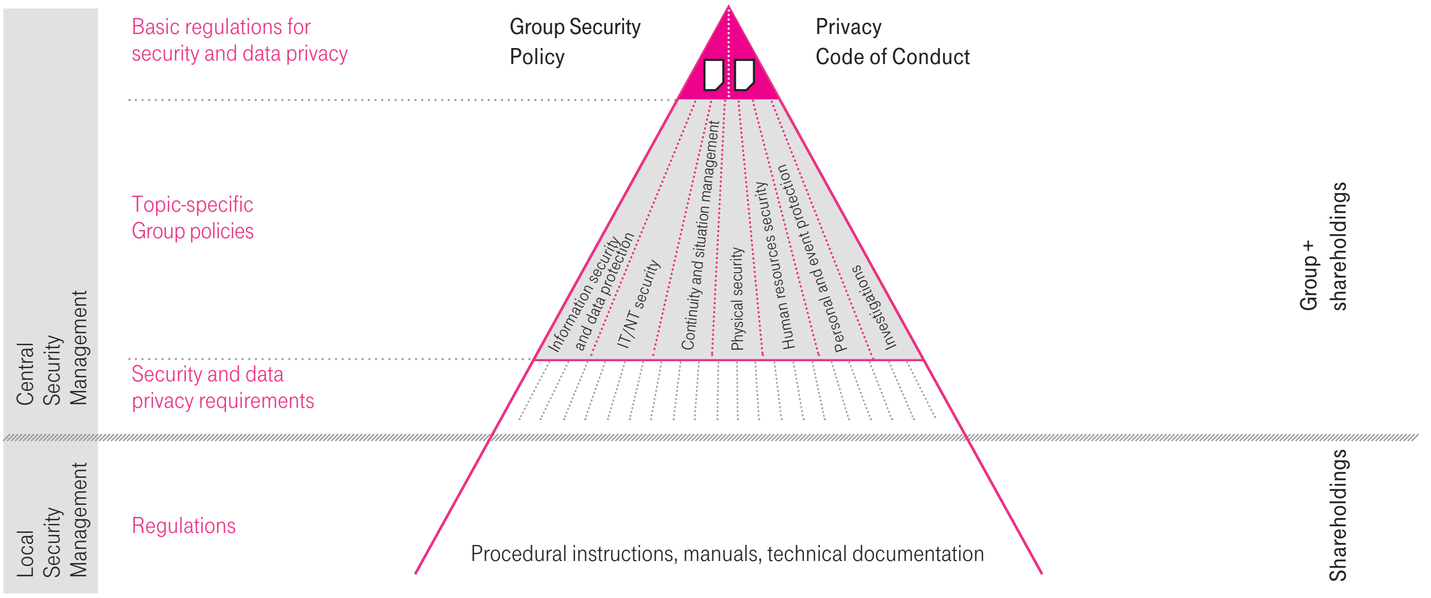
Deutsche Telekom is obligated to take suitable measures to identify developments that could jeopardize the company’s existence at an early stage. This obligation includes, in particular, an internal monitoring system. Violations of data privacy and security provisions must be ruled out as far as possible. For this purpose, Deutsche Telekom continuously further develops its Group-wide security management system, among other things. In 2011, it again adapted the system to the latest developments and expanded it to include other parts of the Group.

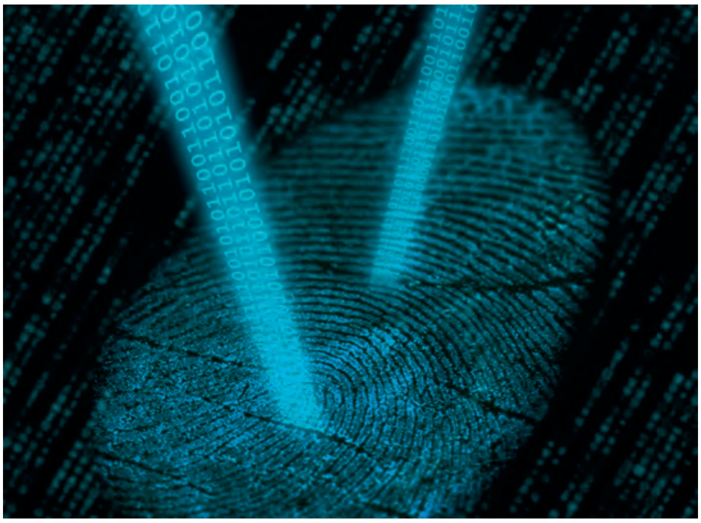
Apart from data privacy, a key component of the security management system is Deutsche Telekom’s Central Security Management department. The Central Security Management department consists of the three organizational units Group Security Policy (GSP), Group Business Security (GBS) and Group Service IT Security (GIS). It governs the interaction between all functions within the Group that are responsible for ensuring security. Central Security Management has been certified under ISO 27001 (see page 45) since 2010, thus meeting the most important international standard.

Security and privacy management are based on the following regulatory framework:

At the top of the regulatory framework are the two basic documents on security and data privacy within Deutsche Telekom: The Privacy Code of Conduct contains the internal requirements for dealing with personal data (general data privacy provisions), while the Group Security Policy includes the Group’s security-

Regulatory framework for security and data protection.


Central Security Management
Basic regulations for security and data privacy
Group Security Policy
Privacy Code of Conduct
Topic-specific Group policies
Information security and data protection
IT/NT security
Continuity and situation management
Physical security
Human resources security
Personal and event protection
Investigations
Group + shareholdings
Security and data privacy requirements
Local Security Management
Regulations
Procedural instructions, manuals, technical documentation
Shareholdings



When hackers attack honeypots at Deutsche Telekom, they leave digital fingerprints of their attack patterns behind.

relevant principles. At the same time, the Privacy Code of Conduct and the Group Security Policy represent a “basic law” for Group-wide data privacy and security practices. These provisions are further specified by seven additional topic-specific Group policies:

- Information security and data protection
- IT/NT security
- Continuity and situation management
- Physical security
- Human resources security
- Personal and event protection
- Investigations

The Central Security Management regulations, which were revised in 2010, were successively implemented in Germany and in the international holdings in 2011. This process is has been largely completed. Local regulations supplement and complete them in the individual units. The policies came into force in 2010 at Deutsche Telekom AG and Telekom Deutschland GmbH.

Early warning systems.

As the largest provider of communications services in Germany, Deutsche Telekom and its customers are a prominent target for cyberattacks. The opportunities posed by such attacks represent a constant challenge. In response, Deutsche Telekom has set up an early warning system, which it continues to expand. Strict German privacy criteria were taken into account in the design of the early warning system, which aims to gather information about the attackers, identify new attacks and develop better defense strategies. Furthermore, this approach makes it possible to identify and implement necessary adjustments to the security mechanisms at an early stage. If Deutsche Telekom’s customers are targets of cyberattacks, the Company notifies the affected parties. In principle, the larger the number of data sources and material available, the better the quality of the early warning system. Accordingly, Deutsche Telekom links its view of the security situation in the Internet – which is based strictly on internally generated information – with generally available manufacturer information and findings from authorities.

Honeypots.

Honeypots Ⓖ are a central component of Telekom’s early warning system. They represent server systems that are accessible from the Internet, but which are isolated from the actual infrastructure at Deutsche Telekom. Therefore, even if they are compromised, the honeypots do not pose a risk to the Group’s infrastructure. Some of these honeypot systems are self-learning, which means they record and analyze unknown attacks, enabling subsequent automatic identification by the early warning system. Deutsche Telekom began building honeypot systems of this type in April 2010. They were originally only intended to provide information about attacks on the company’s Internet applications. Deutsche Telekom now uses the data for various other purposes as well, for example, to notify its customers and other Internet service providers.

As a supplement to the existing honeypot systems for Internet applications, Deutsche Telekom began operating several Secure Shell Honeypots (SSH) in December 2010. These honeypots simulate SSH servers and make it possible to record the sequence of an attack, in the process collecting the deployed malware and authentication information for later analysis.

Deutsche Telekom is the first provider in Europe to develop honeypots that simulate the operating systems for smartphones (Android and iOS (for iPhone)), with the aim of identifying attacks directed at these smartphones and developing defense mechanisms. This new, adapted form of existing honeypots – based on Kippo open source software, among others – shows that systematic attacks against open systems in cellular networks are already an everyday occurrence.

Deutsche Telekom collaborates closely with other providers that work with similar systems, some of which were supplied by Deutsche Telekom initially. This network includes the “Anti-botnet initiative”, a program funded by the German government, which has the declared goal of reducing the number of infected consumer computers.

Since their establishment in April 2010, the honeypots have detected more than 12 million hacker attacks (as of March 2012). Deutsche Telekom has used the insight thus gained about the types and methods of attack to prevent successful attacks on its actual IT systems and to notify customers whose computers are part of a botnet Ⓖ and are thus under external control.

Deutsche Telekom continuously improves its early warning systems to guarantee the best possible protection for its own data and that of its customers.

Telekom CERT.

The Cyber Emergency Response Team (CERT) at Deutsche Telekom is responsible for cyber incident management – the management of all Internet security incidents for all of the Group’s information and network technologies. As such, it carries out the crucial task of protecting the Company and its customers from dangers from the Internet. 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 duties include:

- Cyber incident management: coordination and management of critical security incidents
- Strategic threat radar: responsibility for maintaining a threat radar, to identify threats in the context of current and future core technologies within the Group
- Advisory management: assessment and distribution of security information within the Group, along with the monitoring and implementation of critical security updates
- Vulnerability scanning: regular execution of security scans of portals and systems that are accessible through the Internet
- Central interface: collaboration with law enforcement agencies and interface functions to national and international committees and authorities responsible for IT security.

In 2011, the Telekom CERT issued alerts to internal operating units involving 1,174 vulnerabilities in software components used within Deutsche Telekom. This was a slight increase compared to the previous year. An analysis of the severity of the security alerts reveals a consistently high proportion of critical and highly critical vulnerabilities.

Many of the alerts address vulnerabilities for denial-of-service attacks and drive-by infections. The affected operating systems have hardly changed in comparison to previous years. As a consequence of the market penetration of Unix and Windows systems, both platforms show nearly the same share of vulnerabilities: in a direct comparison, Unix accounts for 48 percent while Windows systems account for 43 percent.

Within the framework of the strategic threat radar, the threat potential of trends, innovations and current and future technologies is examined and assessed. The radar enables Deutsche Telekom to assess the impact of cyber threats at an early stage and develop counter measures as necessary.

The advanced persistent threat (APT) category is currently a particular focus of the Telekom CERT. The CERT has launched a project on this subject together with the Federal Office for Information Security (BSI). The aim of the project is to determine which security technologies and products are suited to providing comprehensive protection against such threats. The results will be made available to the general public.

Privacy & Security Assessment (PSA) process.

The Data Privacy and Data Security departments are laying important groundwork within Deutsche Telekom for reliable products that also satisfy strict requirements for security and data privacy. As early as 2010, they implemented the Privacy and Security Assessment (PSA) process together, to guarantee that all projects within the Group meet the requirements for technical security and data privacy from the very first development step onward.

The process has the following goals:

- Ensure the legal privacy compliance of all products, systems and platforms
- Provide a consistent and adequate level of security and data privacy in all products, systems and platforms that are updated or created from scratch
- Define an integrated process for technical security and data privacy as a component of the product and system development processes
- Establish a support level adapted to project complexity and criticality through the introduction of categorization at the start of each development project

Use of the PSA process is mandatory for all German companies as well as for proposed international Deutsche Telekom projects, provided they are to be managed from Germany. The international rollout of the process made rapid advancements in 2011. Conclusion of the activities is planned in 2012/2013.

Using a categorization tool, projects are categorized at the start of the process as A, B or C according to their relevance in terms of technical security and data privacy. The complexity of support is then based on this. The more critical a project, the more comprehensive the advice and support provided by data privacy and security experts. This approach ensures the optimum use of resources by everyone involved. In addition to data privacy and security experts, the process involves the project manager and system administrators. A development process that was supported by the PSA process always concludes with a security test and privacy clearance.

Deutsche Telekom has made repeated public demands that security and data protection be made obligatory design criteria for products and processes.

“Security in Sales” round table.

As part of the “Risk Management in Sales & Service” project initiated in 2010, Deutsche Telekom established a “Security in Sales” round table. This advisory and information committee supports management at Telekom Deutschland GmbH in dealing with sales-relevant fraud incidents, such as bonus and commission fraud, access and data misuse, involvement of unauthorized sales partners, misuse in the activation of prepaid cards and disconnection of device and SIM card.

The round table consolidates and coordinates all fraud-related activities, providing for transparency across all sales and distribution channels. It also drives and coordinates the permanent implementation of all measures made necessary by the above fraud incidents. In addition, it recommends appropriate preventive measures to reduce security risks.

Where misconduct is identified, the round table makes recommendations on required sanctions and measures. In particular, it also initiates sanctions for sales partners in proven cases of fraud. Sanctions can include written warnings and commission clawbacks, as well as criminal and civil penalties.

The Group Business Security (GBS) department appoints the chair of the round table. Balanced voting rights between sales and non-sales area ensures the parity of the committee.

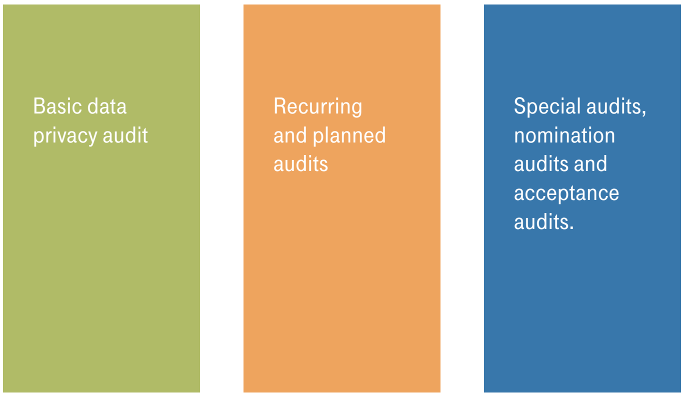
Data privacy orientation for new business areas.

With the new “Fix – Transform – Innovate” strategy introduced by René Obermann in the spring of 2010, Deutsche Telekom set a focus on growth through new, intelligent network solutions and offerings in business areas such as energy, healthcare and automotive. New business areas in particular require information about the importance of privacy considerations in their business models. After all, they always involve the processing of personal data, which Deutsche Telekom places great value in protecting. To this end, Deutsche Telekom established principles in 2011 to summarize and represent the privacy framework for the respective projects and business areas. While these guides provide initial information for new employees as to what they have to pay particular attention to in the individual areas, they also serve experienced employees as an abstract summary of the essential framework conditions.

Audits and certification.

Regular Group-wide audits and certifications relating to data privacy and data security take place at Deutsche Telekom. In the process the Company relies on a system of audits by external and internal bodies. Deutsche Telekom thus serves as a model within the telecommunications industry: certifications for company units are still the exception within the telecommunications sector. Deutsche Telekom's audits for internal control and monitoring of how data privacy and data security requirements are implemented fall into three categories:

Audit categories at Deutsche Telekom AG.



Basic data privacy audit

Recurring and planned audits

Special audits, nomination audits and acceptance audits.

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, external auditors investigate whether the unit's 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 basic data privacy audit is carried out at both the national and international levels. The subject of this audit is compliance with the requirements of Group Data Privacy. 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 includes special audits occasioned by incidents or suspicions, as well as acceptance audits for approving prioritized projects. Specifically, this means before a product is launched, an audit examines whether that new product meets all the required criteria for data privacy and security. During nomination audits, new sales partners are audited before business relationships begin. Deutsche Telekom also checks existing sales partners regularly in recurring audits.

Audits performed.

In 2011, the Internal Auditing, Group Privacy and Central Security Management departments alone performed around 220 audits on data privacy and data security. A large portion of these audits was dedicated to 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 potential gaps. Such gaps can arise due to security deficiencies in software solutions, which are remedied together with industry partners as soon as they are identified. The audits also focused 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.

Sales audits.

In 2011, Deutsche Telekom 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". In 2011, 28 call centers, which handle customer calls according to Deutsche Telekom's requirements within the sales organization, were successfully certified by TÜV-Rheinland.

In addition, the final preparations were made in 2011 to obtain certification for the call centers that carry out customer service on behalf of Deutsche Telekom in 2012. To achieve this, a separate IT ecosystem first had to be set up at the call centers, to enable restricted use of Internet and mail traffic (see page 27). As a result, the security of the customer data has been improved continually, starting from an already high level. At the same time, the certification and maintenance audits of some 350 exclusive retail partners, which were started in 2010, were continued.

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. The round table for "Security in Sales", a body established in 2010, serves as the central coordination and steering instance.

Standard privacy audits.

Deutsche Telekom regularly audits its processes and systems. The TOP audits were the most important audits in the privacy area in 2011.

- Credit check audit: the risk assessment system at Telekom Deutschland GmbH evaluates the risk of non-payment in deals with existing customers and sales partners. The audit revealed deficiencies in the role and authorization concept, as well as in the deletion concept, which are being corrected successively.

- ProKom audit: the ProKom system is used to manage and edit directory entries of telecommunications subscribers. The audit documented an appropriate level of data protection.

- Investigation process audit: for the third year in a row, an audit was carried out in 2011 to examine whether internal investigations within Deutsche Telekom are carried out in a privacy-compliant manner. The audit confirmed that measures introduced after the previous year's audit had been implemented and that both the processes and procedures used meet the demands for data privacy.

- Audit process audit: like in the previous year, the Group Audit department was audited itself to ensure compliance with the defined privacy framework (laws and internal Group requirement). The audit had a positive result: all measures stemming from the previous year's report had been implemented.

- Customer management in mobile communications audit: like in the year 2010, the system for managing mobile communications customers was subjected to an extensive audit. Despite significant improvements in many areas, several deficiencies were identified and have already been remedied. This system, one of the most important at the Company, will continue to be audited annually.

- Fixed network customer management audit: in particular, the audit of the customer management system in the fixed network examined the user interface, the archiving and deletion of customer data and the user concept. No critical deficiencies were discovered. Some minor problems identified in the deletion process have been corrected.

- SAP HR basic audit: checks the collection and processing of employee data, i.e., compliance with the agreed access authorizations. Due to the complexity of the software and the constantly changing environment – reorganizations and system updates, for example – regulation requirements were identified, to which Deutsche Telekom responded through organizational measures. Several items criticized during the audit could be corrected at short notice.

- Data warehouse audit: Ⓖ in 2011, compliance with the data privacy requirements of the data warehouse was checked for mobile communications and the fixed network. The identified weaknesses, such as a lack of encryption have either been rectified or their remediation is in process.
- Audit of misuse detection systems: Deutsche Telekom operates several systems to identify misuse and service acquisition under false pretenses by customers and sales partners. These systems were audited in 2011 and confirmed, in particular, that the filter settings for identifying misuse are designed and recorded in a privacy-compliant manner.

- PCoC at German subsidiaries: compliance with Deutsche Telekom's Privacy Code of Conduct (PCoC) was audited at the subsidiaries Autoscout, Friendscout and Operational Services. A similar audit was conducted of international affiliates (see page 37).

Vulnerabilities identified in all audits were and will be eliminated and the implementation of the measures checked by Group Privacy.

Results of the 2011 national and international basic data privacy audit.

The annual basic data privacy audit was carried out once again in 2011. The objectives of the audit are to measure the general level of data privacy, to identify potential for improvement and to derive countermeasures. To this end, 40 percent of Group employees from Germany and 30 international affiliated companies were surveyed. Self-assessments by the data privacy officers at the international affiliated companies of compliance with the requirements of the Privacy Code of Conduct supplemented the basic data privacy audit. Both the employee surveys and the self-assessments by the data privacy officers are verified through random spot checks.

At the Group level, the 2011 basic data privacy audit showed that the implemented data privacy measures are effective. The already relatively high level of data privacy has continued to improve. The participation rate at the Group as a whole increased from 43 percent to 52 percent; the corresponding figure for Germany was above 60 percent. The employees' high awareness for data privacy was reflected in the question as to how important they feel the topic is. In response, 87 percent of employees Group-wide stated that data privacy is important or very important. This value increased further compared to 2010 and shows that data privacy awareness is similarly high in Germany and internationally.
Other examined subject areas, such as the use of tools for encrypting data, the proper disposal of paper, participation in training courses focusing on data privacy and knowledge of processes

ISO/IEC 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/EIC 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 nonprofit and government organizations.

and reporting paths for privacy showed that employees have a considerable degree of awareness. Individual results were provided for the investigated areas, enabling the units to analyze their specific strengths and weaknesses and work on improvements.

Only a few widespread weaknesses were identified, such as the use of available e-mail encryption mechanisms or the obligation of employees to follow data confidentiality and telecommunications secrecy at international subsidiaries. Like the audits for the Privacy Code of Conduct, the audit revealed that the international domain is often characterized by data protection officers who lack staff, time and equipment. Deutsche Telekom is working on remedying these weaknesses. For more information on international audits, see “International developments” on page 34.

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.

Certification by TÜVIT of the accounting process for consumers.

Following certification of the entire accounting process for consumers in the fixed network by TÜVIT (“Trusted Site Privacy” certificate), the accounting process for consumers in mobile communications is currently undergoing the certification process (as of April 2012).

An audit under the Trusted Site Privacy criteria involves both an assessment of data privacy and an analysis of IT security. Various IT systems and interfaces have already been audited, and technical system examinations carried out, to this extent. The process involves collecting and processing all data generated for over 35 million customers who conduct daily telephone calls over the mobile network. Certification is expected in 2012.

Certification of Telekom Shops.

To maintain a continuously high level of data privacy at the point of sale, the Telekom Shops undergo repeated inspections to verify compliance with data privacy requirements. In addition, the Telekom Shop Vertriebsgesellschaft has been subject to regular external audits since 2009. The privacy and security-relevant processes at the Telekom Shops were once again audited by DEKRA Certification GmbH in 2011. This concluded the three-year audit cycle. The Telekom Shops can continue to display the DEKRA seal “Datenschutz und Datensicherheit gemäß dem Bundesdatenschutzgesetz” (data privacy and security compliant with the Federal Data Protection Act).

Certifications according to international standards.

In 2011, the certifications of Central Security Management and parts of T-Deutschland GmbH were confirmed under the international ISO/IEC 27001 standard. T-Systems also continued the process of certifying its German organization and 19 national companies in 2011. The goal of this process is to obtain the umbrella certificate for the introduction of a Group-wide information security management system. In total, 188 ISO/IEC 27001 audits were carried out worldwide in 2011.

3.6. 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 this sensitive data. Trust in both directions requires communication in both directions. Deutsche Telekom therefore believes in providing its customers with transparent information, while at the same time offering its employees security in the andling of personal data. For this purpose, Deutsche Telekom uses a variety of communications tools and channels, both external and internal.

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

External 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. It also provides information on how it handles stored data. Deutsche Telekom uses different media for this information and is continuously expanding in communications system.

The company already took advantage of European Data Privacy Day as an occasion for information and campaigns in the years 2010 and 2011. The 2012 European Data Privacy Day on January 28th focused on data privacy for children and young people. Claus-Dieter Ulmer, Group Data Privacy Officer, gave a restructured presentation at a school, launching a nationwide series of lectures for which schools could apply at Deutsche Telekom. The interactive presentations and discussions focus on children and young people, who are growing up with the Internet and social media. The aim is to familiarize them with the risks and capabilities available to protect their private sphere. A particular goal is to sensitize them as to which personal data they can reveal and which they rather shouldn't.

Deutsche Telekom is actively involved in public and expert debates on data privacy and data security. In this process, Deutsche Telekom believes the focus should lie on the transparent, well-grounded exchange of ideas and perspectives.
Establishing a dialog was the goal of many of the new approaches Deutsche Telekom initiated in 2011. The Company continued to develop its social media pages and started an enterprise blog that regularly reports on data privacy and data security issues, among other things, stating opinions.
(http://blogs.telekom.com/tags/datenschutz/). The company bloggers have commented on data retention requirements Ⓖ for example, and the security of smart meters. In addition, Deutsche Telekom executives announce their positions on current issues in a new section, "Management zur Sache" ("Management on topic"). Here, as well, data privacy and data security will be examined, for example, with a look at the planned EU Data Protection Regulation or the security of social media.

In addition, Deutsche Telekom is giving new impetus with its telegraph_events. For these events, the Company invites politicians, bloggers, experts and representatives of associations and companies to its Berlin Representative Office, to debate current themes involving developments in the digital world – such as Internet politics, regulation, media transformation and product innovations. Data privacy and data security are a frequent focus. In addition to the exchange of ideas, a particular focus of the events is adversarial meetings, to launch future Telekom topics and occupy positions at an early stage that could arise on the political agenda. Deutsche Telekom hosted a "telegraph_special" at CeBIT 2012 in Hannover that focused on the secure digital identity, again a data privacy and data security topic.

The Company also hosted a "Co:llaboratory" workshop at its Berlin Representative Office in June 2011. This initiative, which was launched by Google, examines developments in the relation between privacy and the public sphere in society. Deutsche Telekom also participated in public debates on employee data privacy and the EU Data Protection Regulation In addition, Deutsche Telekom representatives regularly take part in various expert meetings, trade conferences and public events. The Company participated in several expert hearings before EU committees and international organizations on topics related to data privacy and data security.

Deutsche Telekom has also published a report on the security situation on the Internet since 2011. This quarterly report is available at http://www.telekom.com/dataprotection.

Deutsche Telekom addressed the public with the following additional activities in 2011 and early 2012:

- A new edition of the privacy guide on safer surfing in the Internet
- Redesign of the website for data privacy and data security, with the inclusion of an advice page
- Distribution of privacy guides at Telekom Shops throughout Germany
- Radio spots on topics such as secure WLAN encryption and secure online shopping
- Deutsche Telekom's trade fair presence at CeBIT in March 2012 with a focus on the security aspects of cloud computing
- Presentation of the Company's early warning systems at CeBIT

Internal communications.

For data privacy and data security to be guaranteed, employees at Deutsche Telekom must not only be fully aware of the issues, but also be prepared and trained to deal with their responsibilities. Thus prepared, they can act confidently at all times, in both standard and difficult situations. The Company places special value in providing its employees with the required knowledge on a regular basis. In the process, Deutsche Telekom follows a strategy of including executives, in particular, from the start in data privacy communications with employees. Executives are expected to act as role models to their staffs. In addition, a modular system ensures that employees receive individual training for specific topics and their duties. This guarantees that the subjects of data privacy and data security are met with an ongoing positive response by all Deutsche Telekom employees.

Data privacy coordinators.
Data privacy coordinators are a pillar of the decentralized data privacy organization in Germany: employees who, in addition to their regular duties, support the data privacy area in the introduction and implementation of Group-wide data privacy requirements. Deutsche Telekom can currently rely on some 100 data privacy coordinators to support Group Data Privacy.

One international focus in 2011 was to continue the rollout of the Deutsche Telekom Privacy Code of Conduct at international Group subsidiaries, through communication and training courses to familiarize employees with the principles of the PCoC.
A second focus that was communicated through training courses in Germany and internationally was the Privacy and Security Assessment or PSA process. This process ensures that data privacy and data security are integrated at an early stage of product and system development (see page 42).

Another aspect of internal communications was to train employees in facts of customer data privacy in sales. In light of the high sensitivity of this area, the project is scheduled to run for several years. In addition, all employees throughout the Group are committed to data confidentiality and telecommunications secrecy, and sensitized to aspects of information protection, every two years.

Several different course formats and training media are available for internal communications, including conventional, in-person seminars in classrooms, webinars, self-learning through online formats and course materials, talks with superiors and experts and visits by the data privacy officer. Which format or media is chosen depends on the priority of the learning content, existing individual knowledge and the interests of the employee in question. The material is also available on the intranet.

In May 2011, representatives of Group Data Privacy visited several Deutsche Telekom sites in Germany. In addition to workshops for local site employees and executives, talks with representatives of Group Data Privacy and the data privacy coordinators were offered in which the individual needs of the sites and tasks carried out by the staff were covered. Last but not least, the existing policy database was revised and made available to all Deutsche Telekom employees as a new digital bookshelf on the intranet.

As part of the basic data privacy audit (see page 45), Deutsche Telekom once again presented a national and international data privacy award in 2011. With this prize, the Company recognized the three domestic departments in Germany and three national companies on the international stage that achieved the best results in the audit.

Internal communication at Deutsche Telekom utilizes many different channels. Addressing the recipients personally is tantamount.

Data Privacy Advisory Board at Deutsche Telekom.

A thick shell repels a lot.
Yet external impulses often contribute crucial ideas.

4.1. Tasks and functions.

The Data Privacy Advisory Board at Deutsche Telekom is a body that advises the Board of Management. It promotes interchange with leading experts and leaders from politics, academia, business and non-government organizations on current, data privacy-related challenges. It is also increasingly concerned with data security topics. 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 is not bound by instructions and is independent in its opinion-making.

It deals with a wide variety of topics: business models and processes, dealing with customer and employee data, as well as with IT security and the adequacy of implemented measures. It also examines international aspects of data privacy and the implementations of new legal regulations. The assessment of general data privacy and data security measures at Deutsche Telekom, along with the elaboration of proposals and recommendations on related issues for the Board of Management and Supervisory Board, round out the Advisory Board's duties.

4.2. Composition.

Deutsche Telekom appoints the members of the Data Privacy Advisory Board to two-year terms. To guarantee a qualified, critical reflection of data privacy and data security from outside the company, leading data privacy experts are appointed from various occupational groups and political party backgrounds. The Data Privacy Advisory Board was appointed for a further two years in 2011.

Its members include:

- Wolfgang Bosbach, CDU, member of the German Parliament and Chairman of the Committee on Internal Affairs of the German Bundestag
- Peter Franck, member of the Management Board of Chaos Computer Club (CCC)
- Prof. Dr. Hansjörg Geiger, adjunct 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 (retired)
- 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)

- Dr. Konstantin von Notz, Bündnis 90/The Greens, member of the German Parliament, speaker for Internal Affairs and Internet Policy, chairman of the Enquete Commission on the Internet and Digital Society

- Gisela Piltz, member of the German Parliament, deputy parliamentary groupILeader of the FDP parliamentary group

- Gerold Reichenbach, SPD, member of the German Parliament, Deputy Chairman of the Enquete Commission on the "Internet and Digital Society"

- 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"

- Halina Wawzyniak, DIE LINKE party, member of the German Parliament, deputy party chairwoman, chairwoman of the Enquete Commission on the "Internet and Digital Society"

- Prof. Dr. Peter Wedde, professor of Labor Law and Law in the Information Society, director of the European Academy for Labor at the University of Frankfurt am Main

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

The Data Privacy Advisory Board at Deutsche Telekom is still active, although the company has made vast advances in data privacy. Why?
Deutsche Telekom established the Data Privacy Advisory Board in a crisis situation. The company has changed since then, thanks in no small part to the work of the Advisory Board. The Group has become more sensitive, self-critical and careful in data privacy matters: this progress must not be sacrificed to cost-cutting measures. If a company like Deutsche Telekom wants to highlight a high privacy level as a competitive advantage, the topic must be given strong emphasis, even – and especially – in times of restructuring. Data privacy and data security are also becoming increasingly important for new products. To be successful, the "Telekom Cloud" must become synonymous with personal privacy. Both these factors make the continued commitment of the Advisory Board essential.

In addition to changes within the Company, we see the ever-greater impact of outside developments on our work, such as changes in the legal situation, technical options and societal awareness. The services of the future have long taken their place alongside correction of past mistakes; our agenda now includes the demands of data security in addition to conventional privacy issues. We see that companies must ensure close cooperation between both disciplines to meet the requirements for adequate protection and security and to withstand the increasing threat level. The Advisory Board assists with these activities as well.

4.3. Examples of the Data Privacy Advisory Board's work in 2011.

The work of the Data Privacy Advisory Board is characterized by its function as the Deutsche Telekom Board of Management's most important advisory body. Supporting the Company in achieving its goal of assuming a pioneering role in data privacy and security in the telecommunications sector is another equally crucial focus of its activities.

The Advisory Board can take up data privacy and data security topics independently and elaborate suggestions and recommendations for Deutsche Telekom's Board of Management. Given this latitude, the advisory body concerned itself with future topics involving data privacy and data security in 2011, in addition to the topics it was assigned by the Board of Management.

The Data Privacy Advisory Board met four times in 2011. At these meetings, the members examined the privacy aspects of the strategic growth fields of healthcare and energy. They investigated the privacy implications of international business models and consulted on the impact of training courses within the Group. Another advisory field was a topic that received broad public attention: packet inspection and deep packet inspection. This involves a technology for analyzing data packets, which network operators use to examine packets exchanged between servers and client computers (see box).

The Data Privacy Advisory Board verified compliance with the Telecommunications Act and the transparency of rules governing the use of packet inspection within the Group. Following a recommendation by the Data Privacy Advisory Board, information about the packet inspection methods used at Deutsche Telekom was published on the Internet.

Packet inspection/deep packet inspection.
Packet inspection is a technology for analyzing data packets, which network operators use to examine packets exchanged between servers and client computers. It is used to measure traffic streams, to defend against attacks on the network infrastructure.

Deep packet inspection is another technology for analyzing data packets, one that also scrutinizes packet content. This technology is needed, for example, to discover viruses in e-mail messages. Deutsche Telekom runs both these analysis methods fully automatically, without any employee viewing.

Like all telecommunications companies, Deutsche Telekom is required to provide information on traffic and master data to public agencies under certain circumstances and to monitor telecommunications for public agencies. To this end, the Company developed a new guideline in 2011 and presented it to the Advisory Board. The aim of this guideline is to give employees clear, legally founded rules in cases of doubt for meeting the requirements of the freedom of information, the protection of data and business interests and the national interest in preventing danger and averting criminal activity. The Advisory Board noted and approved this new guideline at its first meeting in 2012 and explicitly praised Deutsche Telekom's handling of the practices for providing information and monitoring.

The Board of Management at Deutsche Telekom will continue the constructive dialog with the Data Privacy Advisory Board with the aim of further advancing the Company's pioneering role in data privacy and data security in the telecommunications sector. The critical examination of the demands of data privacy and IT security and their implementation within the Group by external experts has proven itself – to ensure that Deutsche Telekom customers can continue to trust the security of all the Company's products and services in future.

An external perspective provides new insights and new ideas.

Nature has found perfect mechanisms for protecting its valuables.
Deutsche Telekom helps its customers protect their valuables
in the digital world – their data.

It is hard to imagine life without the Internet: we do our shopping online, chat with friends on other continents, watch movies over the Net – the possibilities are almost endless. And not only in the positive sense, unfortunately, for Internet crime is booming: there is a new victim every fourteen seconds on average and 54 percent of adult Internet users say they have had a computer virus infection at some point. Although there is no absolute protection against scammers, we would like to show you how you can protect yourself and surf safer in the Internet with just a few simple steps.

More helpful tips and assistance are available at **www.telekom.com/dataprotection**, along with information about data privacy and IT security mechanisms and the current threat level in the Internet. If you have questions involving data privacy and IT security, you can contact us through the above web address or by e-mail (**datenschutz@telekom.de**).

5.1. PC security and basic protection.

To ensure that the personal data on your PC remains private and safe, follow these tips.

Always be aware of how sensitive the data is.

You should never use public PCs for confidential information, because you do not know whether they have sufficient protection against viruses, worms, Trojan horses and outside attacks. Protect your PC against prying eyes. Be aware of people watching your screen when you enter sensitive data such as user names and passwords.

Always keep your system up to date.

Software vendors enhance their products continually, including the elimination of discovered security vulnerabilities. Therefore, keep your software – especially virus protection software – up to date to protect yourself against attacks. Deutsche Telekom offers a security package that protects you against such attacks, which can be ordered on a monthly basis.
www.t-online.de/sicherheitspaket

Make sure you have strong security settings.

To protect your data, install virus protection and anti-spyware programs. It is also important to configure your personal firewall. This configuration protects you against Internet-based attacks. Use your e-mail provider's virus scanner, as well, to achieve the highest possible security standard.

Check your downloads and e-mail attachments.

E-mail attachments are a common source of viruses. Therefore, only open trustworthy attachments from people you actually know. Exercise the same caution with software downloads: if you have any doubts about the trustworthiness of the vendor or website, you shouldn't download any software.

Password-protect your PC.

You should always lock your PC with a password to protect it and your data from third-party access. Make sure you have a very strong password. Once you enter the correct password, the screen is unlocked and you can continue working. We recommend configuring automatic activation of the screen and keyboard lockout together with the screen saver, five minutes after the last user activity. Of course, you can configure the activation time freely in your personal environment. You can also activate the lockout instantly, as needed. On Windows computers, press Ctrl-Alt-Del and then click "Lock Computer".

Shut off wireless interfaces.

To protect your personal PC from external attacks, shut off wireless interfaces that you are not currently using – after all, you turn the lights off when you leave the room, too. So why not shut down the WLAN transmitter on your router when you're not currently online? Most current models have a button for this on the back. The same applies to the Bluetooth or WLAN interface on your smartphone, for example, to protect it against viruses, worms and Trojan horses and to prevent unauthorized parties from accessing your personal data, such as your address book, calendar or pictures. Configure the wireless access points on the devices you use. This will make it harder for unauthorized third parties to gain access.

Data backup.

To be safe, you should make regular backup copies of especially critical, for example, on a CD/DVD-ROM or external hard drive.

5.2. Choosing a strong password.

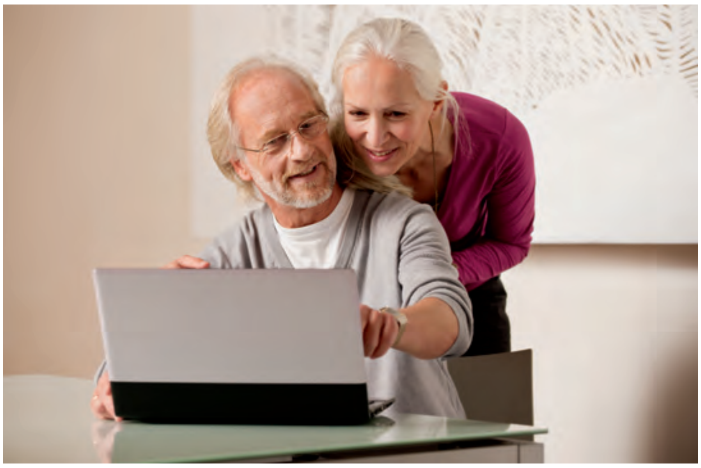
You can't do much on the Internet without passwords. And the stronger the password, the better protected the data behind it. Internet users need user names and passwords to log on to the countless forums, communities and online shopping sites.

With the fifth password, at the latest, it gets hard to keep track. Moreover, strong passwords aren't always easy to remember. But there are workarounds.

How can I create a strong password?

The golden rule for a strong password is that outsiders should not be able to identify it as a logical word. There is a simple trick for this:

Simply choose a sentence that is easy to remember and take the first letter of each word to form the password. To make the password as undecipherable as possible, use numbers and special characters as well. Example: My mom buys 16 eggs at the market every Saturday - $Mmb16eatmeS!.
Experts recommend that strong words have a minimum of eight characters, but they can also be much longer. In general, the longer and more complex the password, the better.



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

Make hackers despair.

The reason: hackers use programs to systematically test all possible password options. Therefore, each additional character increases the number of possible passwords, and thus the number of iterations the computer program needs to crack your password.

Create a separate password for every website.

Another precautionary measure: whenever possible, use different passwords for different websites. Remember that data thieves occasionally manage to steal entire customer records, including their access data.

A password that thieves get their hands on is no longer secure, since the hackers will try this password to gain access to other sites as well.

Therefore, the only strong password is one that you only use for a single website. At the very least, you should apply this rule to your online banking password.

Keep your passwords in a safe place.

In general, you should only keep your passwords in a safe place, to which only you have access. The best place, of course, is in your head. The worst conceivable place is your browser. Therefore, you should turn off the auto-complete function for all critical passwords, and never save passwords on your hard drive or write them down on a notepad near your computer.

Change critical passwords regularly.

You should change critical passwords at regular intervals to increase protection against data theft. We recommend changing passwords around every three months.

When do I need a strong password?

Possibly, you do not always need a password that meets the highest security requirements. You probably don't have to be as cautious on a fishing forum as you are with your online banking, for example.

Before you choose a password, carefully consider the following factors:

- Does it protect personal or business information (such as e-mail, contacts etc.)?
- Can it be used to carry out financial transactions (for example, in online banking or Internet auction sites)?
- Does it grant access to critical data, such as your credit card number or bank details?

If you answer any of these questions with "yes", you should definitely choose the strongest possible password.

In general: think about what the consequences would be if your password got into the wrong hands – and then decide how strong you think that password should be.

5.3. WLAN security at home.

More and more people use WLANs (wireless local area networks) to connect to the Internet.

Most people lock their doors when they leave their homes, to prevent unwanted visitors. This natural behavior in the offline world is also essential online. An unsecured WLAN makes it easier for scammers to download files from the Internet at the owner's expense and responsibility.

Moreover, a decision by the Federal Court of Justice (BGH, I ZR 121/08) requires WLAN owners to password-protect access to their WLANs.

In general, any wireless connection offers less protection than a cable-based connection. Under wireless connections, data is transmitted to the receiver through a radio frequency, which can be intercepted. All the same, you do not have to give up using wireless access: anyone can protect their WLAN against manipulation and data theft with just a few simple steps.

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

Secure your WLAN router.

Routers are usually shipped with a pre-configured network name (SSID). Changing this SSID is useful to achieving a secure WLAN, because it makes more difficult to draw conclusions about the router's manufacturer. As a result, device-specific security vulnerabilities cannot be exploited. Concealing the SSID does not improve security, but increases the configuration effort required. To change the configuration of your Telekom router, enter **https://192.168.2.1** (or, for new Speedport routers, **https://speedport.ip**) in the URL field of your browser and follow the instructions that appear. For other devices, follow the instructions in your router's user manual. Also change the pre-configured access password for configuring your router. For advice on creating a strong password, see the section "Choosing a strong password".

Configure an encryption method.

It is also essential to encrypt the WLAN access, making it inaccessible to others. In most WLAN systems, the WPA2-PSK Ⓖ. encryption method is used. In this method, a key (password) is needed to enter the network. It is important to choose a strong password and to change the default password set by the manufacturer. (See “Choosing a strong password”).

Deactivate your WLAN.

What’s more: you should deactivate your WLAN when you are not using it. In doing so, you not only protect yourself against data thieves and unauthorized use of your access for illegal activities, but also save electricity.

Tip: the Network Manager software, available free of charge at Deutsche Telekom, lets you deactivate your WLAN quickly and easily. The Network Manager helps you configure secure encryption and set up an SSID and strong password. To do so, choose menu items “Router Settings” and “WLAN Settings” in the Network Manager. You can download the Network Manager at **www.telekom.de/netzmanager.**

WLAN security on the go.

When you use public HotSpots with your laptop, in particular, you should follow this advice to protect your data as effectively as possible.

Deactivate your network share.

When you use HotSpots, deactivate the file and directory shares on your mobile device. You can usually deactivate these shares in the network settings of your operating system.

Furthermore, when you use HotSpots, you should never be logged on to your laptop with a user account with administrator permissions.

Activate your firewall.

Before you log on to an external WLAN, activate the firewall on your laptop. The comprehensive security package from Deutsche Telekom contains an intelligent two-way firewall that monitors both incoming and outgoing data traffic. This helps to prevent malware attacks.

Do not establish connections automatically.

Do not establish a connection with a HotSpot if you do not know who is responsible for operating it. Moreover, you should not allow automatic connections with wireless networks, but instead manually select the network you want to connect to.

Be wary of rogue HotSpots.

To gain access to confidential data, criminals set up their own wireless networks whose homepages are very similar to the actual HotSpot, such as Deutsche Telekom’s. When you connect with a rogue HotSpot, you are prompted to enter information such as a credit card number, allegedly to open a new HotSpot account. This manipulation technique is based on phishing techniques, which are explained in the sections on “Safe online banking” and “Protection against phishing attacks”. The only effective protection here is precise examination of the certificates used.

You can also find out about the correct installation and configuration of secure WLAN access under **http://hilfe.telekom.de**.

For information on what you need to watch out for when surfing with your smartphone, see the “Smartphone” section.

Safe online banking.

More and more people are handling their banking transactions on the Internet. This is practical, since the virtual bank branch is available at any time of day or night and can be visited conveniently at home or on the go with a smartphone.

But as convenient as online banking is, it also harbors risks. Sensitive data such as the PIN (personal identification number) and TAN (transaction number), which grant access to bank accounts, can fall into the hands of scammers if you are careless or inattentive. This happens often during phishing attacks, which the Federal Criminal Police Office sees as a serious threat.

Several different procedures have been developed to make online banking as safe as possible:

- Chip TAN procedure: a small reader, into which the EC card is placed, generates a separate transaction number (TAN) for each transaction. This number is comprised of the numeric code displayed on the reader, the EC card, the recipient's account number and the amount of the bank transfer. If parts of the code – such as the recipient's bank account number – are changed, the system cancels the transaction.

- Mobile TAN procedure: the customer gives his mobile phone number to his bank. If he wants to conduct an online bank transfer, he receives a text with a TAN that is valid for that specific transaction. The TAN expires after a short period and is only valid for the specified recipient account and amount.

- Secoder technology is the latest security development in online banking. A Secoder acts as a firewall for chip card applications. If you want to use the new Secoder procedure, ask your bank if they support them.

- Alternatively you can also use special online banking software, such as the banking software from Deutsche Telekom. The software is free of charge and offers maximum protection against pharming and phishing. It works with most online banking platforms.

General precautionary measures:

- Always keep your personal data – passwords, PIN and TAN – in a safe place.

- Never save this information on your computer.

- Never tell anyone your password. Be skeptical: a bank will never ask you for your access data by e-mail. If you receive a mail with a request like this, it is most likely a phishing attempt. For advice on how to protect yourself against phishing, see the "Phishing" section.

- Select a strong password. (see "Choosing a strong password")

- The password you use for online banking should never be used for any other purpose.

- Change your password regularly, to increase security.

- Conduct your banking transactions exclusively on your own devices in your personal environment.

- Make sure you log off at the end of the session and delete the cache on your computer.

- Important: always use up-to-date virus protection software and perform security updates to close security vulnerabilities.

- Check your account postings regularly.

- If you find anything suspicious or irregular, contact your bank immediately.

- Lock out your online banking access if you think you see anything suspicious or unusual. You can call your bank or do so directly in the online banking window.

You can also lock out your online banking account at any time with the emergency number 116116. Call the same number if you lose your cell phone, your EC or credit card, your employee ID card or other access cards.

5.4. Online shopping.

Books, home electronics, clothing and even groceries – you can order nearly anything in online shops. The transaction is worthwhile for both sides. The buyer saves a trip to the store, and maybe even gets a lower price. The seller saves the cost of renting the storefront, and only needs a warehouse.

A Deutsche Telekom survey found that more than 80 percent of German Internet users like to do their shopping online.

But what do you have to watch out for when shopping online?

Only trust who you know. In accordance with this principle, find out about the shop in question before you buy anything. Customer ratings and forum information can help prevent bad decisions and potential damage.

- When you log on to the site, at the latest, make sure the shop's web address contains an "s" after the http – this indicates a secure connection. For example, "**https://www.telekom.de**".
- Always enter the shop address in your browser manually and do not follow any links, which might take you to spoofed pages. This will help prevent scammers from intercepting your data and passwords.
- In addition, a closed padlock icon indicates a secure connection. It is located in the address bar of the browser.
- Be sure to select a strong password for your shop access. For information on how to choose a strong password, see "Choosing a strong password".
- Never tell anyone your password. Be skeptical. A serious shop will never ask you for your access data. If you receive a mail with a request like this, it is most likely a phishing attempt. For advice on how to protect yourself against phishing, see the "Phishing" section.
- Select a secure payment method, such as direct debit, invoice or cash on delivery. Or use the payment options provided by an online payment service.

5.5. Smartphones – how to surf safely.

With the introduction of smartphones, data volumes have increased drastically: from 0.2 million gigabytes in 2005 to 70 million gigabytes in 2010. No doubt - smartphones are a roaring success. As their sales figures rise, however, they are becoming an increasingly attractive target for viruses and other malware.

Safe in the mobile Internet – first steps.

Even the best software is useless if it is outdated, so you should always install updates as soon as possible. This is easier if you only install the applications you really need. Applications you no longer use can be uninstalled.

Basic protection isn't rocket science.

You should always set a password on your smartphone and activate the automatic lockout after a period of inactivity. You can also configure the smartphone to delete all data from the device if the password is entered incorrectly several times in succession. Regular backups of your data are especially important in this case, of course; most smartphones create a backup on the PC during synchronization.

Deactivating the various connection options such as Bluetooth, WLAN and UMTS when you aren't using them will protect you against undesired access. And it helps extend your battery life.

If you don't want your smartphone to reveal your location, you can simply deactivate the location functions (such as GPS).

Security à la carte.

Smartphones run on different operating systems (Windows Mobile, Symbian, iOS, Android and Windows Phone 7). The more widespread a system, the more attractive a target. Useful information on protecting your system is available at **www.telekom.com/dataprotection**.

Deleting data from old devices.

When you buy a new mobile phone, you are faced with a question: what do you do with the old device? Most of them are tossed into a drawer, given to family members or friends as gifts or sold. But what happens to the personal data on your old phone? Is it enough to delete it? To ensure that your friends cannot restore the data you have removed, the best option is to delete the device completely with a system wipe. The various operating systems each have their own methods for doing so. To find out how to delete personal data completely from your devices, visit **www.telekom.com/dataprotection.**

5.6. How to use apps safely.

Applications, or apps, can do a lot: find out when the next train departs, get the latest weather forecast or make waiting times seem shorter with casual games. Simple tips help you use apps safely.

What do I have to bear in mind when using apps?

Which data an app can access is normally displayed during its installation. The Internet connection is normally necessary for the application to send and receive data. However, some programs request significantly more access, for example, to the telephone book, call logs or the location. Most smartphones have a settings menu that allows you to prohibit specific data processing, such as the export of location data. In some cases, however, the operating systems do not allow you to choose. Here you must either agree to the transfer of data or refrain from installing the software.

Apps that gain full access to the telephone book can be a problem. Most users don't use their phone books just to manage telephone numbers, but also addresses and e-mail addresses, birthdays and pictures of their friends or business partners. In the worst case, this data can be forwarded unnoticed to the app developer.

If you want to be sure, read the information for the respective app before you install it. Especially the privacy provisions. Then decide if you are willing to submit to the developer's conditions.

If you detect any processing of your data that is neither displayed in the system nor stated in the user information, you should report this directly to the hotline of the app store provider. Most app stores have regulations that prohibit covert data processing.

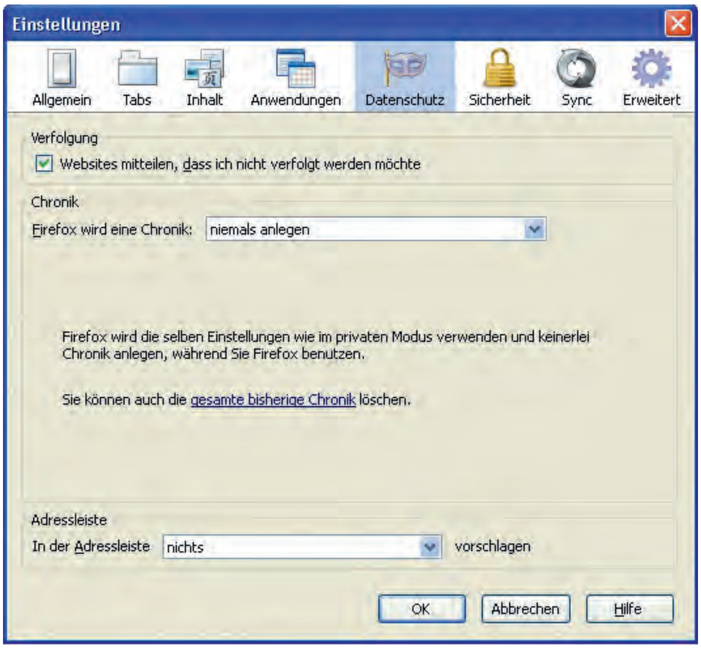
5.7. Surfing without leaving a trail.

Cookies, IP addresses Ⓖ, temporary Internet files, Flash objects, unique browser ID, surfing history and saved passwords are only a few of the trails that users leave behind in the Internet and on their own computers. To protect yourself and this data from this security risk, you should clean up your computer and erase this data at least once per month. We'll tell you how.

Delete cookies.

Web cookies are widespread – entire Internet pages are based on them and are not user-friendly without them. Cookies are small files that are saved from an Internet page to your computer and contain information such as personal page preferences, login information and unique user ID. This can make surfing more convenient.

Cookies are used when you use the shopping cart in an online shop or change the language of a web page. But they may also be used to create a complete, personalized user profile. In addition to web cookies, there are Flash cookies and super cookies, which web providers and advertisers can use to store and retrieve information. To prevent this, most browsers such as Internet Explorer, Firefox or Opera let you determine which cookies you want to accept and which you don't. Some browsers already have an option



Verfolgung

☑ Websites mitteilen, dass ich nicht verfolgt werden möchte

Chronik

Firefox wird eine Chronik: niemals anlegen

Firefox wird die selben Einstellungen wie im privaten Modus verwenden und keinerlei Chronik anlegen, während Sie Firefox benutzen.

Sie können auch die gesamte bisherige Chronik löschen.

Adressleiste

In der Adressleiste nichts vorschlagen

for notifying web providers and advertisers that you do not want to be tracked at all (see screen shot on page 64). This procedure is based on the Do Not Track standardization initiative, which is supported by Deutsche Telekom and all common browsers.

You can find out how to block cookies in your browser at **www.telekom.com/dataprotection**

Little helpers.

It isn't easy to find and delete all traffic and usage data and information. But there are programs that perform this task for you almost completely:

- Spybot Search&Destroy
  This malware protection application recognizes various forms of spyware that can invade your computer and try to spy on your surfing habits. The program deletes all traces of usage – such as surfing histories and download directories. It also closes vulnerabilities in the browser and shuts down gateways for malware and hostile websites.
  http://www.safer-networking.org/en/mirrors/index.html

- Ccleaner
  This cleanup program attempts to delete unnecessary and potentially revealing information from your computer. Among other things, it searches the central Windows database and directories where data such as cookies is usually stored.
  http://www.piriform.com/ccleaner/download/standard

And what can I do if there is information about me in the Internet that I do not want to see there?

Pictures from your school days, from wild parties, your last vacation or last weekend: people like to share their memories with friends in social networks. But what can you do if you appear in the pictures and you don't want to share those experiences with others? And how can you find out what the Internet says about you in the first place? Every 1.5-2 seconds, a new web address is registered somewhere in the world. With these millions of websites, it is nearly impossible to keep track of all the published information. Operated in collaboration with Deutsche Telekom AG, **www.secure.me** is a service that finds, evaluates, and deletes unwanted information in the Internet.

This chargeable service is aimed at consumers, parents, self-employed people and companies who want to gain a comprehensive overview of their "online me".

Anonymous surfing with IPv6.

With the introduction of the new IPv6 Internet standard there will be 340 sextillion new IP addresses in future – enough to assign unique, permanent IP addresses to every single device in the world, thus matching them clearly with specific users.

Deutsche Telekom has developed a solution for anonymous surfing with the new IPv6 Internet standard. Starting in 2013, you – the user – will be able to decide how anonymously you want to surf the web. The new IPv6 addresses consist of two parts: the network prefix, which is assigned by the network provider, and the device part. The Telekom solution employs three steps for both parts:

- Basic protection: when your device is connected to a modern Telekom router, it is regularly assigned a new network prefix. The prefix is generated randomly. This function is pre-configured in the routers.

- Privacy button: the web pages (router firmware settings) of customer routers distributed by Deutsche Telekom (Speedport) will contain a privacy button. When you click this button, you are assigned an entirely new network prefix. This reassignment can take place manually or automatically at a specified time.

- Privacy extension: in addition, on most modern devices the second part of the IP address, the device part, is automatically obscured using random logic. Always make sure that this function is also activated on your devices.

5.7. Phishing.

Criminals obtain sensitive data through spoofed (counterfeit) e-mail and web pages: they phish passwords, PINs and TANs.

Phishing is a combination of the words "password" and "fishing" and describes the interception of passwords, PINs (personal identification numbers) and TANs (transaction numbers). Spoofed e-mail messages and web pages that prompt users to enter their account data, including passwords, give criminals access to sensitive data. In most cases, a link in the mail sends the users to spoofed websites of banks and other companies that bear a great resemblance to the originals. To protect yourself against such attacks, pay attention to the following:

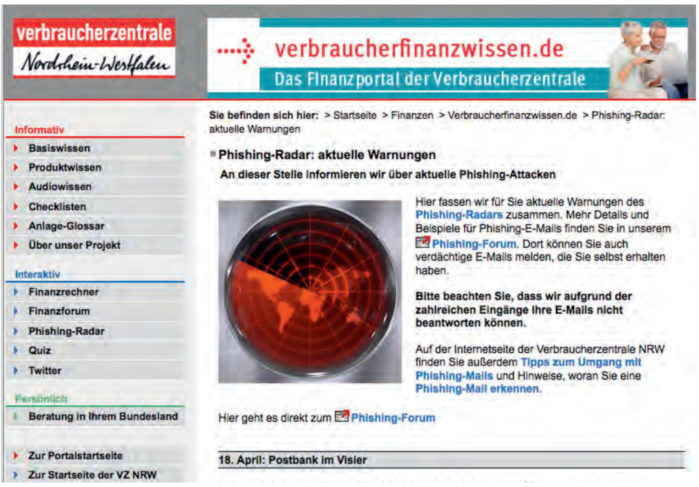
Protection against phishing attacks.

- Make note of the companies with which you do business. If the sender is not among them, the e-mail might be fraudulent, but is spam in any case.
- Pay attention to the subject line: banks and e-mail providers will never use a subject line like "Your_account_check_NOW" for their form letters.
- You can expect a service company to know your name. Most phishing mails are impersonal, at the most containing salutations like "Dear member", or "Dear customer of XY Bank".
- Service companies follow certain rules in their communications. A bank will never ask you to enter confidential data, such as PIN or TAN, in an e-mail form. Nor will a bank ever ask you for sensitive data over the phone. If you are unsure, call your bank at the number you know and ask them.
- Typos and grammar mistakes can never be ruled out in e-mails. But anything beyond one mistake should urge you to exercise particular caution.
- Odd special characters are a frequent warning signal.
- Demands that you shut down protective measures such as popup blockers or virus scanners are just as illogical.
- When you point your mouse at a specified link, the actual target URL will appear in the status bar at the bottom of most browser windows. This allows you to check whether the link actually points to the desired page.
- Activate the phishing protection features in your browser. This is supported in Firefox 3, Opera 9.5, Internet Explorer 7 and later versions.
- Whenever you want to enter personal data online, you should open a new browser window. Once you complete the transaction, log off immediately and close the window.

And the best protection against phishing mail: delete them unread.

Use caution with phishing websites.

- Always pay attention to the security certificate, which some browsers show as a closed padlock icon in the lower right corner of the window. If it does not appear, the page is not secure.
- A secure connection will always have the prefix "https://" in the URL field of the browser. This encryption procedure prevents data from being read or manipulated while you are using it.
- Exercise caution with unknown security certificates. Certificates from banks and serious online shops are known to common browsers. Contact your bank or the online shop before you accept the certificate.
- To ensure that you are always on the real page, always enter your bank's address manually in the URL field of your browser, and do not follow any links.
- A bank login page will never request you to enter a TAN. If it does, contact your bank immediately.



Sie befinden sich hier: > Startseite > Finanzen > Verbraucherfinanzwissen.de > Phishing-Radar: aktuelle Warnungen

Phishing-Radar: aktuelle Warnungen

An dieser Stelle informieren wir über aktuelle Phishing-Attacken

Hier fassen wir für Sie aktuelle Warnungen des Phishing-Radars zusammen. Mehr Details und Beispiele für Phishing-E-Mails finden Sie in unserem Phishing-Forum. Dort können Sie auch verdächtige E-Mails melden, die Sie selbst erhalten haben.

Bitte beachten Sie, dass wir aufgrund der zahlreichen Eingänge Ihre E-Mails nicht beantworten können.

Auf der Internetseite der Verbraucherzentrale NRW finden Sie außerdem Tipps zum Umgang mit Phishing-Mails und Hinweise, woran Sie eine Phishing-Mail erkennen.

Hier geht es direkt zum Phishing-Forum

18. April: Postbank im Visier

Independent websites provide information about current phishing risks.

Phishing radar.

To give consumers a way to find out about risks and report attempted fraud quickly and unbureaucratically, the Federal Ministry of Food, Agriculture and Consumer Protection and the Consumer Association of North Rhine-Westphalia have set up a phishing radar (in German) under **www.verbraucherfinanzwissen.de**. You can report phishing mails in a forum to warn other users, or send the e-mail with a brief note indicating it as a phishing attempt to the consumer association.

5.8. Social engineering.

Fraudsters make targeted use of human characteristics and weaknesses to gain access to sensitive data.

What is social engineering?

Social engineering is the attempt to use interpersonal influence to gain unauthorized access to sensitive and/or personal data. Offenders examine their victims' personal environments and simulate false identities.

How can I protect myself?

It is not easy to defend against social engineering, because attackers generally exploit positive human characteristics: therefore, the victim himself is the most important factor in preventing social engineering, by verifying the identity and authorization of the contacting party without any doubt before further actions are taken. Simply asking for the caller's name and phone number, or inquiring about a non-existent colleague, can quickly expose a poorly informed attacker. Even seemingly minor and useless information should not be revealed to unknown parties, however, because this information can then be combined with other information to scope out a larger situation. It is important to warn all other potential victims; the first instance to contact is the security department at your company, the contact address of the e-mail provider and the other people whose information was misused to portray false circumstances.

Pay attention to the following:

- If you cannot be certain about the identity of the sender of an e-mail, you should always be on your guard.
- When you receive phone calls, even seemingly unimportant data should not be given to unknown parties carelessly, because this information can then be used for further attacks.
- When answering questions by e-mail, never reveal any personal or financial data, no matter who the message appears to be from.
- Do not use any links from e-mails that require you to enter personal data. Instead, enter the URL in the browser yourself.
- If you are uncertain about the authenticity of the sender, contact them by phone to verify that the e-mail is really from them.

Botnets.

If your computer is part of a botnet, it can respond to remote commands by cybercriminals undetected, to send spam or infect other computers for example, when you are online. Botnets are a foundation of Internet crime and are one of the largest sources of illegal income on the Internet. They are networks of computers that are infected with malware.

To protect yourself against such attacks, follow the advice provided by the anti-botnet advisory center (**www.botfrei.de/telekom**):

- Check whether your computer is infected. The DE-Cleaner at www.botfrei.de/telekom finds and deletes potential malware.
- Install the latest service packs and security updates for your system and activate automatic updates.
- Install a virus scanner and update it regularly.
- Use a firewall.

At **www.botfrei.de/telekom**, the anti-botnet advisory center from the Federal Office for Information Security explains what botnets are, which hazards they pose and how you can protect yourself against them.

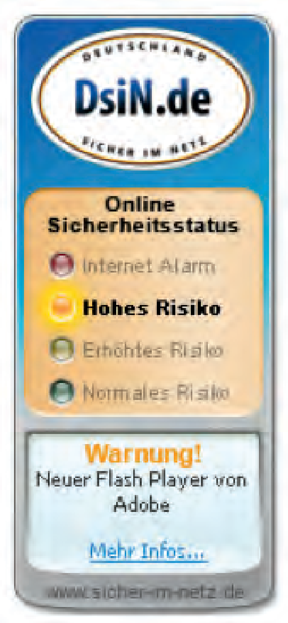
The sections "Informieren" (find out), "Säubern" (clean up) and "Vorbeugen" (prevent) contain all the information you need to protect your computer against malware in the long term.

5.9. The security barometer.

A useful tool for safe use of the Internet is the security barometer, which warns against new and recurring risks.

Located at **www.sicher-im-netz.de**, the barometer shows the current threat level in four levels:

- The blue level means "Normal risk" and tells users how to obtain the highest possible level of basic protection.
- The green level means "Increased risk" and is used to warn against acute threats whose distribution or damage potential is limited. Examples include phishing and pharming attacks with limited scopes.
- The yellow level means "High risk" and is used to warn against acute threats with significant distribution or damage potential.
- The red level means "Internet alert" and is used to warn users against current threats that endanger the availability or integrity of PCs and networks to a large extent.



www.t-online.de/sicherheit, the service pages of Deutsche Telekom, contain useful information on how to protect yourself against potential dangers. At times of normal risk levels – that is, when no acute warnings apply – the barometer provides information about basic security measures and raises awareness for current security-relevant topics and threats.

5.10. How to act in social networks.

With the dawn of Web 2.0, social networks have become a part of our everyday lives. But what do you have to watch out for? Xing, Facebook, Google+, MySpace, Bebo and many others. Many people reveal personal data on social networks as a matter of course, to share with friends, acquaintances and co-workers.

The Internet is not a legal vacuum. But not everyone always follows the valid rules, and even more importantly, the same rules do not apply equally in all countries: privacy regulations, the rights to one's own image and copyrights are not always taken quite as seriously as they are in Germany. Therefore, it is crucial to examine the platform operator's general terms and conditions and privacy notices beforehand.

Designing your profile.

- The most important consideration is to never make any personal data – e-mail addresses, phone numbers, messenger data, photos etc. – available to the general public. If you reveal too much about yourself, you make it simple for others to bombard you with phishing attempts and undesired advertising.

- You can use the network settings to restrict access to your profile. The safest setting is to only grant access to friends.

Privacy.

- Familiarize yourself with the network's privacy settings. To find out how to protect your privacy effectively on the various social networks, you can browse www.klicksafe.de in addition to the network's own privacy notices and general terms and conditions.
- Personal data should only be made accessible to your true friends.
- Some networks feature the option of dividing friends into different groups and granting different permissions to these groups. This lets you control who sees which information.

Profile pictures and photo albums.

- Although it seems almost normal to post pictures of yourself on the Internet nowadays, some pictures violate privacy protection rules. Therefore, you should consider carefully which pictures of yourself you want to show on the Internet.
- When you create photo albums, make sure that only direct friends have access to them. You can configure this in the photo album settings.
- In general, you should only upload pictures for which you own the copyright.
- Pictures that you upload to the Internet often remain saved in the cache for a long time, even if you delete them or the entire photo album. (See "secure.me" for more information.)
- Since you probably don't want to see unflattering pictures of yourself on the Internet, show your friends and acquaintances the same respect for their privacy and ask them before you post their pictures. And delete them if they ask you to.

Adding friends.

- Before you accept friend invitations or send them to others, make sure you know who they really are.

Scheduling on the Internet.

- Social networks are often used to make dates with friends and coordinate other appointments. However, private information such as dates or "I'm home alone tonight" should not be posted on your public wall under any circumstances. This information should only be exchanged privately, for example, by e-mail or messenger service.

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

Report and ignore functions.

- You should always report people, content or groups who violate the code of conduct of the networks. You can normally use the report button on your profile page for this purpose.
- The ignore function lets you ban users who harass you from appearing in your feed. Ignored users cannot send you private messages, either. In addition, you should report such people to the provider.
- Address book synchronization.
- Some networks make it possible to link external e-mail address books with the community. The sites can then match the data to see who is already a member of the network and who is not (yet). However, it is unclear what happens to this data subsequently and whether or how it is used.

- It’s not what you say, but how you say it.

- In the analog age, good manners were a sign of a good upbringing. Digital communication demands rules as well. **www.eetiquette.com** features many rules for good behavior online.

5.11. Security for kids on the Internet.

Young people between the ages of 10 and 18 are the most highly networked age group: 98 percent of them use the Internet. Most 13-year-olds are online daily.

Despite their familiarity with the digital world, many children and young people lack the knowledge to protect themselves and their data effectively. A survey of young people conducted by the German Association for Information Technology, Telecommunications and New Media (BITKOM) showed that every fourth respondent does not know how to protect data on the Internet.

In light of this, it is no wonder that parents are worried about their children’s safety. To abate this worry, you can make your children aware of the proper use of the Internet:

- Explore the Internet together.

- Speak with your children about their experiences.

- Keep an eye on the screen when your children are sitting at the PC.

- Educate your children about potential dangers in the Internet.

The website **www.klick-tipps.net** (in German) gives you and your children useful information about which websites they can surf safely, without fear of encountering inappropriate content. In its One Network for Children initiative (**www.ein-netz-fuer-kinder.de**), Deutsche Telekom promotes child-friendly websites in the Internet. **www.fragfinn.de**, a search engine, provides a safe place for children to surf.

Children and young people need to be educated in proper use of the Internet: to take full advantage of its potential, they need appropriate skills and – especially – protection.

- Define rules for Internet use and find out about safety measures.

- Special filters that you can install on your computer block pornographic, violent and neo-Nazi content automatically. Deutsche Telekom offers a solution to its customers free of charge under www.telekom.de/kinderschutz-software.

- Explain to your children that they must never reveal their personal data. When setting up an e-mail address or a chat room account, your children should make sure they only use nicknames.

- Talk with your children about the risks of real-life meetings with people they meet on the Internet. Make it clear that your children should consult with you before arranging any such meetings. Children cannot tell whether a person’s intentions are honorable.

- Discuss the accuracy of web content with your children.

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

- Encourage them to use good netiquette. Advice is available at www.eetiquette.com.

- More comprehensive information on child safety on the Internet is available (in German) at www.klicksafe.de. On behalf of the European Commission, another page will promote media skills in the use of the Internet. Children, young people and parents will find data privacy advice for Internet communities (in German) at www.watchyourweb.de.

More information and offers are available at the following websites (some are German only):

- www.klick-tipps.net
- www.ein-netz-fuer-kinder.de
- www.fragfinn.de
- www.klicksafe.de
- www.watchyourweb.de
- www.blinde-kuh.de (search engine)
- www.internauten.de (children's portal)
- www.jugendinfo.de/cyberbullying (tips against cyberbullying for children)
- www.netzcheckers.de (youth portal)
- www.schau-hin.info

Appendix.

Effective protection structures must grow and be nurtured. Deutsche Telekom works continuously on improving data privacy and data security.

6.1. Special data privacy and data security measures since 2008.

In the past years and months, Deutsche Telekom has developed and implemented measures intended to help increase the level of data privacy and data security within the Group and permanently improve the corresponding systems and processes.

These 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. Another focus is active interchange with other companies, experts and official bodies.

Measures taken by Deutsche Telekom.

- Late 2011: Presentation of a procedure that allows largely anonymous Internet use even under the new IPv6 standard.
- 2011: Expansion of the PSA process, which guarantees data privacy and data security from the very first planning step of processes and products, to the international subsidiaries.
- Mid-2010: Introduction of a standard security and data privacy procedure with standardized documents for the German Group companies (PSA process).
- Late 2009: Board resolution on the restrictive handling of process and individual case audits in the personnel area beyond the scope of section 32 BDSG.
- Mid-2009: Establishment of a separate unit specialized exclusively in data privacy audits.
- February 2009: Formation of a Data Privacy Advisory Board with leading data privacy experts from politics, academia, industry and independent organizations
- Publication of a data privacy report containing information on all recent events under www.telekom.com/dataprotection.
- 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.
- Realignment of Group Security and control structures according to the dual-control principle.
- 10-point program of immediate measures (March 2009)
- 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.

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. In general, access only to data required for the user's specific duties (need-to-know principle), an increase in general monitoring and monitoring of administrators through Group Data 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.

Interchange and collaboration.

- Interchange at the expert level among national and international Computer Emergency Response Teams.
- Sharing of analyses from attacks on Deutsche Telekom's early warning systems.
- Notification of detected malware for the anti-virus industry.
- Sharing of know-how for the establishment of cyberdefense centers.
- Participation by experts in the "LÜKEX" security exercise.

Increasing public awareness.

- Free data privacy brochure available at www.telekom.com/dataprotection
- Redesign and expansion of the online offerings on data privacy and data security at www.telekom.com
- Presentations at schools on safer surfing in the web.
- Consulting on data privacy via Datenschutz@telekom.de.
- Support for initiatives such as fragFINN e.V., Deutschland sicher im Netz, Teachtoday.
- Extensive information for customers whose computer systems have been infected with malware.
- Regular radio broadcasts with tips on safer ways to surf the web, etc.
- Chat on data privacy and data security.

6.2. Organization of Group Privacy.

Group Privacy, under the management of the Chief 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 who are not 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 supervisory authorities on employee data privacy issues at operating level.

4. Products and Services.
The Products and Services 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.

6.3. 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 specialist units concerned.

IT Service and Application Security.

The IT Service 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 (SIA) team is responsible for the security of Deutsche Telekom's internal applications, with a special focus on mission-critical applications. The Portal Systems Security (SIP) 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 (SOK) 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 (SPI) department designs security measures for Deutsche Telekom technology needed for handling value creation processes. SPI 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 team 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.

6.4. 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.

Request for information.

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

Botnets.

Botnets are networks of computers that are infected with malware. If a computer is part of a botnet, it can respond to commands by cybercriminals undetected by the true owner, to send spam or infect other computers for example, when they are online.

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, the successor organization 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.

Call centers.

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.

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.

Data breach notification.

A data breach notification is used to notify the parties affected by a violation of the security of their personal data or the misuse of same. European companies are legally subject to a data breach notification duty toward supervisory authorities and customers, as the result of an EU directive.

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.

Denial of service attacks.

Denial of service attacks are attacks from the Internet that aim to achieve a digital overload of infrastructure systems, which break down as a result.

Data protection concept.

A data protection concept is a document that contains information about the legality of data processing during the collection, processing and use of personal data. It is part of the documentation of an IT system, along with the technical concept, operating concept and security concept.

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 versions of Microsoft Internet Explorer) and browser add-ons so that a computer system can become infected simply by visiting an infected website.

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 include Google Street View and Microsoft Bing.

Research Union.

The Economy – Science research union is the central advisory committee on innovation policy that supports the implementation and further development of the German government's 2020 high-tech strategy.

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.

Group-wide consent clause (KEK).

section 95 of the Telecommunications Act defines that a customer's master data may only be used for advertising purposes if the customer has granted prior consent to do so. Deutsche Telekom asks for this consent in a Group-wide consent clause. With this clause, customers can define whether Deutsche Telekom may phone them or send them e-mails/SMS/MMS for advertising purposes, also in the spirit of section 7 of the Law on Unfair Competition.

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 notices.

Penetration test.

A penetration test is a comprehensive security test to evaluate the security of all the components and applications of a network or software system. In penetration tests, security experts use the same tools and methods that hackers use to gain unauthorized access to the system (penetration).

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.

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.

Smart metering.

The service consists of the reading, processing, presentation, and billing of power and energy consumption, using smart 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.

Telecommunications Act [Telekommunikationsgesetz].

The Telecommunications Act defines the regulatory framework for telecommunications networks and services. It regulates the telecommunications market, among other things providing protection to the general public and to individual customers. The Telecommunications Act also regulates the allocation of frequencies, as well as the numbering and approval of value-added services such as 0900 numbers.

Traffic data.

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

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.

WPA2-PSK.

An encryption method for wireless networks.

Central Security Management.

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

Certification.

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

6.5. Abbreviations.

BDSG	German 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
cIAM	Corporate Identity Account Management – manages digital identities for users and work centers 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-wide consent clause
PSA	Privacy and Security Assessment
T-Labs	Telekom Laboratories
TKG	Telecommunications Act [Telekommunikationsgesetz]
TSG	Telekom Shop Vertriebsgesellschaft

Publishing information.

Deutsche Telekom AG
Corporate Communications
53262 Bonn, Germany
Phone: +49 (0) 228 181 4949
Fax: +49 (0) 228 181 94004
www.telekom.com

Concept:
Deutsche Telekom AG and
Beecken's Agentur für
Unternehmens-Kommunikation GmbH, Düsseldorf

Design and production:
Beecken's Agentur für
Unternehmens-Kommunikation GmbH, Düsseldorf

Photos:
Deutsche Telekom AG, Fotolia

Contact.

Data Privacy, Deutsche Telekom AG
datenschutz@telekom.de
www.telekom.com/dataprotection

Life is for sharing.