Data Privacy Report 2009.

About this report.

Last year, Deutsche Telekom published a data privacy report for the first time, in which it presented the main events and focal activities of 2008. In 2010, the company is continuing its course of reviewing past events and improving operational data privacy further at the same time. In addition, Deutsche Telekom is reinforcing a corporate culture under which employees recognize the importance of data privacy and exercise the necessary diligence.

The 2009 data privacy report provides information about events relevant to data privacy, and demonstrates how Deutsche Telekom has made consistent developments in the area both internally and externally again in 2009 and what data privacy may look like in the future.

This year‘s report has a new layout: in the management report, Deutsche Telekom gives an overview of special events occurring during the past year and audit processes carried out by government agencies. It also details the measures taken to improve data privacy. In another focus section of the report, “Data privacy in detail”, the Group takes a stand on key aspects of data privacy and discusses the latest technical and political developments with an impact on data privacy.

The 2009 data privacy report delivers a clear message: Deutsche Telekom is communicating the subject of data privacy openly and transparently, and intends to set the bar in the telecommunications industry by implementing far-reaching measures and raising awareness among both employees and customers.

Content.

Preface by the Board of Management.

Dr. Manfred Balz

Dear Readers,

When Deutsche Telekom made its data privacy report available to the public for the first time last year, we found ourselves in the midst of processing data privacy incidents at our company that had shaped public discussion in 2008. In the meantime, we have succeeded in eliminating many of the identified vulnerabilities and preventing new incidents within the Group. This was also made possible by firmly anchoring the topic of data privacy at the Group Board of Management level last year within legal affairs and compliance. In the future, the accelerated pace of technical development and the strategic realignment of the Group will further increase the demands for data privacy within the company.

„The prudent handling of personal data, the customer trust built upon this prudent handling, and the transparency in handling the data are Deutsche Telekom's highest priority."

Society will face additional challenges in the future as the permanent availability of key data becomes increasingly important to users. At the same time, however, the need to keep these data as secure as possible is also growing. Data that are available from anywhere at any time must also be protected everywhere and at all times. Deutsche Telekom is supporting its customers in this area and is working to pioneer in data privacy.

The prudent handling of personal data, the customer trust built upon this prudent handling, and the transparency in our handling of the data are our highest priority. That's why we are opening ourselves to critical reviews from outside the company, such as through independent certifications and our external Data Privacy Advisory Board. I would also like to invite you, our readers, to form your own opinion on data privacy at Deutsche Telekom. This report is intended to support you in this endeavor.

I hope you find the reading interesting.

Yours sincerely,

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

Interview with the data protection officer.

Mr. Ulmer, has awareness about data privacy at Deutsche Telekom grown since the data incidents in 2008 became known?

Awareness about data privacy has definitely grown since 2008. The data incidents were inexcusable isolated cases. The resulting intense media attention triggered a real shock in the Group. The only correct consequence and response to it was to go on the offensive and address the issues transparently. The variety of actions taken and extensively communicated are the clearest evidence that sensitivity toward data privacy has increased. Greater awareness of data privacy, however, is not demonstrated solely by the reactions of top management. Since last year, we have received more than twice as many queries for advice and support for projects, systems and business models. The number of comments or queries from employees has risen to a similar extent. This means that data privacy has become a topic throughout the entire organization.

Customer and public trust hit a low point in 2008. Do you think you were able to win back that trust last year?

I am certain that at the very least we have regained a considerable portion of it. Even before the data incidents, we had a wide range of regulations and structures in place intended to ensure the trustworthy handing of our customers' data. It is always difficult to prevent or discover and expose cases of misuse that are committed with a high degree of criminal intent. To be sure, the understanding of data privacy concerns also was not as pronounced as it should have been in all areas. Even today, not everything is going perfectly yet. What's important for our customers to see, however, is that we're serious about privacy. There's no doubt that a cultural transformation has taken place.

What aspect of data privacy did you devote the most time and effort to in 2009?

There were topics related to various aspects. A primary consideration was to further work through the data incidents. But we also actively supported projects that worked toward consolidating the German Group company into a single company, Telekom Deutschland GmbH. We've done a lot in the area of auditing. Above all, we have achieved the establishment of our new auditing department, created a new auditing concept and supported the actual audits. In the international arena, we have increased our efforts and carried out our coordination function more intensely than in previous years.

In your opinion, what could have gone better in 2009 in the area of data privacy at Deutsche Telekom?

We initiated many measures and accomplished a lot. In light of this, I can say that despite the need for action that undeniably remains, I am very satisfied with progress in 2009. Unfortunately, as the data privacy organization we were not always easily accessible to our employees last year because we were so busy with operational tasks. I will address this aspect this year, though, by planning to have a stronger presence at the individual sites as well as other measures.

In the 2008 Data Privacy Report, you announced you wanted to take on a pioneering role in the area of data privacy. Did you succeed?

The Group does indeed seek a pioneering role in data privacy. That's also a management responsibility, and I welcome it heartily. I also believe we are on the right track. I know of no other company that is tackling the issues with the same transparency and consistency. And in the past at other companies, I have rather seldom observed the kind of self-criticism that we have directed at ourselves. In the operational area, we have also carried out a large number of measures and tests that are exemplary. We have delivered on the promises we made. We're carrying out the measures that we feel are necessary to offer our customers the highest possible level of data privacy.

If you could express a wish to Deutsche Telekom employees, what would it be?

Our core business model is based on the way we handle the personal data of our customers. Please always keep in mind that every action that you take can be relevant to data privacy.

If you could express a wish to the p, what would it be?

In the pending revisions of various data privacy laws, it is imperative to create regulations that cannot be interpreted ambiguously and that provide legal certainty for all involved parties. I can only urgently recommend that politicians incorporate the experiences and suggestions from some veteran data protection officers into their considerations. Nobody knows the business and its vagaries better than the experts.

Deutsche Telekom has a board member responsible for Data Privacy and you as the Group Privacy Officer. How do your activities actually differ?

According to legal regulations, the data protection officer is an independent and autonomous officer who performs a supervisory and advisory function for the company. Therefore, by definition he or she cannot be an executive manager or a member of the board of management of a company. The responsibility for the business development of a company in particular could lead to a conflict of interest with the legal supervisory function of the data protection officer. Deutsche Telekom is the first company to create a corresponding function in top management. As a primary part of the Group Board of Management, the Board Member responsible for Data Privacy, Legal Affairs and Compliance can point out data privacy concerns right from the start of strategic discussions. In addition, he or she brings more clout to the table based on his or her authority to give instructions to management and employees. In this respect, the two functions interact very well. Naturally, the Board Member responsible for Data Privacy, Legal Affairs and Compliance also has a number of other important responsibilities that go beyond mere data privacy. Legal affairs and compliance in particular are not of secondary importance, but have at least as much significance for the Group as data privacy. In this case as well, I feel it is important that these overarching issues have a direct representative on the Group Board of Management who is responsible solely for these topics.

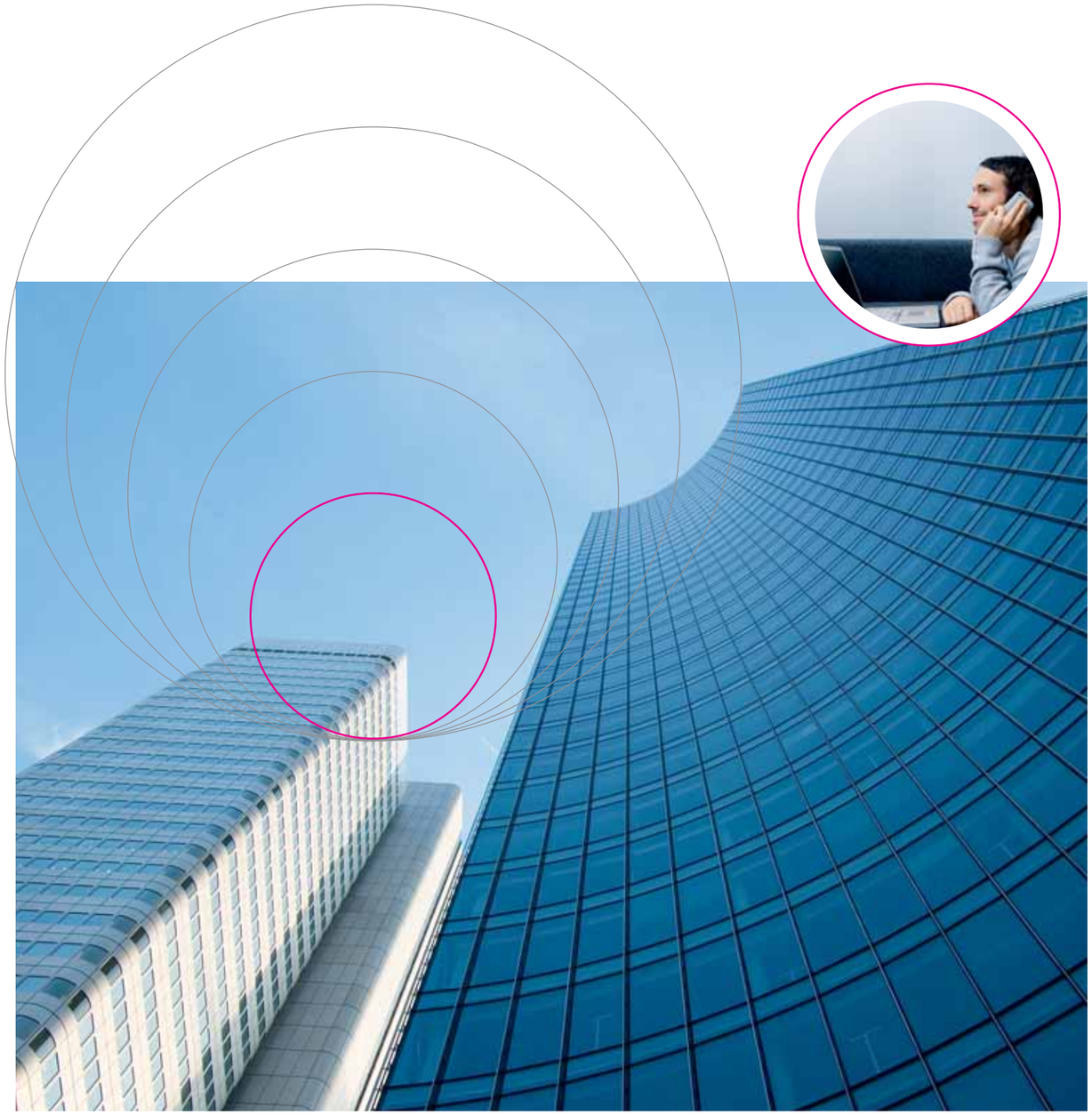
Dr. Claus Dieter Ulmer

What is absolutely necessary for successful data privacy in the company?

In everything we do, we must never forget – and this is truly important to me – that Deutsche Telekom has more than 130 000 employees in Germany alone and roughly 260 000 employees worldwide. One thing I have learned from the widely varied reactions in the past two years is that the topic of data privacy was and is an important concern for the vast majority of them. This statement is true of everyone from top managers to colleagues in the call center. If we had not had this solid foundation, we would not have been able to build on it to the extent that was absolutely necessary while we were working through the data incidents. I would therefore like to take this opportunity to especially thank these people. I hope we can also continue to successfully shape the future together on this basis.

Yours sincerely,

Dr. Claus Dieter Ulmer
Group Privacy Officer of Deutsche Telekom AG



Personal information is involved whenever data flows. Protecting this is crucial for Deutsche Telekom, which is why we are constantly stepping up our efforts in the area of data privacy and aiming to set new standards. These are our yardstick.

Management report.

2009 in review – A year of change.

After the extraordinary year of 2008, 2009 was a year of change for data privacy. Deutsche Telekom is still dealing with a wide variety of tasks simultaneously. In addition to the rapid and comprehensive resolution of the known incidents, the company has created new structures and implemented numerous measures with respect to technical and organizational aspects of data privacy. Within the Deutsche Telekom Group, measures have been initiated in all relevant departments that not only operationally improve data privacy, but foster a culture that will continue to strengthen data privacy within the company over the long term.

All efforts in the area of data privacy and data security require the support of management and employees to succeed. At the heart of data processing is the person who processes data and must be sensitized to protecting these data. That's why the initiated process of cultural change will be continued – a process that makes all employees aware that they are responsible for handling data that has come into their possession.

Measures to improve data privacy: The 10-point program of immediate measures.

In October 2008, Deutsche Telekom set up a new Board of Management department for data privacy, legal affairs and compliance. The new Board of Management department's responsibilities include centrally agreeing on the data privacy and data security measures that are necessary within the Group, initiating their implementation, and monitoring them.

The Board member responsible for this department, Dr. Manfred Balz, introduced a 10-point program of immediate measures in March 2009. This program focuses on both measures for internal data privacy and measures intended to ensure the protection of data against theft and misuse. The individual points:

1. Increased protection of Supervisory Board members.
Supervisory Board members will be better protected from unauthorized internal investigations through a new "consultation procedure." This means that beyond the regularly occurring compliance audits, the Board of Management must consult the responsible Supervisory Board committee before initiating internal investigations.

2. Protection of Works Council members.
Deutsche Telekom has established an approval process similar to that for the Supervisory Board members to protect the Works Council members. In this case, the responsible chairperson of the Works Council must be informed before internal investigations are initiated. A similar principle applies to members of the speakers' committees who represent executives.

3. Protection of media representatives.
Internal investigations of media representatives are generally ruled out. However, because journalists – regardless of their professional practice – can commit crimes, it is not possible to completely prohibit internal investigations of media representatives. In a specific case of suspicion, however, the investigations must be approved by mutual agreement between the Board Member responsible for Data Privacy, Legal Affairs and Compliance, Dr. Manfred Balz, and the Head of Corporate Communications, Philipp Schindera.

4. Countersignature of the Board Member responsible for Data Privacy, Legal Affairs and Compliance when external investigation services are commissioned.
If it is necessary in individual cases to commission external investigation services, such a commission is issued only after review and countersignature by the Board Member responsible for Data Privacy, Legal Affairs and Compliance. The "second set of eyes" principle of dual control, which is procedurally embedded in the procurement, ordering and billing systems of Deutsche Telekom, applies in this case.

5. Protection of traffic data.
The German Telecommunications Act (TKG) requires the safeguarding of telecommunications secrecy. In strict exceptions, the Act permits the analysis of traffic data if possible evidence of misuse exists in order to expose or prevent unlawful use of the telecommunications network. Steps are taken at Deutsche Telekom to ensure that, as far as possible, every access of traffic data complies with laws and regulations, is monitored strictly and is traceable. The employees who are responsible for potentially accessing traffic data have been instructed intensively in training sessions.

6. Introduction of data privacy sponsors.
A technical and a legal data privacy expert each have been assigned as sponsors of the central IT systems at Deutsche Telekom. In addition to the regular advisory and monitoring processes under Group Privacy, the responsibilities of these data privacy sponsors include unannounced checks of the IT systems. Moreover, the sponsors are available to the individual departments as contacts for data privacy questions.

7. Tightened control.
A new, technically oriented department has been established under Group Privacy Officer Dr. Claus Dieter Ulmer that focuses on the monitoring of processes, IT systems and organizational units and thus expands the existing corporate infrastructure to include relevant privacy and security standards. Thus, an important module has been added to the existing multiple-stage monitoring process.

8. Release and ongoing support of IT systems.
Deutsche Telekom has established a tighter process for the release of IT developments in a manner compliant with data protection laws. The recently implemented guideline on involvement defines in concrete terms the requirements from the Privacy Code of Conduct (protection of personal rights in the handling of personal data) in force at Deutsche Telekom. It also governs the processes of early involvement of Group Privacy with regard to development and operation of IT systems, processes and business models in a manner compliant with data privacy laws.

9. Implementation of data privacy contacts.
Data privacy contacts have been appointed at the Board of Management level and in the IT departments of the strategic business areas of Deutsche Telekom. These contacts ensure communication with the Board Member responsible for Data Privacy, Legal Affairs and Compliance, implementation of legal data privacy requirements, and process flows in compliance with data privacy laws.

10. Establishment of the Data Privacy Advisory Board.
In February 2009, Deutsche Telekom established a Data Privacy Advisory Board as the first board of its type in Germany. This Board advises the Deutsche Telekom Board of Management in topics related to data privacy. Its members include leading data privacy experts and specialists from the political, university and business arenas, as well as independent organizations. They hope to play a role in putting exemplary data privacy standards into effect at the company and providing impetus to the entire market to do the same.

Implementation of new legal regulations.

In September 2009, the amendment to the German Federal Data Protection Act (BDSG) entered into force. Many of the provisions also affect Deutsche Telekom. Group Privacy has implemented the new regulation by means of a Group-wide project and supported it with extensive information and communication campaigns. The essential topics for Deutsche Telekom are the following:

Definition of the rules for commissioned data processing.
The German legislature has defined in concrete terms the rules for commissioned data processing. The law now stipulates more precisely what must be contractually agreed, for instance, what the subject matter and duration of the commission are. Furthermore, information on the scope, type and purpose of the intended collection of data, on processing and use of the data, as well as on the type and scope of the data is mandatory. The customer is obligated to verify that the regulations are complied with before and during data processing and to document the results.

The detailed commissioned data processing models implemented at Deutsche Telekom before the amendment essentially already met the strict requirements of the new regulation and therefore had to be modified only slightly. However, Group Privacy used the occasion of the new regulation to simplify the manageability of the standard contracts it provides by adding explanations.

Requirements for consent.
Until now, consent from customers who permitted certain data processing operations always had to be in writing. Therefore, in the event that consent was given verbally or electronically, it was necessary to obtain written confirmation from the company. According to the new regulations, by way of exception written confirmation can be dispensed with if the consent is logged electronically, the involved party can call up the content at any time and consent can be revoked at any time in the future.

Electronic logging of consent was mandatory in the telecommunications and telemedia industry even before the amendment to the Federal Data Protection Act. In this respect, Deutsche Telekom welcomes the general implementation in the interest of a uniformly high level of data privacy in Germany.

**Address trading and advertisement –
Opt-in principle and mandatory selection.**
Under the amendment to the Federal Data Protection Act, the use of personal data for the purpose of address trading or advertising is permitted in principle only if the concerned party has given express consent (opt-in principle). A preselected check box in consent fields or strike-out solutions are now impermissible.

As early as 2007, Deutsche Telekom undertook to implement the opt-in process on its own accord beyond the legal regulations with its “Guideline for consumer-friendly digital products and services“ and defined and recommended this opt-in process as an additional quality criterion for consumer-friendly digital products and services.

Dr. Manfred Balz (center) presents a certificate

Deutsche Telekom has significantly expanded its activities related to certifications and audits.

Duty to inform in the event of data breaches.
Affected parties must be notified if third parties illegitimately gain possession of their data and threaten material impairment of their rights or interests meriting protection. In addition to the affected parties, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) must be informed.

Deutsche Telekom goes beyond these requirements by reporting current and critical data privacy incidents on a special web page (www.telekom.com/datenschutz) and in its public Data Privacy Report. It is the first telecommunications company in Germany to do so.

Employee data privacy.
The Federal Data Protection Act stipulates which data may be collected, processed or used for purposes of the employment relationship. The personal data of an employee may be used for discovering criminal offenses only under certain conditions. Since this regulation is interpreted in various ways in the legal sphere, Deutsche Telekom has chosen a very strict interpretation that ensures compliance with data protection laws until a clear legal regulation exists or a clear court decision is made.

Audits by government agencies.

Group Privacy at Deutsche Telekom is in continuous dialog with the Federal Commissioner for Data Protection and Freedom of Information and the German Federal Network Agency (BNetzA) regarding current issues related to data privacy as well as the measures taken at the company. Integrating the supervisory authorities early on in the event of critical data privacy issues increases transparency vis-à-vis the supervisory authorities, allowing action conforming to the law to be initiated in good time.

In 2009 the Federal Commissioner for Data Protection and Freedom of Information conducted four consultation and inspection visits. Two of these visits concerned data retention at T-Home and T-Mobile. In addition, the Federal Commissioner conducted a three-day inspection visit at T-Mobile Deutschland in May 2009. The main points were to review the processing of traffic data within the billing process and to review a system for detecting misuse. In August 2009, the Federal Commissioner visited an external call center for customer service. During this visit, he principally examined the introduction and implementation of technical and organizational requirements for commissioned data processing stemming from the amendment to the Federal Data Protection Act.

Certifications and audits.
In 2009 Deutsche Telekom significantly expanded its activities related to certifications and audits. As one of the immediate measures from the new Board of Management department for Privacy, Legal Affairs and Compliance, a new department was established within the sphere of responsibility of Group Privacy Officer Dr. Claus Dieter Ulmer to increase the auditing activities related to data privacy. All in all, over 450 internal audits and several hundred external audits were conducted on the topic of data privacy and data security in 2009. Deutsche Telekom thus relies on both internal and external expertise in ensuring a high level of data privacy and data security.

Certification by TÜV.
TÜV Informationstechnik (TÜViT), a company of the TÜV NORD Group, has audited and certified the billing process for consumers in the fixed network. As part of the billing process, all traffic data are processed and prices are calculated. This data is generated every day by approximately 30 million customers making phone calls and using the Internet and e-mail. This billing process entails very sensitive and, above all, extensive data processing by Deutsche Telekom.

In addition, TÜV Rheinland tested and certified three different customer portals in the sales department. These portals are data-processing applications that are used in daily customer contact and that give customer service representatives access to the underlying customer databases. TÜV Rheinland examined the procedures, security measures and possibilities to access data via these systems. In addition, the TÜV experts monitored how customer service representatives work with the portals. They visited Telekom shops, service centers and sales partners and spoke there with the employees. TÜV Rheinland also tested and certified the contractual agreements underlying the data processing operations performed by sales partners.

Certification by DEKRA.
The neutral testing organization DEKRA awarded the Deutsche Telekom shops its “data privacy and data security” seal. The test essentially covered two areas: First, DEKRA experts reviewed physical security, and second, they examined the handling of customer data. Several hundred shops were tested, and they all received the data privacy seal.

Internal audits.
Internal audits are important for checking the implementation of and compliance with standards on data privacy and data security. The internal auditing concept of Deutsche Telekom is based on three pillars, which will be explained in detail later in this report.

Special events in 2009.

Unauthorized cooperation with subpartners.
At the end of May 2009, Deutsche Telekom received several tip-offs from external whistle-blowers with information that orders were being generated for T-Home by call centers not authorized by Deutsche Telekom. In this context, a call center operator from Turkey also contacted Deutsche Telekom and alleged to have worked for various sales partners of Deutsche Telekom. However, he had not received any premium payments from these sales partners.

Analysis of the order data provided confirmed the suspicion that the subpartners had worked together with call centers in Turkey that were not authorized. Internal investigations revealed that the orders had been made via various sales partners and sales channels. The thresholds for detecting misuse had been bypassed intentionally. Consequently, Deutsche Telekom pressed criminal charges.

Deutsche Telekom issued warnings to three main sales partners and imposed contractual penalties. Furthermore, it demanded a return of the premiums. The sales partners asserted that they had known nothing about the illegal transactions and cooperated during clarification of the transactions. Another sales partner was terminated. Furthermore, all sales partners were firmly reminded of the requirement for authorization of subpartners and informed that Deutsche Telekom does not accept certain, specifically named marketers as subpartners.

Open Book.
After bringing criminal charges against the Group in May 2008 over the so-called spying affair, the German public prosecutor’s office seized documents from the archives of Group Security and employees’ offices with full cooperation from the company in late May 2008. In July 2009, the public prosecutor’s office allowed Deutsche Telekom access to the documents that did not appear connected to the investigation or provide any leads to prosecutable criminal acts.

Unlike the investigations by criminal prosecutors, who focused on prosecutable criminal acts not under the statute of limitations, the internal investigation analyzed the documents for any other compliance violations. These also included other acts – whether or not the statutory period of limitation had passed – that are liable to prosecution or constitute administrative offenses, such as violations of the legal provisions of data privacy or the Telecommunications Act, as well as transactions in which the conduct of Group Security, while not strictly illegal, must be viewed as ethically questionable. For example, income, asset, and other personal information was obtained illegally from sources not publicly available in Germany and abroad. Cases in which disproportionately intensive observations took place without good cause or – even if the sources were mainly publicly accessible – inappropriately large amounts of information were complied on individuals were also deemed questionable for Deutsche Telekom. In the discovered cases, Group Security had worked together on numerous occasions with external security service providers whose commissioning had long been prohibited by the Board Member responsible for Data Privacy, Legal Affairs and Compliance, Dr. Manfred Balz. Deutsche Telekom took appropriate measures to deal with the critical facts discovered in the project. These facts included not only the information of the affected parties, but also the appropriate measures against the persons involved.

Data privacy incident at T-Mobile UK.
In November 2009, the British data protection officer publicized a data privacy incident that had taken place at T-Mobile UK in 2008. An employee had forwarded customer data and information on contract renewals to third parties without the knowledge of the company. The data were apparently purchased by intermediaries and resold to other telephone companies. T-Mobile UK had immediately notified the responsible supervisory authority after the facts were discovered internally in 2007 and requested support. The authority conducted its investigations with assistance from T-Mobile UK. At the request of the supervisory authority, the public was not informed about this case at first. The investigations led to the discovery that an employee of T-Mobile UK had accessed data improperly within the scope of his duties. The employee in question has left the company in the meanwhile.

Alleged security gap at T-Mobile USA.
A blogger alleged that he had hacked the servers of T-Mobile USA. The allegation has been investigated thoroughly in the meantime. However, no indications were found that hackers had had access to customer data or company information. The allegedly affected systems are now monitored more closely due to the allegation.

Miscellaneous: Queries about data privacy.

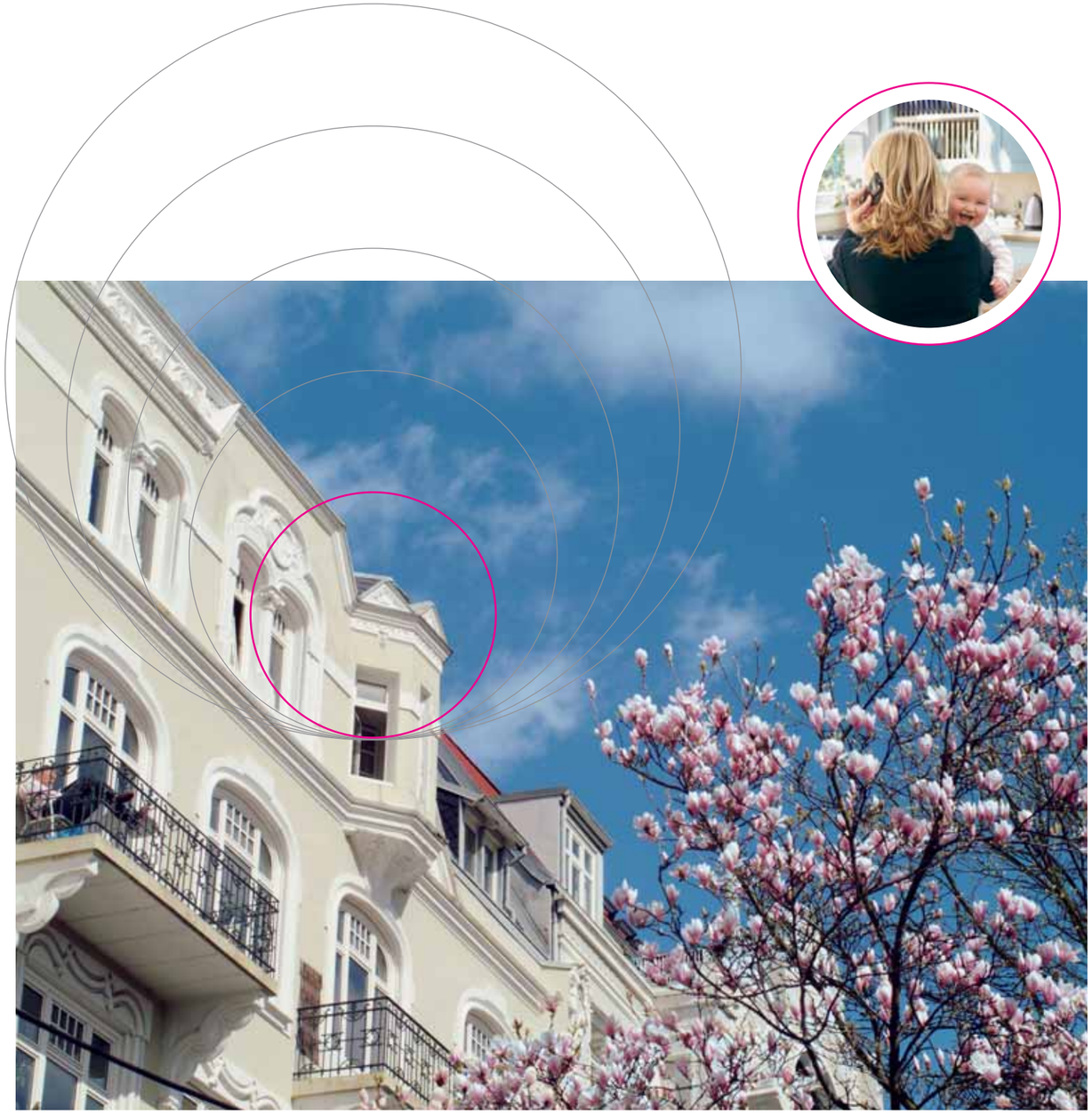
Queries.
The number of customer queries has risen dramatically since the data incidents. In 2007 there were about 600 queries, and in 2008 the number climbed to about 1 400. In 2009 as well, the number of queries remained at a high level of 1 179, the most frequent queries concerning stored data (35 percent), advertising campaigns (15 percent) and (telephone) directory listings (8 percent).

Queries from supervisory authorities have also increased. In 2007 about 170 queries were processed, and in 2008 the number was around 250. This high level was exceeded in 2009, with 264 queries. The most frequent queries concerned inconsistencies in advertising campaigns (18 percent), (telephone) directory listings (11 percent) and information on stored data (5 percent).

The queries directed at Deutsche Telekom Group Privacy with respect to project, contract and concept reviews have also risen significantly in recent years. From 2007 to 2009, the number of queries regarding employee data privacy rose from about 250 to 500, regarding customer data privacy from about 400 to 950, and regarding business customers and products from about 100 to 350.

Summary

Deutsche Telekom has attached fundamentally new importance to data privacy since the incidents in 2008 as the creation of the new Board of Management department Data Privacy, Legal Affairs and Compliance in 2008 clearly demonstrates. Deutsche Telekom understands data privacy more comprehensively than before and has reviewed its data privacy measures to date and is optimizing them all the time. At the same time, the company is working on fully clearing up all episodes linked to the incidents in 2008. Deutsche Telekom’ s focus was, and still is, on the transparent presentation of all relevant occurrences. At the same time, the Group attaches great importance to constructive cooperation with government agencies and secure and certified data privacy standards.



Phone calls, e-mail, chats, Internet shopping or cell phones as a mobile navigation device. The realm of possibilities offered by telecommunications is increasing all the time – along with the amount of data we disclose. Deutsche Telekom makes sure that this data is secure. For business customers, consumers and its own employees.

Data privacy in detail.

General regulations and measures.

In 2009, prime concerns of Deutsche Telekom Group Privacy were an understanding of data privacy issues, sensitization of employees and customer communication.

Customer communication.

Data privacy report.
In May 2009, Deutsche Telekom became the first DAX-30 company in Germany to publish a data privacy report. This report will now be published annually. Publication of the data privacy report is a further step toward fulfilling the promise to provide greater transparency in the area of data privacy and to lay the company open to public criticism.

Special web page.
After the data incidents in 2008, Deutsche Telekom set a goal of reporting extensively on the topic of data privacy within the Group. The web page www.telekom.com/datenschutz provides customers with information on the following aspects:

- Tips for handling data on the web
- Information on relevant laws and corporate regulations
- Information on security standards at Deutsche Telekom (certifications, audits and training)
- Documentation of all data privacy incidents and the measures initiated as a result
- Answers to the most frequently asked questions
- Opportunity to download the data privacy reports
- Opportunity to contact Group Privacy

Data privacy consultations.
At CeBIT in Hanover, the open house of the city of Bonn and IFA (consumer electronics trade fair) in Berlin, Group Privacy employees of Deutsche Telekom answered questions related to data privacy and web security. A contest with targeted questions on data privacy allowed interested persons to test their knowledge of data privacy and to become aware of potential dangers of revealing personal data on the web. In addition, at T-Mobile headquarters in Bonn, the Group Privacy Officer of Deutsche Telekom, Dr. Claus Dieter Ulmer, shared information related to data security on the web to all interested parents, teachers and youth during a question and answer session.

Perspectives from the Data Privacy Advisory Board.

Question

directed to Prof. Peter Gola,
President of the German Association for Data Protection and Data Security

Where do you see the greatest challenge to data privacy in the information society?
Processing of personal data has become ubiquitous in the meantime. Even those persons who want to reveal as little data as possible will not be able to escape from this reality. This applies especially to the dissemination of personal data on the web. The resulting threats to personal rights represent one of the most important requirements on data privacy. As with cloud computing these threats can be of a technical nature, caused by data processing by third parties or the affected parties themselves, in particular due to indiscriminate use of social networks.

Internal communications measures.

To firmly anchor the topic of data privacy within the company and to further improve the awareness of data privacy, the company also conducted numerous internal training sessions and awareness campaigns in 2009.

Training sessions.
The Group Privacy training concept calls for both regular mandatory training sessions and specific training sessions for individual departments and categories of employees. Some of these training sessions will be offered as e-learning modules. New employees will receive data privacy instruction when they are hired, and during a training session concluding with a test they are bound to maintain data secrecy in accordance with the Federal Data Protection Act and telecommunications secrecy in accordance with the Telecommunications Act. This training will be repeated every two years.

In 2009, Group Security and Auditing employees in particular received training. In more than 30 training sessions lasting a full day or several hours, all Group Security employees were familiarized in detail with the general legal conditions and requirements related to data protection. These training sessions built upon a solid basis, the intensive training program of Group Privacy for the security department in 2008. The auditing department received intensive training on the impact of the amendment to the Federal Data Protection Act and on handling employee data from a legal data protection viewpoint. The data protection review and consultation requirements were permanently integrated into the auditing processes. The basic data protection concept, which was developed jointly with the Auditing department and implemented there, defines in concrete terms the Auditing department's specific duties to become involved and furnish information in accordance with the guideline on involvement of Group Privacy. The basic data protection concept also clarifies the aspects that need to be taken into account during analyses with personal data.

Data protection conference for executives.
Another focus was providing support to executives in dealing with questions regarding data privacy. Deutsche Telekom therefore worked together with Datenschutzkongress für Führungskräfte (data protection conference for executives) to organize for the first time a two-day data protection conference in November 2009 in Frankfurt for all Deutsche Telekom executives in Germany. Dr. Manfred Balz, Board Member responsible for Data Privacy, Legal Affairs and Compliance, took on the role of patron. Deutsche Telekom attracted notable data privacy experts from business and representatives of supervisory authorities to speak at the conference.

Newsletter and intranet.
Group Privacy provides interested employees with information on current data privacy topics in a regular newsletter. Additional information on the topic of data privacy is available to employees on the intranet.

Cooperation with the data privacy coordinators/ Setup of local data privacy organization.
The data privacy coordinators of all business areas take on a key multiplier function for data privacy in the company. In mid-November 2009, a meeting of data privacy coordinators took place for the third year in a row at Deutsche Telekom Group Headquarters in Bonn. The main item on the agenda was presentations on new developments in data privacy at Deutsche Telekom and on implementation of the new legal regulations. In 2010 cooperation with the data privacy coordinators will be further intensified in several workshops.

Awareness campaigns.
The successful implementation of data privacy and data security requirements requires the support of management and employees. Therefore, awareness campaigns on data privacy and security were carried out in the Group in 2009 as well. In one campaign, the need to ensure that only authorized persons are present in company buildings was pointed out to employees. The campaign also included topics such as locking up important documents and the paperless office.

New procedure model for consultation and support of product and system development processes.
The procedure model was developed in the course of restructuring the Board of Management department for Data Privacy, Legal Affairs and Compliance. It defines how the individual areas within the Board of Management department for Data Privacy, Legal Affairs and Compliance collaborate and how they interact with the specialized departments of the other Board of Management departments.

A uniform procedure model was developed to define how an adequate level of data privacy and security can be ensured within the scope of consultation, release and monitoring of IT and network technology systems. The more critical a project is, the more comprehensive the consultation and support effort by the monitoring units is and the deeper the review processes and audits delve. The joint procedure takes advantage of synergy effects in the area of data privacy and data security.

Information and involvement guideline.
As part of the immediate measures on data protection, Group Privacy has drawn up an information and involvement guideline. It regulates when and how the Group Privacy department must be involved in measures related to data protection. The guideline also regulates obligations to provide information in the event of data protection violations in the Group. It applies to Deutsche Telekom AG and all national majority shareholdings. In the meanwhile the guideline has been implemented to the greatest possible extent.

Group-wide guidelines on safeguarding technical data privacy.
Greater technical data privacy means a higher level of customer confidence over the long term – which creates added value in the value added chain. Therefore, Group Privacy has worked on various basic regulations for technical data privacy jointly with IT Security. The Group Security Policy and the Privacy Code of Conduct are at the top of the hierarchy governing the guidelines on technical data privacy. These guidelines are used to create minimum Group-wide standards for an adequately high level of technical security at Deutsche Telekom. Central guidelines result in further subject-specific guidelines which detail selected aspects of particular importance to the data privacy and data security.

Setup of a separate department for monitoring.
As part of the immediate measures program of the Board of Management department for Data Privacy, Legal Affairs and Compliance, a new department has been established within Group Privacy. The department's responsibilities are to ensure implementation of data protection requirements through increased monitoring and audits of IT systems as well as increased efforts toward establishing uniform data protection standards.

Auditing concept of Group Privacy.
Data privacy audits are an important element for checking the implementation of and compliance with standards on data privacy and data security.

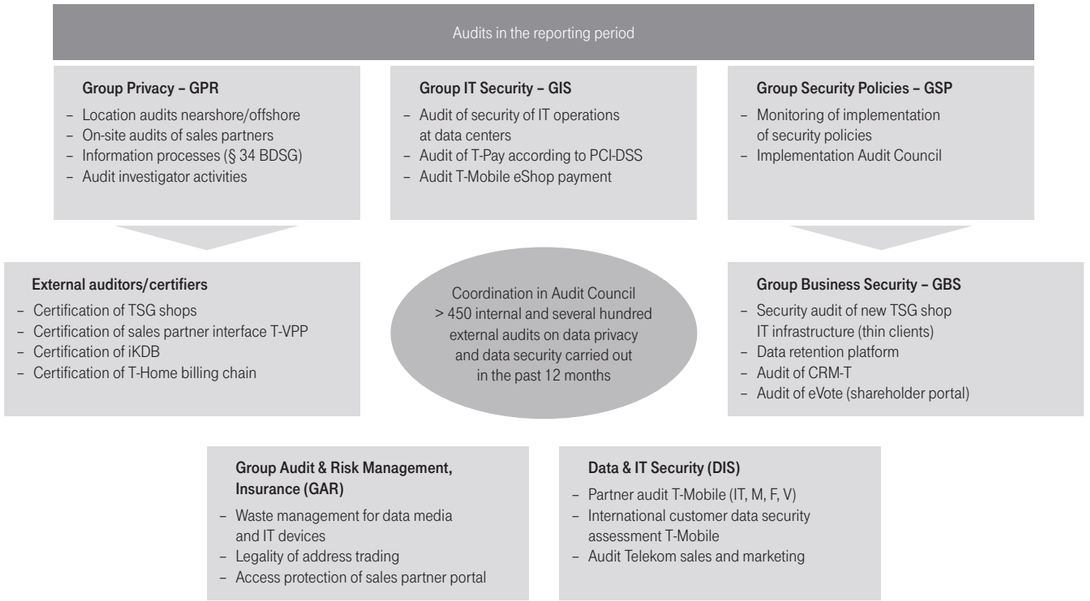
Data privacy and data security audits.

	Organizational controls	Standard procedures	Audits
Internal	BilMoG data privacy CLCs International basic data privacy audit BilMoG security CLCs S-OX security controls	Data privacy consultation Review and approval of data privacy concepts Case-related reviews after internal indications Vulnerability management	Annual audit plans Acceptance audits Event-driven audits External certifications
External	ISO 27001 audits Audits by the BfDI	Case-related reviews after external complaints (BfDI, customer, BNetzA)	Review of security concepts acc. to TKG § 109 by Fed. Network Agency

Nevertheless, audits are only one, albeit important, component for achieving an adequate level of data privacy at Deutsche Telekom. Many other monitoring mechanisms ensure that data privacy and data security measures have been implemented. In addition to organizational controls according to the U.S. Sarbanes-Oxley Act (S-OX), the German Accounting Law Modernization Act (BilMoG) or certifications according to recognized standards (ISO 27001), these mechanisms include the processes for consultation, review and approval of data privacy and security concepts, external reviews through supervisory authorities and the processing of information and complaints from customers and employees regarding data privacy problems.

The auditing concept of Deutsche Telekom comprises three pillars. The first is the basic data privacy audit, which is conducted at both the national and international level. The second pillar covers system, organizational and process audits. The third pillar provides for special audits in the event of incidents or suspicion. The third pillar also includes the acceptance audits, which are conducted before the release of prioritized projects.

Overview of audits in the Group environment on data protection and data security.



Audit focus in 2009.
The audits conducted in 2009 focused on the following aspects:

International audits.
One focus was the review and certification of an appropriate level of data privacy of internal and external service providers in the nearshore and offshore environment. For instance, several T-Systems production sites in Russia, the Czech Republic and Hungary were audited and an appropriate level of data privacy was certified for them under certain noncritical conditions. The same applies to external partners such as Cognizant in India and Reksoft in Russia.

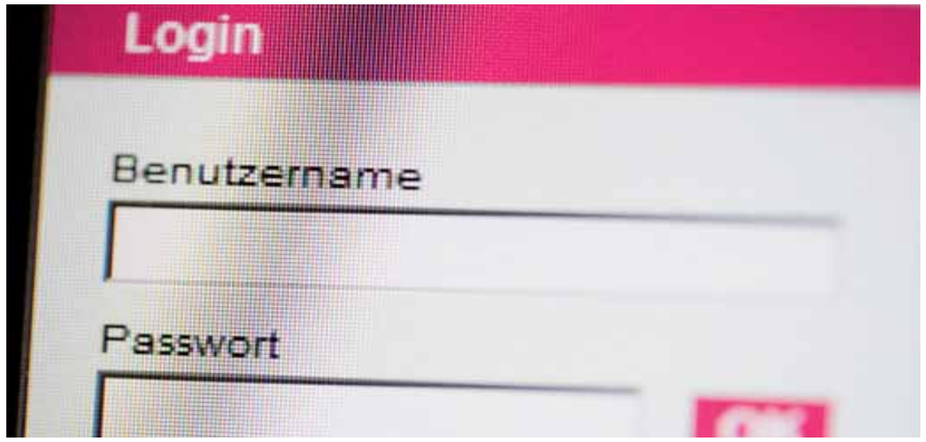
Disposal of data media in compliance with data privacy laws.
Deutsche Telekom had audits carried out regarding the disposal of paper and data media in compliance with data privacy laws at several Group sites and at various sites of the disposal company. The auditors also investigated the process designed to ensure that mobile communications devices returned by customers are disposed of in compliance with data privacy laws and that data stored on these devices are reliably deleted before the devices are recycled.

Audits of sales partners.
Various sales partners of Deutsche Telekom were also audited. In addition, auditing and certification criteria on the topic of data privacy were defined, according to which selected sales partners are required to go through a certification process for certain business models or outbound call centers of Deutsche Telekom are certified. Outbound call centers are Deutsche Telekom's partner companies that support the Group in telephone sales of Group products. Furthermore, criteria were defined to enable a more conclusive evaluation of service providers' compliance with the technical and organizational data privacy measures based on existing contracts for commissioned data processing.

Process audits at Group Security.
A number of internal processes at Deutsche Telekom were audited. For instance, the way in which Group Security carries out its investigation process was reviewed. Given the spying cases that took place, this is viewed as a sensible measure subsequent to reorganization of Group Security and introduction of the data protection concept for this department.

Monitoring the company within the scope of the German Accounting Law Modernization Act.
In accordance with the German Accounting Law Modernization Act (BilMoG), Deutsche Telekom has established an internal control system that covers a wide range of departments. This control system is examined annually by external auditors with regard to its suitability and implementation. Within this system, a separate control environment that deals specifically with the organization as well as the regulations and processes for compliance with legal data protection requirements has been assigned to Group Privacy. The audit was successfully conducted for the first time in 2009. The potential areas for improvement identified during the audit were directed to the responsible offices and implementation was initiated.

Outlook for auditing focus in 2010.
In 2010, more audits of sales partners and commissioned data processors will be carried out. In addition to audits of internal and external service providers in the nearshore and offshore environments, a focus in the international arena is on-site audits on the implementation of and compliance with the Privacy Code of Conduct in the international units of Deutsche Telekom. Moreover, the most critical and most important applications and databases in the Group will be audited, and acceptance audits will be carried out for the most important IT systems and platforms.



Deutsche Telekom has established an internal control system that covers a wide range of departments. This is examined annually by external auditors with regard to its suitability and implementation.

Perspectives from the Data Privacy Advisory Board.

Questions

directed to Prof. Dr. Peter Wedde,
Professor of Labor Law and Law in the Information Society at the University of Applied Sciences, Frankfurt a.M.

Recently an employee data protection act was discussed. Do you think we need more legal regulations in this area?
A single, comprehensive legal regulation on employee data privacy is long overdue. An employee data protection act would create legal certainty for employers and employees alike and prevent many conflicts from occurring in the first place. This includes, for example, the definition of clear boundaries for the permissibility of monitoring employees by means of technical equipment such as video cameras, as well as the regulation of the permissibility of medical examinations in application processes. It is also important to limit the permissibility of "voluntary" consent of employees for cases in which the existence of a pressure situation cannot be reliably ruled out.

Should personal use of the Internet be allowed at work?
Web applications such as e-mail and browsers are matter-of-course sources of information and means of communication for many people today. Many employers do not have a problem with employees occasionally using company Internet access for personal reasons. The only problem is that the permission for personal use means that the Telecommunications Act necessarily applies. From a legal viewpoint, employers are then automatically subject to the same high requirements for data privacy and data security as, for instance, a provider of mobile telephone services. This results on the one hand in high requirements on the technical security of the business systems. In addition, provisions of the Telecommunications Act preclude employers from viewing the contents of their employees' communications without a way to differentiate whether the messages are business or personal e-mail. It would be good if the legislature would ensure that this mechanism is rescinded. To this end, only a slight modification to the Telecommunications Act would be necessary to rule out the situation that the limited personal use of business systems alone means that this Act applies.

Status of employee data privacy.

A series of cases in which German companies illegally collected and used employee data became known in 2009. This clearly shows the lack of understanding that still prevails in at least part of the economy and the insufficient knowledge with respect to the legal framework of use of personal data.

Following the motto "Trust is good, but control is better," companies are justifying their monitoring activities based on their need to actively protect themselves against employee misconduct. From a legal perspective, this is a trade-off between employers' rights, protection of the company, and employees' personal rights established in the German Basic Law.

Under no circumstances may a general suspicion be sufficient to encroach upon personal rights. According to the German Federal Data Protection Act, personal data may be analyzed only in specific cases, for example, in the case of definite suspicion of a criminal offense in the employment relationship. And this is permitted only if less drastic means to clarify the suspicion have been exhausted.

Framework conditions in the Deutsche Telekom Group.
Central framework conditions on employee data privacy have been defined in the Privacy Code of Conduct and the works agreements at Deutsche Telekom. The Privacy Code of Conduct uniformly regulates internal requirements on handling of personal data within the Deutsche Telekom Group. In addition, the works agreements create special rights and duties for employers and employees and thus form binding standards for handling personal data within the scope of the agreements. A prominent example of a works agreement with a strong legal data privacy component is the rule on handling video surveillance measures. Employee data may be analyzed only in the event of security incidents and only by offices authorized to do so. These offices are then listed in a data protection concept. Activities to monitor behavior and performance that go beyond this limit are expressly prohibited. The works agreements also include regulations regarding deletion periods. Furthermore, employees are informed about the use of video equipment.

Every two years, Group employees in Germany are obligated to maintain data privacy and telecommunications secrecy.

Projects from 2009

Telekom Awareness for Compliance and Ethics.
Since 2009, one of the world's leading providers of compliance training has offered a uniform training and communications platform related to compliance with codes of conduct, laws and directives, for example, to prevent corruption. Due to its stock exchange listing in the United States and the resulting requirements, Deutsche Telekom is obligated to implement special training measures throughout the Group. A number of these web-based training modules apply to selected employees, and others must be completed by every employee within a specified time frame. Deutsche Telekom has adapted the service relationship itself and the training system to the strict data privacy requirements in the Group. In particular, the company has taken steps to ensure that impermissible evaluations based on training results cannot take place.

1000° survey tool from Multimedia Solutions GmbH (MMS).
"1000°" is a new web-based system that Deutsche Telekom has used for employee surveys since 2009. In this case, the Group had to ensure that neither participation in the survey nor the statements made in the survey can be traced back to individual employees. To prevent employees from participating multiple times, the Group does e-mail a personalized invitation to a survey to the participants. However, the personal reference is automatically deleted after the e-mail is delivered and in this way the responses are analyzed without reference to individuals. If department results are queried, the results are analyzed only for departments that exceed a certain number of employees to prevent the possibility of indirectly tracing results back to individuals. The individual surveys are submitted to Group Privacy for approval.

Review of electronic personnel files.
In 2009 the system for managing personnel files was converted to an electronic process. A prerequisite for this was the availability of personnel files in electronic format. In this context, the electronic personnel files of employees were reviewed by Group Privacy and Human Resources Service Telekom with the involvement of the employee representatives to determine whether personal data of other employees had been incorrectly mapped to them. In 2 056 424 documents, 3 678 documents were found with personal data of other employees. This represents a (slight) error rate of 0.18 percent. The main cause of these errors was incorrect allocation in the documents that had originally been provided for digitization. If there are still individual cases where the personal data of other employees is found in personnel files, each employee can correct the information on the intranet using a complaint and correction process that has been agreed on with the employee representative.

Group-wide obligation to maintain data and telecommunications secrecy in 2009.
Every two years, Group employees in Germany are obligated to maintain data privacy and telecommunications secrecy. Regular training sessions on the Privacy Code of Conduct are required in the other parts of the Group. The regular repetition of the obligation in connection with a training and sensitization campaign ensures that all employees are reminded on an ongoing, continual basis that it is necessary to comply with the data privacy regulations. In addition to ensuring a high level of data privacy, Deutsche Telekom thus also fulfills the contractual and legal obligations towards its customers.

Implementation of § 32 German Federal Data Protection Act (BDSG).
There were special requirements in 2009 with respect to implementation of the provisions of the new § 32 BDSG. For the first time, the provision explicitly regulates the principles of employee data privacy within the general data protection law. The wording of the provision had resulted in some uncertainty among experts, even though it had been the legislature's goal to present the existing legal situation more clearly. The new provision creates clear regulations on handling employee data, on carrying out the employment relationship and on using employee data in the prosecution of criminal misconduct of employees within the employment relationship. At the same time, however, it further increases the uncertainty in the area of mass processing of data to monitor processes. The question of to what extent the processing of large volumes of data is still permissible for the purpose of checking whether employees are behaving properly still has not been clarified. The Deutsche Telekom Board of Management has therefore decided to limit corresponding monitoring processes to their verified permissible core for now. As a result, Group-internal investigations by Group Security and Group Auditing in particular are no longer conducted as a rule. Exceptions are subject to a strict approval process.

Handling health data.
The handling of data concerning the health status of employees is governed in a restrictive manner at Deutsche Telekom. Such data may be processed only if this is absolutely necessary to carry out the employment relationship and legal provisions require this. Questions regarding the health status of employees are permissible only if it is feared that the relevant employee is impaired for a designated job. In the case of disability, questions may not be asked regarding the cause of the disability or the medical diagnosis. Only those persons who, for actual and legal reasons, are directly involved in the respective process out of necessity – under a strict interpretation of the principle of necessity – may receive such information. In 2009, all executives in Germany were once again explicitly referred to this regulation.

Outlook.
In the future, a manual on the privacy of personal data will be developed and introduced within the Group as an orientation guide for handling employees' personal data. Its purpose is to summarize the partly isolated legal data-protection regulations, standard questions and provisions and to serve employees as a "data privacy compass." Goal: Establish clear specifications and standards to facilitate communication, reduce the complexity of the contents, and foster a basic understanding with regard to the processing of employee data.

After the decision handed down by the German Federal Constitutional Court, Deutsche Telekom immediately stopped retaining and providing information about all stored data.

Status of customer data privacy.

Framework conditions in the Deutsche Telekom Group.
In 2009 quite a few legal regulations entered into force, resulting in changes and reforms in customer data privacy:

Data retention.
Data retention was introduced for fixed-network and mobile telephony starting in 2008. The regulation stipulated the obligation of telecommunications companies to store information including the telephone number of the calling party, time and duration of the call and, in mobile communications, the cell in which the connection was started. In January 2009, the duty to store e-mail messages and Internet usage data also entered into force. According to the German Telecommunications Act, as of this date the mailbox ID of the sender and every recipient, the IP address of the sender, and the date and time of e-mailing including the time zone had to be stored for six months when e-mail was sent. In the case of Internet usage, the data retention obligation covered the dynamic IP address of the user, the unique line ID used for access, and the date, time and time zone of the beginning and end of the Internet session under the allocated IP address.

Deutsche Telekom Group Privacy provided legal data-protection support to the responsible departments in implementing the data retention specifications in the Group. The focus was on separating the database from the actual customer database, securing it against unauthorized access and complying with the legal deletion periods. During an informational visit in 2009, the Federal Commissioner for Data Protection and Freedom of Information gained an overview of the actual implementation of data retention at T-Home and T-Mobile. The supervisory authority was satisfied with the chosen solutions.

After the decision handed down by the German Federal Constitutional Court on March 2, 2010, which declared the existing regulation on data retention to be unconstitutional, Deutsche Telekom immediately stopped retaining and providing information about all stored data; the data stored was deleted irretrievably.

Perspectives from the Data Privacy Advisory Board.

Question

directed to Prof. Dr. Hansjörg Geiger,
Honorary Professor of Constitutional Law at the Johann Wolfgang Goethe University, Frankfurt, and State Secretary of the Federal Ministry of Justice from 1998 to 2005

In 1983 the Federal Constitutional Court derived the right to privacy of personal information from the general personal rights and human dignity. Does the use of creditworthiness data encroach upon the right to privacy of personal information?
The subject of creditworthiness data concerns the right to privacy of personal information in several ways. It starts with the question of the legality of collecting creditworthiness data or the information from which "creditworthiness data" is derived. A potentially essential aspect in this case may be whether this collection takes place with the consent or at least the knowledge of the affected person.

Another crucial point is whether the creditworthiness data in reality correctly reflect the current creditworthiness of the affected person. Also the way in which such creditworthiness data are brought about, such as the transparency of the "calculation" of the creditworthiness, touches upon data privacy. It must also be evaluated to what extent such data should be retained for vaguely definable purposes and whether this take place for one's own justified business purposes in connection with contractual relationships with the affected person to the extent necessary for this.

The use of creditworthiness data, meaning their collection, storage, forwarding and other processing, thus obviously touches upon the right to privacy of personal data, because creditworthiness data represent personal information. However, this does not mean the ban of all uses of creditworthiness data. Use of these data may be permissible on the one hand with the express and clear agreement by the affected person, insofar as this permission is granted in cognizance of its significance ("informed consent") and is not made dependent on the performance of other services. In addition, their use may be permissible, insofar as a corresponding compliant and clear legal regulation exists for this and the principle of proportionality is kept.

Perspectives from the Data Privacy Advisory Board.

Question

directed to Prof. Dr. Peter Wedde,
Professor of Labor Law and Law in the Information Society at the University of Applied Sciences, Frankfurt a.M.

What do you think about the purchase of data for advertising purposes?
In view of the numerous cases of misuse in this area as well, I am skeptical about this topic from a legal data protection viewpoint. In addition, in the last amendment to the Federal Data Protection Act the legislature did not really succeed in effectively strengthening and safeguarding the rights of customers and consumers. As long as the possibility is not ruled out that affected parties could be adversely affected or personally encumbered, I favor a restrictive judgment of the permissibility of purchasing data for advertising purposes.

Location-based services.
The German Telecommunications Act governs the use of mobile communications location data for location-based services (LBS). There are two different methods of positioning. In device-based positioning, subscribers with mobile devices identify their location themselves as part of a location-based service, such as to find establishments in their vicinity. Various location-based services also offer network-based positioning. This allows subscribers to determine the location of other subscribers. For instance, this service allows parents to determine the geographical location of their children.

For both methods of positioning, § 98 Telecommunications Act stipulates that mobile phone users must have consented to the use of their location data, or positioning, in advance. On the initiative of the government, in August 2009 the regulation with respect to network-based positioning was tightened: Since then consent must be in writing. In addition, subscribers must be notifed via text messaging about the positioning operations after no more than five operations. The LBS providers are contractually obligated by T-Mobile to obtain the corresponding consent in writing. Furthermore, T-Mobile specifies the precise consent wording and obtains corresponding monitoring rights from the LBS provider. The informational text message is sent directly from T-Mobile to the subscriber. Against this backdrop, the discussion concerning the issue of whether the mentioned new regulation in § 98 Telecommunications Act addresses network operators or service providers is not relevant to Deutsche Telekom. As the network operator, T-Mobile has provided the preliminary services and already implemented the necessary steps.

These business models will change in the future: The support of the mobile network operator will no longer be necessary for positioning in the future. Mobile devices increasingly have their own, much more accurate positioning option via GPS and give their location directly to the respective service providers via an Internet connection. New services build upon this option.

Use of data for advertising purposes.
The amendment to the German Federal Data Protection Act, which entered into force on September 1, 2009, stipulates that the use of data for advertising purposes requires the active consent of the party involved. Previously, the parties involved had to opt out if they did not wish to receive advertisements. This change does not affect Deutsche Telekom. The Telecommunications Act that applies to telecommunications service providers had already required such consent prior to this. Deutsche Telekom had already actively queried its customers for permission to use their data for advertising purposes in the past in accordance with the legal regulation. If customers give consent verbally, they are also sent a written confirmation containing the exact wording as well as explanations of the object of the advertisement consent.

Topics from 2009.

Cooperation with sales partners.
The protection of customer data in sales and service occupied Group Privacy during all of 2009. In 2008 marketing contracts containing new, stricter agreements for commissioned data processing had already been concluded with sales partners. In 2009 various technical hurdles intended to prevent unlawful mass processing of customer data records were introduced. These hurdles are built into the IT systems and customized based on need and operating scenario.

Furthermore, Deutsche Telekom introduced a list of IP addresses that were explicitly approved for access to customer data. At the same time, it issued a list of IP addresses that were expressly barred from access. In addition, it designed various alarm systems that are activated if abnormal activity occurs, such as elevated numbers of data access operations.

The protection of customer data in sales and service occupied Group Privacy during all of 2009. In the same year various technical hurdles intended to prevent unlawful mass processing of customer data records were introduced.

Perspectives from the Data Privacy Advisory Board.

Question

directed to Peter Franck,
Chaos Computer Club (CCC)

What do you think are the greatest data risks for Internet users?
A risk to be taken seriously even though it's hard to grasp is the steadily growing number of data pools in which every user leaves tracks – usually unknowingly. This information has become a significant economic factor in the meantime. However, it's not only Internet users who are affected, but also for instance mobile phone users, who continually disclose information about professional and social relationships as well as their current location.

The biggest risk occurs in the merging of different data pools, since this allows third parties to create a precise profile of each and every person that represents their personal, social, political and economic relationships. Deutsche Telekom possesses a formidable volume of such data pools, because it serves in many different roles, including as network operator, information agency, payment system provider and media provider.

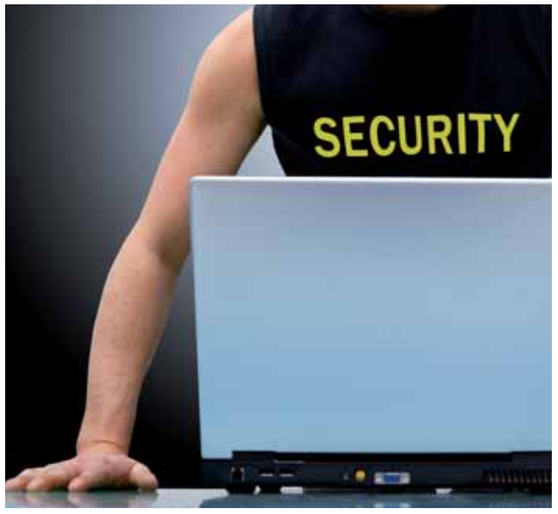
Implementation of a TAN procedure.
To protect customer data even better, Deutsche Telekom had already implemented a TAN procedure for mobile communications in 2008. Customers who contact a customer agent in the Telekom shops receive a text message with a TAN (transaction number) on their mobile device as soon as the customer agent would like to call up their customer data in the system. The Telekom shop employee cannot access the data of the involved customer until he or she has entered the TAN provided by the customer into the system.

After the TAN procedure was implemented, it was discovered that the procedure cannot be used in isolated cases, such as if the SIM card has been blocked or the mobile phone has been lost. In 2009 an alternative to the TAN procedure was introduced for these isolated cases. In addition to their phone number, the customers give the customer agent their SIM card number, customer number or account number. The customer agent cannot access the involved customer's data until this procedure has been followed. Moreover, the customers receive a confirmation text message to ensure that no unauthorized orders or changes are made. To limit the alternative procedure to individual cases, the Telekom shops may each support only a set percentage of customers via this procedure.

T-Home Entertain: Data delivery of set-top boxes.
The receiver used for T-Home Entertain, the set-top box, is connected to the Internet. Deutsche Telekom delivers the television programs and videos requested by customers to their set-top boxes via the Internet connection.

In addition to the operating data that is necessary for using the services of T-Home Entertain, the set-top box also recorded the customers' usage data, meaning the date and time, the length of time and the content of the respective TV session for statistical purposes (viewing figures).

The usage data were transferred to a central server and then anonymized for the statistical analyses. Group Privacy criticized this procedure, since the data should be anonymized as soon as possible. As a result, the collection and transfer of data were totally stopped. Procedures that allow anonymization as early as possible or strong pseudonymization of the data are currently being investigated. Likewise, consent models that allow transmission for purposes of supplementary services are being discussed.



Text messaging for reverse searches at T-Mobile.
In a reverse search, directory assistance provides the name of the subscriber that belongs to a phone number. T-Mobile Deutschland did not support the reverse search in the past and therefore did not inform its customers about the possibility of this kind of search. Accordingly, T-Mobile Deutschland also did not use customer data for reverse searches or transmit data to providers of information services. This practice was in keeping with the widely held view in the market that § 105 Par. 3 Telecommunications Act governing the reverse search contained only the right, but not the duty, of service providers to use the possibilities of the reverse search. However, in a decision in July 2007, the German Federal Court of Justice (BGH) applied a divergent interpretation to the relevant provisions of the Telecommunications Act. To protect the business model of information service providers – contrary to the wording of § 105 Par. 3 Telecommunications Act – telecommunications service providers are obligated to make their customer data available to information service providers for reverse searches. While the decision directly affects only the involved parties to the dispute, thus not T-Mobile, T-Mobile nevertheless decided to make the reverse search available according to the decision of the German Federal Court of Justice.

In Deutsche Telekom's view, the limitations on the processing of customer and traffic data in non-EU countries laid down in the German Federal Data Protection Act need to be reviewed.

In June 2009, T-Mobile implemented the reverse search technically. As a prerequisite, T-Mobile had to inform the affected customers about the new search and in particular point out to them their right to object to the release of their data for the reverse search. In June 2009, T-Mobile sent a text message to roughly 900 000 customers who were already listed in the telephone directory at their own request. In the message, the company referred to reverse search and the data storage associated with it as well as the option to object. The text message resulted in a small number of inquiries from journalists and customers. The data privacy organization and customer service informed the affected parties in detail about the background and the necessity of the action. The explanations were received positively. There were no lasting complaints.

Unwanted listing in the phone directory.
Through a notice issued by the Federal Commissioner for Data Protection, Deutsche Telekom was made aware that customers had been listed in the phone directory against their will when they switched products. Research by Group Privacy revealed that this error was attributable to the entry of around 720 000 faulty data records over two weeks into a system that makes the directory listings. The error was corrected at the behest of Group Privacy.

Vivento customer services.
On behalf of Deutsche Telekom customer service (DTKS), the Fraunhofer Institute checked all internal and external service providers who are acting for DTKS in the context of commissioned data processing. On February 3, 2009, an audit was carried out at Vivento Customer Services (VCS), a subsidiary of Deutsche Telekom. The Fraunhofer Institute discussed issues related to organization, human resources, information security and instructions with VCS employees. The Fraunhofer Institute certified that VCS meets the requirements of commissioned data processing. In its final report, the Fraunhofer Institute especially highlighted the involvement of Group Privacy in the acceptance of new or modified software in a positive light. In addition, it recognized the clear responsibilities, good process documentation, the high degree of organization of the five-year-old "start-up", as well as the successfully tested establishment of a security management program with regional security managers.

Need for regulation and action.

Revision of the German Federal Data Protection Act.
The coalition agreement of the German federal government of October 2009 stipulates that the German Federal Data Protection Act should be easier to understand and read. Deutsche Telekom welcomes this plan. The regulations on commercial use of data were already very comprehensive before the amendment to the Federal Data Protection Act. The amendment of September 2009 has added new regulations and differentiations that make a legally secure assessment of the various provisions more difficult.

Review of special regulations for the telecommunications industry.
In Deutsche Telekom's view, the limitations on the processing of customer and traffic data in non-EU countries laid down in the German Federal Data Protection Act need to be reviewed. The regulation in § 92 Telecommunications Act prohibits the processing of telecommunications data outside of Germany with a few exceptions.
Telecommunications traffic data is particularly sensitive data. However, in the eyes of Deutsche Telekom this does not justify the heavy restriction on data processing in non-EU countries via the regulation in § 92 Telecommunications Act if an appropriate level of data privacy is in place locally. Within the scope of a new regulation, higher requirements could be placed on telecommunications data than on data in other economic sectors.

For the maintenance and service of its data centers operated in Germany, a company like Deutsche Telekom depends on international companies that distribute the maintenance tasks to their worldwide branches according to the "follow-the-sun principle." As viewed from Germany, this means that maintenance is carried out from Asia in the morning, from Europe in the afternoon, and from American countries in the evening. The current legal regulation prevents such global, competitively priced maintenance, because in many cases the support services also require a glance at data out of necessity. As a result, Deutsche Telekom must build up additional resources for three-shift operation in Europe.

German Data Protection Audit Act.
Within the scope of the amendment to the German Federal Data Protection Act, an independent Data Protection Audit Act was not enacted in 2009. Deutsche Telekom thinks such a law regulating the process and framework conditions of data protection audits at companies is urgently needed. The government coalition has now announced an independent data protection foundation that is to be responsible for independently and neutrally auditing and evaluating the compliance of products and services with data protection laws. Deutsche Telekom expressly welcomes this. However, steps must be taken to ensure that data protection audits in the future are based on uniform and reliable standards in order not to lose the confidence-building effect of certification marks. Especially as regards customer contact, externally verified compliance with data protection laws is an important means of gaining customer trust over the long term.

Especially as regards customer contact, externally verified compliance with data protection laws is an important means of gaining customer trust over the long term.

Status of data privacy of business customers and large projects.

Projects from 2009.

De-Mail.
De-Mail, the communications solution that T-Systems has developed in conjunction with partner companies such as United Internet and the German Federal Ministry of the Interior (BMI), will make it possible to send electronic messages in a way that is legally binding, confidential, and tamper-proof. A requirement for this is that both the sender and the recipient provide unique identification. The provider also supplies the user with a legally binding confirmation to substantiate the dispatch and delivery of a De-Mail. From October 2009 through March 2010, De-Mail is being tested in a pilot project in the T-City of Friedrichshafen, the "future lab" of Deutsche Telekom. After a successful pilot phase, Deutsche Telekom plans to launch the product throughout Germany.

Group Privacy has been supporting the project in Friedrichshafen. Group Privacy tested and approved a data privacy concept that is required in the draft of the underlying Citizens Portal Act.

Electronic health card/electronic patient file.
Electronic health cards are to replace the present health insurance cards in the future and will serve as the access key to various healthcare applications. Insured physicians in private practice and hospitals should be able to jointly access centrally stored patient files in the future.

T-Systems has developed a corresponding system with support from data privacy and data security experts at Deutsche Telekom. Access to patient data requires that patients identify themselves with their electronic health cards and PINs and physicians identify themselves with their electronic health professional cards. In addition, special hardware – a connector – is needed to establish a connection to the server with the electronic patient files. Thus access from a PC at home is not possible. Patients can view their patient files at self-service stations at hospitals or doctors' offices.

The electronic health card transfers the power of disposal over one's own file from the physician to the patient for the first time. In this way the patient can grant a new physician access to his or her file without having to ask the previously attending physician to hand them over.

New (electronic) identification card.
In November 2010, a new identification card is scheduled to be launched throughout Germany. Each citizen from the age of 16 and up will receive an identification card the size of a credit card, either when their current ID card expires or earlier if desired.

This new identification card is equipped with an RFID (radio frequency identification) chip. The chip stores data, can encrypt and decrypt, and enables all necessary processes for handling and using certificates. The new identification card also enables an electronic signature. As a result of public discussion in Germany, a biometric fingerprint is voluntary upon request by citizens and no longer mandatory. According to information from the German Federal Office for Information Security (BSI), no data will be stored centrally. Furthermore, only the data that are noted in printed form on the ID are recorded locally by the identification authorities.

T-Systems received support from data security and data protection experts from Deutsche Telekom while developing the new identification card. The data stored on the cards are encrypted, ensuring that only those persons who have a justified interest can read the data. Every service provider who must be able to read relevant data receives a terminal certificate in advance from a central agency. This certificate is restricted to the uses permitted by law. The entity that will be this central agency for issuing and managing the terminal certificates (authorization service and blocking service) is currently under discussion. The terminal certificate and the requested data, divided into necessary and voluntary information, are displayed to identification card holders when they use their identification cards. The identification card holders release the data by actively confirming the request and entering a six-digit PIN known only to them. If a wrong PIN is entered three times, the identification card will be blocked and will no longer function.

In cloud computing, data is no longer processed and services are no longer performed on the users' computers, but via a network service which the users can access from their respective terminals.

Need for regulation and action.

Implementation of new consultation models and Group Privacy approaches in the business customer and product development areas.
An important component of Group Privacy activities in the future will be the redesign of the consultation model for large projects. Corporate customers are increasingly demanding data protection and data security solutions. Therefore, the more highly standardized review processes already implemented for the consumer market and employee data privacy will be applied to corporate customers in the future, which will require even greater professional integration of sales employees. This will ensure that corporate customers receive expert data protection advice from the very first contact. The product unit where new services and business models are developed for the entire Group will also provide more advice on standardized requirements in the future.

Cloud computing.
After the technical conditions were created, cloud computing has been the focus of increasing attention at Group Privacy. In cloud computing, data is no longer processed and services are no longer performed on the users' computers, but via a network service which the users can access from their respective terminals, including mobile devices. As a key technical condition, Deutsche Telekom first had to enable data transfers at suitably high data transfer speeds from mobile devices as well. This is the only way to offer customers satisfactory run times for a business transaction. The company must create a large number of other basic technical conditions that require intensive support related to data protection laws.

Status of international data privacy.

International data privacy in the face of new challenges.
In recent years, the trend of processing personal data transnationally has continued to gain ground. As companies expand operations globally, the markets grow closer together. At the same time, customers have become more dynamic themselves and are demanding global interaction with their service providers.

This market development has necessitated appropriate, transnational data privacy. In Germany and the European Union, the framework conditions for using personal data are being developed further and further; countries outside the EU are pursuing a different data protection policy. Homogenous international data privacy does not currently exist, a situation that international data privacy experts criticize. At the 31st International Conference of Data Protection and Privacy on November 4-6, 2009, in Madrid, more than 1 000 representatives of companies and organizations from over 80 countries worked out the "International Standard on the Protection of Personal Data and Privacy", an important step for creating international standards for data protection and privacy. For companies with global operations, the government initiatives to reach a uniform standard for data protection and privacy at the international level as well are vitally important.

Perspectives from the Data Privacy Advisory Board.

Question

directed to Prof. Dr. Hansjörg Geiger,
Honorary Professor of Constitutional Law at the Johann Wolfgang Goethe University, Frankfurt, and State Secretary of the Federal Ministry of Justice from 1998 to 2005

Under what conditions should online searches be allowed?
Article 1 Par. 1 of the German Basic Law stresses that human dignity is inviolable. From this the German Federal Constitutional Court (BverfG) derives a "core area of the private conduct of life" which may not be encroached upon and which is also excluded from any balancing with other equally important legally protected interests. The general personality right according to Article 2 Par. 1 in conjunction with Article 1 Par. 1 of the Basic Law also includes the basic right to the guarantee of confidentiality and integrity of information technology systems.

Online searching is a covert measure that represents a particularly serious encroachment upon basic rights. There exists the general assumption that a lot of sensitive personal data is stored on a private "information technology system." According to the judgment of the Federal Constitutional Court, the complete monitoring of the data stored on such an information technology system also makes it possible to draw far-reaching conclusions about the personality of the affected party, up to and including the possible development of behavior profiles due to the potentially extremely large and meaningful pool of data. The information that is stored on a privately used computer, and the conclusions that can be drawn about personal interests based in part on the use of the computer as a means or communication and of obtaining information on the web, can touch upon the core area of the private conduct of life.

Consequently, online searching can be compatible with the German Basic Law only if steps have been taken to ensure that this core area of the private conduct of life and thus human dignity of the person affected by such a search are not violated.

Even an online search that safeguards this core area may not disproportionately encroach upon the rights of the affected person. It should be noted that "security" must never be the sole criterion for the permissibility of serious encroachments upon basic rights. Rather, the balance between freedom and security provided by the Basic Law must be safeguarded at all times. This means that an online search cannot be taken into consideration at all unless the situation is a matter of protection for extremely paramount interests such as the lives of people or the existence of the state.

The legislature itself must also prescribe the necessary procedural precautions to prevent encroachments upon the core area of private conduct of life as well as disproportionate measures. Apropos, an online search that included the information technology system of an uninvolved third party, that is, of a non-troublemaker, would also not be proportionate. In particular, the exclusion of such non-troublemakers requires intensive preliminary investigations that the legislature must make within the scope of the necessary precautions to protect uninvolved persons. Besides, the inviolability of the home established in the Basic Law must also be respected. Ultimately, the legislature must define the prerequisites for effective judicial supervision and procure adequate briefing of the affected party.

International data privacy at Deutsche Telekom.
Due to the lack of international standards on data protection and privacy, Deutsche Telekom, represented in 50 countries worldwide, has created its own Privacy Code of Conduct as a foundation for international data privacy. This Code establishes explicit framework conditions and a clear organizational structure with binding responsibilities regarding data privacy at the parent company and its subsidiaries around the world.

To support the international activities of Deutsche Telekom, Group Privacy is promoting and coordinating the establishment of an international network of data protection experts. On an international level, data protection officers bear the responsibility for data privacy at their national companies. They deal with the implementation and execution of and compliance with the Privacy Code of Conduct. Furthermore, they advise and support project teams during projects that fall under data protection laws and provide both regular reports and incident reports to Deutsche Telekom Group Privacy.

In 2009 Deutsche Telekom Group Privacy also conducted audits at the national companies to review and support local implementation of data privacy specifications. Moreover, Group Privacy and the local data protection officers are available to the national companies for support concerning all data privacy issues both on a legal and a technical basis.

The experiences gained in the cooperation between the parent company and the subsidiaries of Deutsche Telekom have shown that further increasing efforts to cooperate internationally makes sense for securing the level of data privacy over the long term.

International projects from 2009.

"Internationalization of Data Privacy, Legal Affairs and Compliance" project.
The Board of Management department for Data Privacy, Legal Affairs and Compliance has highlighted cooperation with the national companies of Deutsche Telekom by launching the "Internationalization of Data Privacy, Legal Affairs and Compliance" project. In the area of data privacy, the company is building upon the international data privacy organization coordinated by Group Privacy.

Perspectives from the Data Privacy Advisory Board.

Question

directed to Prof. Peter Gola,
President of the German Association for Data Protection and Data Security

More and more personal data are being stored electronically. How secure can such storage be anyway?
Absolute security will never be achieved, as is generally the case when technology is used. Based on the criteria specified and to be further developed by the legislature, the security standard must be at such a level that any remaining hazard potential can be accepted. The principle of proportionality is definitive.

International data protection manual.
The "International Manual for Data Protection at Companies of the Deutsche Telekom Group" has been written, creating another basis for supporting the internationalization of data privacy in the Group in addition to the Privacy Code of Conduct. The data protection manual contains information about implementing Group Privacy standards at the subsidiaries. It also contains training programs and support on international issues.

Support of international projects.
The increasing internationality of projects means that the need for advice related to international data protection is steadily rising. Group Privacy has supported a large number of projects concerning customer and employee data privacy. The number of requests from T-Systems International GmbH for support with large orders has also gone up. As customers, multinational groups are demanding multinational solutions that Deutsche Telekom must support within data protection laws. In 2009, Group Privacy also supported the acquisition of parts of telecommunications companies outside of Germany. The national companies are contacting the parent company with more and more inquiries and complex cases regarding transnational agreements on the processing of order data. This development illustrates the general trend toward internationalization and calls for in-depth support in cross-border data protection issues.

International audits.
Group Privacy of Deutsche Telekom carries out data privacy audits at the national companies to support local implementation of the data protection requirements of the Privacy Code of Conduct. In the international basic data privacy audit, the participating companies comment on their conformity with the Privacy Code of Conduct as part of a self-disclosure statement. In 2009, Spain, Hungary, Great Britain, Austria and the Netherlands took part in the basic data privacy audit, as well as the United States, Mexico, South Africa and Japan from outside the EU. In 2010, on-site implementation was verified through numerous spot tests.

Need for regulation and action.
Owing to the interweaving of various technologies and the further development of the web into a global social communications platform, data protection challenges are becoming increasingly complex. Therefore, creation of international data protection standards is vital. As a global telecommunications company, Deutsche Telekom will face these challenges in the future and implement its own international data protection standards jointly with its national companies.

Status of cooperation with government agencies.

Consultation and inspection visits by the Federal Commissioner for Data Protection and Freedom of Information.
In 2009 the Federal Commissioner for Data Protection and Freedom of Information visited Deutsche Telekom four times for consultation and inspection. The visits involved the following areas:

Review of data traffic processing at T-Mobile Deutschland.
The focus of the three-day inspection visit at T-Mobile Deutschland in May 2009 was to review the processing of traffic data within the billing process as well as to check a misuse detection system. The Federal Commissioner determined a need for regulation with respect to individual data storage periods and the logging of access to the traffic data. The responsible departments are presently implementing the new requirements. Group Privacy is supporting this process by providing advice. The supervisory authority is also involved in this process to ensure that all requirements are fully met.

Data protection review at the call center.
The consultation and inspection visit to a call center for customer service in August 2009 was focused in particular on the technical and organizational processes and measures that are necessary in accordance with the legal regulations in § 11 Federal Data Protection Act to ensure the necessary level of data protection and data security within the scope of a contractual relationship with external service providers. The Federal Commissioner for Data Protection and Freedom of Information had, in view of the additional restrictions that entered into force on September 1, 2009, listed specific requirements that were used as the basis for the review. He appeared to be satisfied with the results of the inspection visit and determined that Deutsche Telekom is implementing his requirements in contractual documents. In addition, he certified that the sales partner is complying with the agreed technical and organizational measures.

Special government regulations.
Various German laws at the national and state level oblige telecommunications companies to allow the security authorities to monitor telecommunications as well as to issue information about traffic and customer data to the security authorities.

The legal basis for monitoring telecommunications stems from the German Code of Criminal Procedure and the individual state police codes. A telecommunications monitoring operation must be ordered by a judge.

Traffic data includes information on who communicated with whom, when, and what telecommunications equipment was used. The contents of telecommunications are not reported, just as for a telecommunications monitoring operation. The requirements to obtain judicial orders stem from the German Code of Criminal Procedures and the individual state police codes and, for intelligence services, from the German Federal Constitution Protection Act (BVerfSchG) and the individual state constitution protection laws. Normally, a judicial order is required.

Customer data means the data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services. The legal basis for obtaining information on customer data is found in the German Telecommunications Act. A judicial order is not required insofar as the information is necessary for prosecuting criminal or administrative offenses, for defending against threats to public safety and order, or for fulfilling the legal regulations of the constitution protection authorities at the national and state level, the German Intelligence Service or the Military Intelligence Service.

At Deutsche Telekom, three “regional offices for special government regulations” in Frankfurt, Hanover and Berlin are involved with issuing information related to the fixed network and the web. The “authority information” office in Münster issues information related to mobile communications. Legally correct handling of queries from security authorities is centralized not least because a telecommunications company like Deutsche Telekom quickly runs into danger of rendering itself liable to prosecution itself due to obstruction of justice (for furnishing allegedly insufficient information) or due to breach of telecommunications secrecy (for furnishing information too “generously”).

Police requests for information.
In accordance with § 113 Par. 1 German Telecommunications Act, anyone who provides telecommunications services commercially or contributes to such services must in individual cases furnish information about customer data to the responsible offices immediately upon request, insofar as this is necessary for defending against threats to public safety or order. As the authority that prosecutes criminal or administrative offenses and that is responsible for defending against threats to public safety or order, the police are authorized to request information. According to an order by the German Federal Network Agency and a decision by the Higher Administrative Court (OVG) in Münster, information about the name and address of a subscriber distinguished by means of a dynamic IP address must also be furnished to the responsible offices if they must access traffic data in their investigation.

The regional offices for special government regulations of Deutsche Telekom presently respond to police requests for information on the basis of this requirement without demanding the submission of a judicial order.

Information on owners of copyrights and ancillary copyrights.
Since September 2008, providers such as Deutsche Telekom have been obliged to furnish to owners of copyrights and ancillary copyrights upon request information about customers who allegedly have offered the copyright-protected works on web exchange sites. The right to information of the copyright owner stems from the German Copyright Act. Due to the associated encroachment into telecommunications secrecy, however, the copyright owner must first apply for judicial permission.

In a manner permissible under data protection law, Deutsche Telekom stores the corresponding data for seven days. The provisional court order must be presented within this period. The court checks whether all legal requirements for obtaining information have been met. It investigates whether the applicant is really the owner of the copyrights or ancillary copyrights, whether the situation is an apparent 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 court order is issued on the basis of which Deutsche Telekom releases the secured data (IP address, date, time, first name, last name, street address, city, postal code, user ID) to the respective copyright owner or the owner’s legal representation. After completion of the process, Deutsche Telekom deletes all corresponding data in accordance with legal requirements.

Status of data security at Deutsche Telekom.

Experts make a distinction between data privacy and data security. The German Federal Office for Information Security defines the term “data privacy” as the protection of personal data from misuse by third parties. “Data security” means the confidentiality, availability and integrity of systems that process and store information. Another term for data security is the designation “information security.”

Three Board of Management departments at Deutsche Telekom deal with the topic of data security. The Board of Management department for “Privacy, Legal Affairs and Compliance,” headed by Dr. Manfred Balz, establishes the Group-wide data security strategy as well as specific rules regarding data security. The Board of Management department for “Product Development, Technology and IT Strategy” converts these security requirements into technical systems. The Board of Management department for Germany is responsible for reviewing the procedural and technical security measures. Spreading the data security topics among three Board of Management departments ensures a principle of multiple control. This takes into account the great importance of data security at the company.

Within the Board of Management department headed by Dr. Manfred Balz, the Group IT Security department is responsible for establishing the data security strategy and specific rules regarding data security. It is led by Thomas Tschersich, who has been entrusted with security issues of Deutsche Telekom since 1995.

Data security projects from 2009.

Privacy and Security Assessment.
The objective of the Privacy and Security Assessment project was to incorporate integrated IT security and data privacy concepts, as well as corresponding specifications in these areas, into the respective Group development processes early on. Previous distributed and non-uniform approval processes were replaced and a uniform, standardized procedure for IT security and data privacy was implemented in the projects. This ensures that only those IT systems and platforms that have been tested explicitly for security and data privacy requirements are put into operation.

Vulnerability and advisory management.
A slight element of uncertainty is inherent in IT systems. As time goes on, new vulnerabilities emerge that were not known yet at an earlier point in time. This situation makes it necessary on the one hand to eliminate newly discovered vulnerabilities in a timely manner. On the other hand, steps must be taken to ensure that those responsible for IT systems can deal with reports about new vulnerabilities in a timely manner.

Personnel responsible for IT systems receive current security reports about their systems and software via the CERT (Computer Emergency Response Team) platform installed in 2009. At the same time, the elimination of known vulnerabilities is monitored fully and continuously with defined deadlines. Furthermore, Deutsche Telekom established a central IT scanning system that is capable of searching through all IT systems within the Group's network for current vulnerabilities. This scanning takes place at regular intervals, whereby the system components that work with particularly sensitive data are checked more frequently than others. The system's criticality determines the scanning frequency.

Identity and access management (IAM) system.
The goal of an identity and access management (IAM) system is to uniquely identify physical persons or services in an organization. In addition, the system checks access to resources in this organization. Resources may be released only after an approval process has been completed. This process is monitored and documented by the IAM system. If the validity of access authorization to resources has expired, the IAM system revokes access authorization. By setting up a central IAM system in place of the current distributed systems, Deutsche Telekom can further increase data security and reduce costs.

Optimization of Security Policies.
Only when uniform security policies can be implemented easily throughout the entire Group will this also happen in practice. The development of clear, understandable and unambiguous security policies is the goal of the Optimization of Security Policies project. Optimization creates transparency and boosts users' acceptance of the policies. This in turn has a positive effect on how well the security policies are adhered to and on IT security as a whole. In addition, the intelligibly written policies enable employees involved in projects that are affected by the security policies to clarify questions on data security themselves.

Next-Generation Network Security Framework.
The next-generation network (NGN) will be the future network infrastructure for services such as voice, data, video and IPTV. It is based on Internet technology, meaning that all data of all services are transported by means of the Internet protocol (IP). The innovative technology and architecture of the future network infrastructure entails new kinds of risks and dangers. They are a huge challenge for safeguarding an adequate level of security.

In 2009 the goal of the Next-Generation Network Security Framework project was to design a general framework for security in an NGN-based infrastructure, which will now form the basis for setting up the security functions in the next generations of networks.

Future

New data processing models throw up new challenges for data privacy specialists all the time - the latest topic under discussion: cloud computing. Storage services and applications are no longer operated from PCs at home, but from a network of data centers in what is termed a "cloud." A variety of clouds are possible: private clouds in which just one company combines storage services and applications, or public clouds in which different customers share capacities. A public cloud of this kind can, in turn, extend across various geographical areas. Experts are currently discussing how sensitive data can be best protected and secured in cloud computing. The IT and telecommunikations industry association BITKOM is calling for a separate "Cloud made in Germany."

Interview with Thomas Tschersich.

What are the data security challenges of the future? Thomas Tschersich, Head of IT Security, shares his thoughts.

What do you think will be the greatest data security challenge in the next few years?

That's certainly the virtualization of IT systems, which we're now seeing in the business customer segment. The term "cloud computing" is on everyone's lips. It means that a separate system is not set up for each application, but that many "virtual" systems are installed on one and the same computer. This makes things more complex and also increases the potential security risk.

Which data security project of the past few years are you particularly proud of?

I am proud that we managed to obtain certification for our sales partner systems from TÜV Rheinland. That was a particular challenge, since the certifiers impose very strict standards. I'm especially proud that the project team assembled from many units of the Group accepted the challenge and implemented the necessary measures for system certification in record time.

One of your goals for 2010 is to establish uniform procedures and methods for managing identities and authorizations. What does this mean exactly?

The challenge for large companies with a wide range of IT systems is to manage different users and their respective authorizations in all of these systems and keep them up to date. Users change jobs within a company, receive additional authorizations and must relinquish others. Over time the company has an extremely complex network that entails enormous potential for optimization for the sake of efficiency alone. The goal for 2010 is to work with the IT department to jointly establish central systems for managing users.

Another goal is to establish early warning systems and emergency response processes. Can you name a few examples of emergencies in the area of data security?

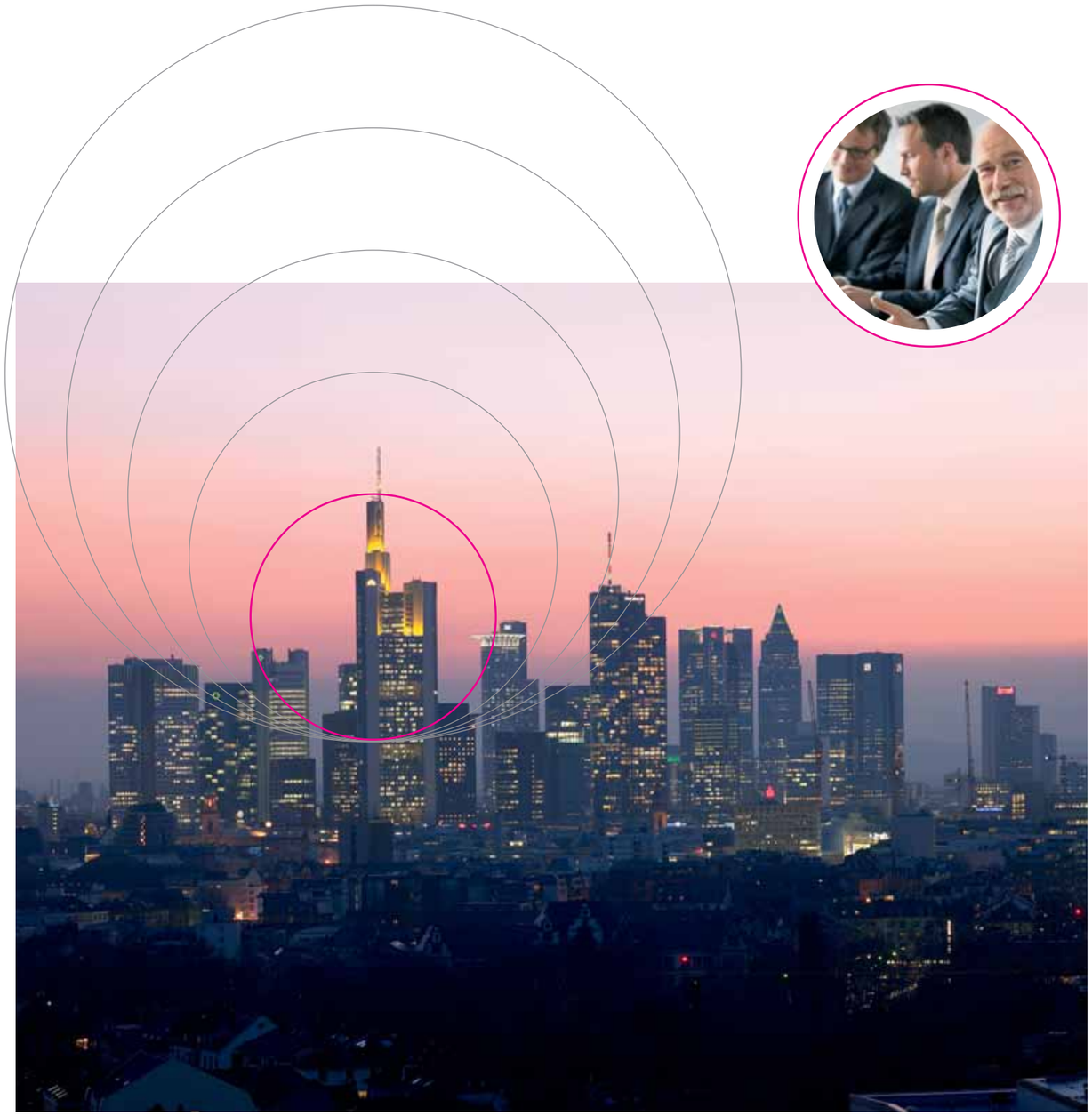
We're all familiar with the messages reporting about new security gaps and risks in IT systems. Our job is to make sure that newly discovered vulnerabilities cannot be exploited to the detriment our customers. Especially with regard to early warning systems, there's still a need for action at Deutsche Telekom as well. It's imperative to detect new vulnerabilities so early that preferably they are closed before they can be exploited by criminals. We're working together on this at an international level with computer emergency response teams (CERTs), a type of fire department for IT systems.

NGN stands for next-generation network, the future network infrastructure for services such as voice, data, video and IPTV. In NGN, all data is transferred via the Internet protocol. What data security challenges are associated with that?

Previously we had a telecommunications infrastructure that was virtually self-contained. The telephone network around the world was operated by just a few companies, and there were no open interfaces to other systems. That's different in today's world. All systems are networked with each other via the Internet. As diverse as the new communications options are, the associated challenges to secure the involved systems against each other are just as diverse.

What does "IT system criticality" mean? Which of Deutsche Telekom's IT systems have a high criticality with respect to their data security? Which have a low criticality?

Each Deutsche Telekom system is evaluated with respect to its criticality. The purpose is to determine whether particularly sensitive data, such as customer data, are processed in a system. We apply the following principle: The higher the criticality, meaning the more sensitive the contents in a system are, the higher the requirements are that we place on the security measures to be taken.



Data Privacy Advisory Board.

Data Privacy Advisory Board of Deutsche Telekom.

The Data Privacy Advisory Board of Deutsche Telekom was established in February 2009. It grapples with design approaches to data privacy in telecommunications and telemedia. It works out proposals for designing processes and products of the Deutsche Telekom Group and the telecommunications industry in a way that complies with data privacy. It deals with the following topics in detail:

- Business models for handling customer data
- Business processes for handling employee data
- IT security and the appropriateness of measures
- International data processing
- Implementation of new legal regulations

Its members include leading data privacy experts and specialists from the political, university and business arenas, as well as independent organizations.

- Wolfgang Bosbach, Member of the German Parliament, lawyer and Chairman of the Committee on Internal Affairs
- Dr. Michael Bürsch, Member of the German Parliament, retired
- Peter Franck, Chaos Computer Club (CCC)
- Prof. Dr. Hansjörg Geiger, Honorary Professor of Constitutional Law at the Johann Wolfgang Goethe University in Frankfurt am Main, and State Secretary of the Federal Ministry of Justice from 1998 to 2005
- Prof. Peter Gola, President of the German Association for Data Protection and Data Security (GDD)
- Bernd H. Harder, lawyer, member of the Executive Committee of BITKOM e. V.
- 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
- Silke Stokar von Neuforn, Member of the German Parliament, retired
- Dr. Peter Wedde, Professor of Labor Law and Law in the Information Society at the University of Applied Sciences, Frankfurt a.M.

Perspectives from the Data Privacy Advisory Board.

Questions
directed to Peter Franck,
Chaos Computer Club (CCC)

Why are you, a hacker and member of the Chaos Computer Club, working on the Data Privacy Advisory Board of Deutsche Telekom?
At the end of 2008, I was invited by Deutsche Telekom to participate in the Data Privacy Advisory Board. The decision to participate was not easy for me to make. Ultimately, for me the opportunity to play a role in shaping the largest German network operator to the benefit of netizens was greater than the risk to possibly serve as a “fig leaf”.

What can a company like Deutsche Telekom learn from the Chaos Computer Club?
As a hacker, one has a completely different view of networks and systems. I can bring this view to the Data Privacy Advisory Board. I hope that Deutsche Telekom will internalize the open communications culture created by the Internet and participate in discussions about the future in more ways than just through press releases and product demonstrations. This has been a matter of course all along for the Chaos Computer Club, for example.

Experts from business, law and associations are opening up new perspectives. Deutsche Telekom has therefore placed its trust in an independent advisory committee on the subject of data privacy since early 2009. Change of perspective guaranteed.

The Data Privacy Advisory Board has established itself as an important advisory council for Deutsche Telekom in issues related to data privacy and data security. It naturally cannot and should not examine all Group processes related to data privacy. Nevertheless, last year it dealt with a wide range of processes.

It worked on reorganizing Group Security and realigning data privacy. It also discussed topics being discussed in public such as data protection in indirect sales and employee data privacy. It discussed the effectiveness of measures taken by Deutsche Telekom with respect to improving the level of data privacy, for instance, the principle of dual control when external investigation service providers are commissioned, Group-wide blocking of certain service providers and dealing with requests from authorities for data. In addition, it grapples with data retention and data privacy aspects of T-Home Entertain.

The results of the consultations range from simple acknowledgement without further recommendations to a request for a more detailed description of issues that have arisen to specific process recommendations. The latter were accepted and implemented by Deutsche Telekom.

The establishment of the Data Privacy Advisory Board has proven to be an effective measure for further improving data privacy in the Group. Deutsche Telekom is expecting the Advisory Board to make vital contributions related to data privacy in 2010 as well.

Perspectives from the Data Privacy Advisory Board.

Questions

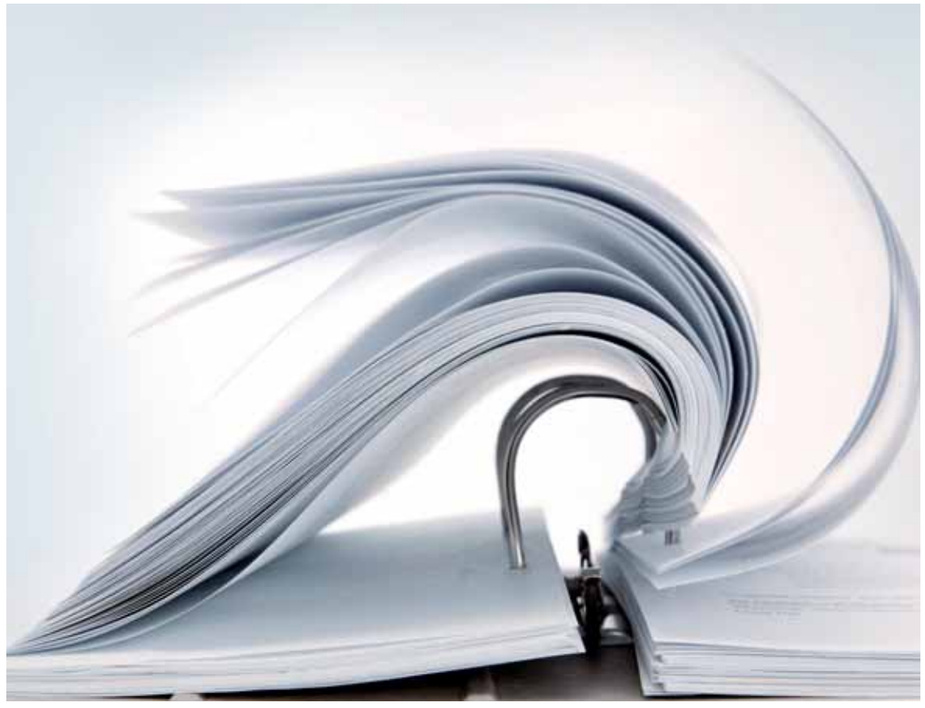
directed to Lothar Schröder,
Chairman of the Data Privacy Advisory Board, member of the ver.di National Executive Board and Deputy Chairman of the Supervisory Board of Deutsche Telekom AG

Why did you decide to become a member of the Data Privacy Advisory Board of Deutsche Telekom?
At first I was furious and distanced from the company, because irresponsible persons tarnished the business foundation of the company and intruded into my personal rights in the spying affair. But then I became convinced that it's necessary to support the actions to clear up the affair, especially because tens of thousands of people at the company do a good job every day with respect to data privacy and one must not allow the impudent behavior of a few to hurt everyone. Via the Deutsche Telekom Supervisory Board, I recommended to the Board of Management that it establish a Data Privacy Advisory Board to open itself up to recommendations from critical experts. The Board of Management followed this recommendation. After I learned about the misuse of my telephone data from sources within the company and from the public prosecutor's office, it was a matter of course for me to play a role on the Data Privacy Advisory Board, also because I myself used to do research related to data privacy.

What do you think were the most important topics that the Data Privacy Advisory Board dealt with in 2009?
We first discussed our business foundation and clarified that we also want to take up certain topics ourselves. The spying affair repeatedly appeared on the agenda. We dealt with the recommendations from the report of the Oppenhoff law office, which was in charge of an independent investigation of the spying affair, and supported many steps to improve the data privacy organization in the Deutsche Telekom Group.

What topics will be discussed by the Data Privacy Advisory Board in 2010?
The follow-up work to the Schäfer report will keep us busy. The former Presiding Judge at the Federal Court of Justice (BGH) dealt extensively with the entire data privacy organization in the Group. We have placed data privacy in the Entertain package on the political agenda and, among other things, we again want deal with the controlled access of service providers to the customer data of Deutsche Telekom. We hope to present a record of our work so far to the public in the middle of the year. We plan to critically evaluate our own work near the end of the year.

In your opinion, when will the work of the Data Privacy Advisory Board be completed?
When we have made ourselves expendable and the standard of data protection in the Group is so high that there is no longer a need for external critical reflection. I would be happy to achieve this goal, but it would surprise me if we were able to reach it soon in view of the rapid advance of technology and the ongoing changes in requirements regarding data privacy.



The establishment of the Data Privacy Advisory Board has proven to be an effective measure for further improving data privacy in the Group. Deutsche Telekom is expecting the Advisory Board to make vital contributions related to data privacy in 2010 as well.

Technical development is always a challenge with data privacy: employees need to be up-to-the-minute on the latest trends. At the same time, they need to be sensitized to handle data properly and with due care. Deutsche Telekom will continue working on the best solutions in the future.

Summary and outlook.

Summary and outlook by Dr. Claus Dieter Ulmer.

As was the case in 2008, the year 2009 was characterized by numerous operational and strategic measures that were taken to further reinforce data privacy in the Deutsche Telekom Group. All initiated measures have already been completed or have been continued systematically. In view of the organizational and technical developments in the Group and in the information and telecommunications industry, though, the number of operational tasks is not declining.

In 2009 as well, we recognized the continued development and strengthening of sensitivity in dealing with data privacy issues, both among our employees and in public. A high level of sensitivity to data privacy makes it easier to communicate the legal data privacy requirements and ensures their implementation. The establishment of the department for Data Privacy, Legal Affairs and Compliance has boosted the Group executives' heightened awareness of data privacy issues already described multiple times. The collaboration among the departments combined under the Board of Management department has also led to a much greater level of integration of data privacy into Group operations than before.

In spite of everything, we must not let up in our efforts to strengthen the cultural change that has already begun. That's why further awareness-raising campaigns are essential at all levels in addition to the necessary technical and organizational measures. To complement the variety of tools already implemented in the training and information area, we have planned to establish a Group-wide "Welcome Day" in 2010 for all new employees to our company. At this event, new employees will have the opportunity at the start of their employment relationship to familiarize themselves with the legal data privacy requirements and their implementation at Deutsche Telekom. For its part, the data privacy organization has the opportunity to make its approaches and plans transparent and to communicate its organization and contacts.

Data privacy is a hot topic not only in Germany. The new business models, such as cloud computing in particular, involve international data transfer in the medium term. In cloud computing, users no longer rely on their own computers at home and the programs installed on them. Rather, they use central network services to use any necessary applications and storage capacities. The advantages are that they always have access to the most recent versions of programs and they are protected by the latest security solutions. For the companies providing the services, though, this means developing new concepts for handling their customers' data confidentially. For the companies that want to process the customer data at various data centers around the world in the future, according to the totally understandable principle of "wherever there's room", this means they must develop and implement completely new framework conditions for the international arena. The companies' data privacy organizations must do the preparatory conceptual work in due time. The greatest possible level of protection for customer data should be ensured from day one of such a model.

In this context, I would like to refer to the "Delphi Study 2030 [1)]". In late 2009, the study stimulated a broad discussion about opportunities and risks of the information and knowledge society. Around 550 ICT experts from politics, business and academia were surveyed on significant developments in their sectors for the next twenty years. The study illuminates the perpetual dynamism with which information and communication technologies change the world in which we live today. Some of the core messages of the study on the future are:

1. Digitalisation and the still increasing penetration of ICT into all areas of professional and private life will be even more all-embracing in molding the information society in the future.
2. People's acceptance and trust in using ICT are the foundation for developing a modern, open information society.
3. The mobile use of the Internet and its services will have a lasting impact on the information society and create independent new areas of application.

These core messages make the importance of data protection to future developments clear.

[1)] http://www.tns-infratest.com/presse/zukunft_Informationstechnologie.asp

Data privacy will remain a priority, both in public and here at Deutsche Telekom. Deutsche Telekom's data privacy organization is standing by to advise and support this matter that is so important for the future. In the spirit of the general principle "Creating areas of trust!"

In as little as six to ten years, tools and connected digital assistants that allow people to use their digital data in all kinds of usage contexts and enable them to manage their (multiple) identities on the Internet will be widespread in Germany and throughout Europe within the scope of the cloud computing mentioned above. We have recently had a first taste of these possibilities with so-called apps, which can be loaded onto mobile devices. Each of these applications processes personal data to a greater or lesser extent.

Especially against this background, users' complete control over the use of their personal data remains a primary goal that, as it now stands, will be achieved only with considerable effort. Neither have the key issues in dealing with the digital identity of a person been resolved worldwide, nor do the involved companies or countries have a coordinated approach for dealing with them.

Programs that facilitate access to data stored on the network over long periods of time and provide data are also an ongoing problem. The availability of information for documentation purposes is only one aspect thereof. The other is the question of how users can remove content referring to them from the network. Placing digital documents on the network with a digital expiration date, that is, providing them with a planned date and time for deletion, are just one possible solution.

All in all, these issues can yield significant business opportunities, but also risks for the information technology industry. However, the latter must be solved, and these solutions must be implemented internationally. What's also needed above all is suitable IT security measures. By this I mean secure e-signatures, secure e-mail communication, the safeguarding of digital identities and an identity management solution that's reliable and easy to use for everyone. Only in this way can secure and reliable digital communication between people and also increasingly between people and machines be ensured over the long term and the trust of users be earned. Of course, the companies cannot make these efforts alone. In particular, socially relevant institutions must help support and promote the global creation of recognized standards.

In addition to these future-oriented issues, operational issues will continue to keep us busy in 2010 and beyond. Supporting the wide variety of projects and individual measures initiated following the data incidents will continue to play an important role. First of all, Deutsche Telekom Group Privacy will create new comprehensive regulations for the customer contact departments, meaning sales, customer service and technical services, to safeguard the appropriate handling of our customers' data even better. We will support the measures regarding audits of sales partners and play an even greater part in the development processes for IT systems together with our colleagues from data security. We will provide intensive support on data protection issues to a Group-wide project that has originated from the Compliance department and focuses on consumer protection.

In the area of employee data privacy, we will provide advice on the new legal requirements we expect in 2010, work through them and initiate their implementation in the Group. The objective in this case is also to derive regulations that are as uniform as possible for the entire Group from the individual sets of regulation of the various companies.

Last but not least, the tedious, extremely time-consuming process of converting the Group IT infrastructure and the communications networks to the next generation is ahead of us. In this area as well, in 2010 we expect the first substantial conversions requiring our support.

This means data privacy will remain a priority, both in public and here at the company. The data privacy organization of Deutsche Telekom is standing by to advise and support this matter that is so important for the future. In the spirit of the general principle

"Creating areas of trust!"

Deutsche Telekom Group Privacy is firmly resolved to strengthening and steadily improving the confidence that our customers, the public and our employees have placed in us.

A well-functioning data privacy system requires a well-functioning organization. Deutsche Telekom is constantly enhancing its data privacy area. Strictly formulated guidelines give employees guidance on handling data.

Annex.

Annex 1
Organization of Group Privacy.

Group Privacy, under the management of the Group Data Privacy Officer, provides the national companies with direct support on data privacy issues and works towards establishing an appropriate level of data privacy throughout the Deutsche Telekom Group. The Group Data 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. Following the data privacy incidents, a further department (Privacy Audit and Technical Know-How Management) was established, which is currently still in the implementation phase.

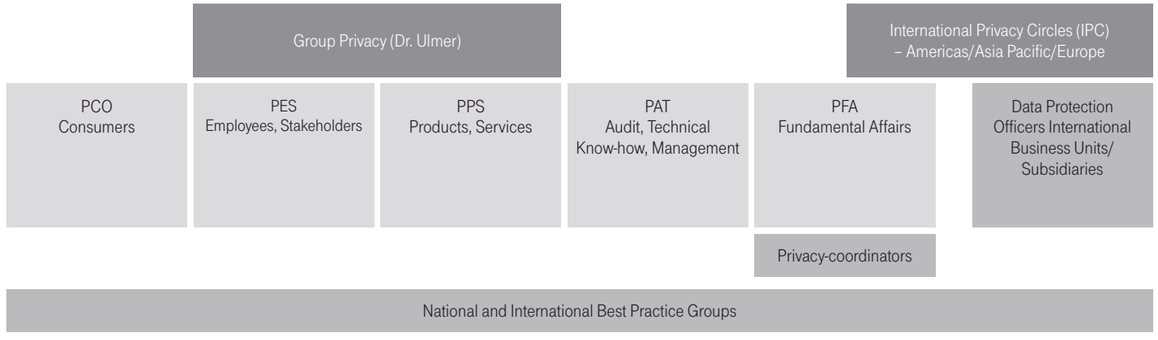
Data privacy interfaces and data privacy coordinators are installed as on-site data privacy contacts for legal entities, departments and other organizational units. At international shareholdings, this function is assumed by data protection officers appointed for this purpose. Both data privacy coordinators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

2. Privacy Consumers.
The Privacy Consumers department advises and supports the Group and its strategic business areas on consumer 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.

The data privacy organization.



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

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

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

The Privacy Code of Conduct, which sets out Group-wide regulations on data privacy, is the central basis for processing customer and employee data at Deutsche Telekom nationally and internationally.

Annex 2
Framework conditions for our actions.

Legal framework conditions.
The German Federal Data Protection Act (BDSG) and relevant industry-specific regulations in the area of communications are the starting point and regulatory basis for all of Group Privacy's activities. The latter includes in particular the German Telecommunications Act (TKG) and the German Telemedia Act (TMG). At a European level, the Group's actions are governed primarily by the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, the data protection directive for electronic communications.

Based on these legal requirements, additional framework regulations, policies and guidelines tailored to the specific data processing conditions and work processes at Deutsche Telekom were issued or integrated in key processes by Group Privacy. This chapter only looks, however, at the overarching framework regulations in place in the Group.

Group-wide framework regulation.
The Privacy Code of Conduct, which sets out Group-wide regulations on data privacy, is the central basis for processing customer and employee data at Deutsche Telekom nationally and internationally.

On the basis of European legal provisions and the requirements of the German Federal Data Protection Act, the Deutsche Telekom Group introduced its Privacy Code of Conduct (PCoC) in 2004 as an internal data privacy regulation in the Group. The Privacy Code of Conduct governs worldwide internal requirements concerning personal data consistently. The companies within the Deutsche Telekom Group that are bound by instructions are obligated by the underlying Board of Management resolution to introduce the Privacy Code of Conduct and make it binding. All other companies are advised to introduce and implement it. The Privacy Code of Conduct forms the legal prerequisite for international exchanges of personal data within the Group to the extent that such exchanges go beyond the borders of the European Union. It includes the requirements under European law for protection of personal data. All other specific internal provisions through to the Employee Data Privacy Handbook are derived from the Privacy Code of Conduct.

The Privacy Code of Conduct, which sets out Group-wide regulations on data privacy, is the central basis for processing customer and employee data at Deutsche Telekom nationally and internationally.

Annex 3
Privacy Code of Conduct Deutsche Telekom AG.

Code of Conduct
for the Protection of the Individual's Right to Privacy
in the Handling of Personal Data within the Deutsche Telekom Group

Preamble and Recitals

(1) Due to increasing networking of information and communications systems, the protection of personal data of customers, sales partners, employees and shareholders is a significant concern of all companies in the Deutsche Telekom Group worldwide.
(2) The most important target of this Code of Conduct, therefore, is to create a uniform and high level of data protection in the Deutsche Telekom Group worldwide. In particular, in the case of transnational data flows it must be guaranteed that personal data is processed by the recipient according to the principles of data protection law that apply for the sender of such data.
(3) Deutsche Telekom Group companies are aware that the success of Deutsche Telekom as a whole is dependent not only on global networking of information flows, but also above all on trustworthy and safe handling of personal data.
(4) In many areas, the Deutsche Telekom Group is perceived by its customers as a single entity. Therefore it is the common concern of Deutsche Telekom Group companies to make an important contribution to the joint success of the company and to support the claim of the Deutsche Telekom Group of being a provider of high quality products and services by implementing this Code of Conduct.

Part One
Scope and Application

§ 1 Legal Nature of the Code of Conduct
This Code of Conduct is a Directive, which is binding for the entire Deutsche Telekom Group and comes into effect upon adoption and publication by the respective company management. It applies to the handling of all the personal data of natural persons, in particular the data of customers, shareholders, employees and other third parties, contracting parties or business partners.

§ 2 Legal Provisions to be Applied
(1) The principles set out below are intended to guarantee a uniformly high level of data protection throughout the entire Deutsche Telekom Group. However, they do not replace the required – and where necessary, statutory – conditions that must exist to legitimize the handling of personal data. Any obligations and regulations applying to individual companies on the processing and use of personal data which go beyond the following principles, or which contain additional limits on processing and use of personal data, shall remain unaffected by this Code of Conduct. Irrespective of the foregoing, the companies agree that laws applying for individual companies shall not prevent these companies from fulfilling their obligations under this Code of Conduct.
(2) Data collected in Europe must be processed according to the legal provisions of the country in which the data was collected, even in the event of transmission abroad.
(3) The collection of personal data and its transmission to public bodies shall – unless within the framework of a normal customer contractual relationship – be done in accordance with the obligatory legal provisions of the country.
(4) This Code of Conduct shall be governed by the law of the Federal Republic of Germany.

§ 3 Termination
The expiry or termination of the Code of Conduct – irrespective of the time, circumstances and reasons – shall not release the companies from the obligations and/or provisions of this Code of Conduct regarding the processing of data already transmitted.

Part Two
Principles

Article 1
Transparency of Data Processing

§ 4 Duty to Inform
The data subjects must be given easy access to information about the appropriate handling of their personal data, for example by publishing privacy policy and this Code of Conduct on the Internet.

§ 5 Content and Form of Information
(1) The data subjects shall be adequately informed about the following:

a) The identity of the data controller(s) and their contact details.
b) The intended scope and purpose of the collection, processing and/or use of personal data. This information should include which data are being recorded and/or processed/used, why and for what purpose and for how long.
c) If personal data are transmitted to third parties, the recipient, extent and purpose(s) of such transmission.
d) The manner of data processing and/or use, especially if it is to be processed or used in another country.
e) Their legal rights (see Article 7).

(2) Irrespective of the chosen medium, data subjects should be given this information in a clear and easily understandable manner.

§ 6 Availability of Information
The information shall be available to data subjects when the data are first collected and, subsequently, whenever it is requested.

§ 7 Consent
(1) Unless the collection, processing or use of the data is required for purposes of initiating or fulfilling a contract or unless there is some other statutory authorization, the consent of the data subject shall be obtained at the latest when data starts to be collected, processed or used.

(2) In addition to the obligations to inform as set out above, the following shall be observed with regard to consent:

a) Content Consent must be given expressly, it must be voluntary and it must be on an informed basis that points out to the data subject, in particular, the scope of what he/she is consenting to and also the consequences of non-consent. The wording of declarations of consent shall be sufficiently precise and shall inform data subjects of their right to withdraw their consent at any time.
b) Form Consent shall be obtained in a form appropriate to the circumstances (normally in writing or electronically). In exceptional cases it can be obtained verbally, if the fact of the consent and the special circumstances that make verbal consent seem adequate are sufficiently documented.

Article 2
Use for Specific Purpose

§ 8 Principle
Personal data shall not be used for purposes other than those for which the data was originally collected.

§ 9 Prohibition of Tying-in
The use of services, or the receipt of products and/or services, shall not be made conditional on data subjects consenting to the use of their data for purposes other than the initiation or fulfillment of a contract. This shall only apply if it is not possible or not possible within reason for the data subject to use comparable services or comparable products.

Article 3
Special Data Processing Cases

§ 10 Direct Marketing
(1) Data subjects shall be informed that they may, at any time, object to their personal data being used for direct marketing purposes. Furthermore, they shall be made aware of the nature, content and period within which their data may be used for direct marketing purposes.
(2) Data subjects shall be informed about their right to object whenever they receive direct marketing communications. Furthermore, data subjects shall receive appropriate tools for exercising their right not to receive such communications. They shall receive, in particular, information about the body to whom the objection is to be made.
(3) Special legal provisions pursuant to sentence 2 of § 2 (1) of this Code of Conduct, which make the use of personal data dependent on the consent of the data subject, shall take precedence over other provisions.

§ 11 Automated Individual Decisions
(1) Decisions which evaluate individual aspects of a person and which may entail legal consequences for them, or which may have a considerable adverse effect on them, shall not be based exclusively on automated processing. This includes in particular decisions for which data about the creditworthiness, professional suitability or state of health of the data subject is significant.
(2) If, in individual cases, there is an objective need to make automated decisions, the data subject shall be informed without delay of the result of the automated decision, and shall be given an opportunity to comment within an appropriate period of time. The data subject's comments shall be suitably considered before a final decision is taken.

§ 12 Special Categories of Personal Data
(1) The handling of special categories of personal data shall be subject to express, legal authorization or to the data subject's prior consent. It shall also be permissible if it is necessary to process the data in order to fulfill the rights and obligations of the responsible body in the area of labor law, provided that this is permissible due to national law that provides for adequate guarantees.
(2) Prior to the commencement of such collection, processing or use, the data protection department of the company in question shall be properly consulted, in writing, of all cases where this is necessary. Due consideration should be given to the nature, extent, purpose, necessity and legal basis of using the data .

Article 4
Data Quality, Data Economy and Data Avoidance

§ 13 Data Quality
(1) Personal data shall at all times be correct and, where necessary, kept up do date (data quality).
(2) In light of the purpose(s) for which the data are being collected, processed or used, appropriate measures shall be taken to ensure that any incorrect or incomplete information is erased or, if necessary, corrected.

§ 14 Data Economy, Data Avoidance, Anonymization and Pseudonymization
(1) Personal data shall be appropriate, relevant and not excessive with regard to the use of the data for a specific purpose (data economy). Data shall only be processed within a certain application when it is necessary (data avoidance).
(2) Where possible and economically reasonable, procedures shall be used to erase the identification features of data subjects (anonymization) or to replace the identification features with other characteristics (pseudonymization). Anonymization and pseudonymization shall be carried out in such a manner that the original identities of the data subjects cannot be revealed, or can only be revealed with disproportionately great effort.

§ 15 Profiling, Statistical Analyses
(1) Organizational and technical measures consistent with the appropriate state-of-the-art concepts or technology shall be used to ensure that profiling (e.g. movement profiles, user profiles, consumption profiles) is not allowed unless by express legal permission or the data subject's prior consent.
(2) Purely statistical analyses or studies on the basis of anonymized or pseudonymized data remains unaffected in this regard.

§ 16 Data Archiving
The principles of data processing, particularly the principles of data economy and data avoidance, shall be taken into account when developing data archiving rules. Personal data must not be archived without the express consent of the data subject, unless where necessary for operational reasons or required by law.

Article 5
Restriction on Further Transmission

§ 17 Transmission of Data to Third Parties
(1) The transmission of personal data to a third party shall require a legal basis. This may arise because it is necessary to fulfill a contractual requirement towards the data subject or because the data subject has provided their consent.
(2) Paragraph 1 does not apply if national restrictions, in particular for reasons of security of the state, national defense, public safety or the prevention, investigation, detection and prosecution of criminal acts exist which require the transmission of personal data for these purposes.

§ 18 Responsibility
(1) When transmitting data to third parties that are not public bodies, the company that originally collected the data shall ensure that it is being processed or used lawfully. Accordingly, prior to the transmission of the data, appropriate data protection and data security measures shall be discussed and agreed with the recipient. Where agreements are concluded with bodies in countries without adequate data protection levels, sufficient guarantees must be ensured with respect to the protection of the right to privacy of the individual and the exercising of rights connected with this.
(2) In accordance with generally accepted standards, appropriate technical and organizational measures shall be taken to ensure the integrity and security of data during its transmission to a third party.

§ 19 Subcontracted Data Processing
(1) When a company engages the services of a subcontractor, then, in addition to a service agreement comprising the work to be performed, the contract shall also refer to the obligations of the subcontractor as the party engaged for processing the data. These obligations will set out the instructions of the company (the data controlling unit) concerning the type and manner of the processing of the personal data, the purpose of processing and the technical and organizational measures required for data protection. Sentence 3 of § 18 (1) of this Code of Conduct applies accordingly.
(2) The subcontractor shall not use the personal data for its own or third-party processing purposes without the prior consent of the data controlling unit. In the case of the latter, the above-stated rules shall also be agreed with such subcontractor(s).
(3) Subcontractors shall be selected according to their ability to fulfill the above-stated requirements.

Article 6
Data Protection, Organization and Data Security

§ 20 Data Protection Officers
(1) Each company shall appoint a data protection officer, whose task is to ensure that the individual departments are advised on the statutory and/or Group-internal requirements and on data protection and privacy policy.
(2) The data protection officer must be involved in the design of new products and services from the early stages to ensure that they are in harmony with the principles that are set out in this Code.

§ 21 Checks on the Level of Data Protection
Checks on the level of data protection (e.g. by data protection audits) should be carried out at regular intervals to review the effectiveness and success of the technical and organizational data protection measures implemented. Such audits may be carried out internally by the data protection officer or other organizational units which have been awarded an audit assignment or, alternatively, by an independent external third party approved by the data controlling unit. The basis for establishing the level of data protection shall be the legal and corporate policy requirements that apply for the respective organizational unit as well as the requirements of this Code of Conduct.

§ 22 Technical, Organizational and Employee-Related Measures
Appropriate confidentiality undertakings shall be agreed in writing with employees when commencing their work within the company. In addition, appropriate technical and organizational measures for handling personal data shall be established for the company processes and Information Technology systems.

Such measures shall include

a) preventing unauthorized persons from gaining access to data processing systems on which personal data are processed or used **(physical access control);**
b) ensuring that data processing systems cannot be used by unauthorized persons **(denial-of-use control);**
c) ensuring that those persons authorized to use a data processing system are able to access exclusively those data to which they have authorized access and that personal data cannot, during processing or use or after recording, be read, copied, altered or removed by unauthorized persons **(data access control);**
d) ensuring that, in the course of electronic transmission or during their transport or recording on data carrier, personal data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to examine and establish where personal data are to be transmitted by data transmission equipment **(data transmission control);**
e) ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, altered or removed **(data entry control);**
f) ensuring that personal data which are processed by subcontractors can only be processed in conformance with the instructions of the ordering party **(subcontractor control);**
g) ensuring that personal data are protected against accidental destruction or loss **(availability control);**
h) guaranteeing that data which have been collected for different purposes can be processed separately **(separation rule).**

Article 7
Rights of Data Subjects

§ 23 Right to Question and Complain
Every data subject has the right at any time to contact the data protection department of the responsible company with questions and complaints regarding the application of this Code of Conduct. If not subsequently specified otherwise, for the purpose of these provisions, the responsible company shall be any company that has a contract relationship with the data subject or that processes the data subject's personal data. The company that the data subject has contacted shall make sure that the data subject's rights are properly observed by the other responsible companies.

§ 24 Right to Information
(1) Every data subject may at any time request information from the responsible company concerning:

a) the personal data recorded on them, including its origin and recipient(s);
b) the purpose of the processing or use;
c) the people and units to whom/which their data are regularly transmitted, particularly if the data are transmitted abroad;
d) the provisions of this Code of Conduct.

(2) The relevant information should be made available to the enquirer in an understandable form within a reasonable period of time. This should generally be done in writing or electronically.
(3) Where permissible under the relevant national law, a company may charge a fee for supplying the relevant information.

§ 25 Right of Protest/Right to Have Data Erased/Blocked
(1) The data subject concerned can protest to the responsible company against the use of his/her data, if he/she has the right to do so.
(2) This right to protest shall also apply in the event that the data subject had previously consented to the use of his/her data.
(3) Rightful requests to have data erased or blocked shall be promptly met. Such requests are rightful particularly when the legal basis for the use of the data ceases to apply. If a data subject has the right to have data erased, but erasing the data is not possible or not possible with reasonable effort, the data shall be protected against non-permitted usage by blocking. Statutory retention periods shall be observed.

§ 26 Right to Correction
The data subject may at any time request that the responsible company corrects the personal data recorded on them insofar as such data are incomplete and/or incorrect.

§ 27 Right to Clarification and Comments
(1) If a data subject claims that his/her rights have been breached in the form of unlawful data processing, particularly in the event that this Code of Conduct has been breached, the responsible companies shall clarify the facts without culpable delay. In this case they shall work together closely and grant each other access to all information necessary for establishing the facts of the case.
(2) The company's responsible data protection department most closely associated with the relevant issues must coordinate all the relevant correspondence with the data subject.

§ 28 Exercising of Rights of Data Subjects
Data subjects shall not be disadvantaged because they have availed themselves of these rights. The form of communication with the data subject – e.g. by telephone, electronically or in writing – should respect the request of the data subject, where appropriate.

Article 8
Data Protection Process Management/Responsibilities

§ 29 Responsibility for Data Processing
(1) The companies shall, in their capacity as Data Controllers, be obliged, particularly vis-à-vis data subjects, to guarantee compliance with the requirements of data protection and with the provisions of this Code of Conduct.
(2) The data protection officer of the respective company shall be informed without delay about any breaches (including suspicion of a breach) of data protection provisions and of this Code of Conduct. In the case of incidents that are of relevance to more than one company, the central Group Privacy Department should also be informed. The company's data protection officer shall also inform the Group Privacy Department if any changes are made to the laws applying for a company that are significantly unfavorable.
(3) The data protection departments of the individual companies shall coordinate their activities within the framework of the Group's data protection policy. Accordingly, they should mutually support each other and make use of existing synergies.

§ 30 Coordination by the Group Privacy Officer
(1) The Group Privacy Officer shall coordinate the processes of cooperation and agreement in all significant issues regarding data protection. The Deutsche Telekom Group Coordination Committee on data protection shall serve as the coordinating body.
(2) It shall be the duty of the Group Privacy Officer to develop and evolve the Group's policy on data protection. Also in this regard, the data protection departments of the companies shall engage in coordination.

§ 31 Supervisory and Consultation Duties
(1) The data protection officers of the respective companies shall be responsible for monitoring compliance with national and international data protection regulations and with this Code of Conduct. In this regard, all departments of the respective companies shall be obliged to inform the relevant data protection officer of appropriate developments and future plans.
(2) In the absence of legal restraints, the respective data protection officers shall be authorized to examine on-site all processing techniques that involve the use of personal data.
(3) Where appropriate, and within the framework of their examination duties, the data protection units of the companies shall use mechanisms which are identical throughout the Group, e.g. in the form of common data protection audits.

§ 32 Employee Training and Commitment
(1) The employees of the companies shall be sufficiently trained with regard to the data protection regulations and application of this Code of Conduct.
(2) The companies shall, with the participation of the competent data protection departments, devise suitable training materials.

§ 33 Cooperation with Supervisory Authorities
(1) The companies shall agree to respond to enquiries by the supervisory authority responsible for them or if applicable for the company exporting the data within a reasonable period of time and to a reasonable extent and to follow the supervisory authority's recommendations.
(2) In the event of a change in the legislation applicable to a company which might have substantial adverse effect on the guarantees provided by this Code of Conduct the relevant company will notify the change to the relevant supervisory authority.

Article 9
Terms and Definitions

Automated individual decisions
Shall mean decisions which produce legal effects for the data subject or which significantly affect him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Company
Shall mean any company that has agreed to be bound by this Code of Conduct and that is listed in Annex A hereto.

Data controller
Shall mean the company which alone or jointly with others determines the purposes and means of the processing of personal data.

Data subject
Shall mean any natural person whose personal data is handled in the Deutsche Telekom Group.

Data processor
Shall mean any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller (subcontracting data processing).

Deutsche Telekom Group
Shall mean Deutsche Telekom AG and all companies in which Deutsche Telekom AG directly or indirectly holds more than a 50 % share, or over which it has control.

Handling of personal data
Shall mean any operation or set of operations which is performed upon personal data such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This also includes the processing of personal data in structured manual files.

Personal data
Shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Recipient
Shall mean any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not. However, public authorities that may receive data as part of a single inquiry shall not be considered to be recipients.

Special categories of data
Shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life.

Third party
Shall mean any person or body outside the data controller. Third parties shall not mean the data subject or persons or bodies who by order collect, process or use personal data in Germany, in another member state of the European Union or in another state party of the agreement on the European Economic Area.

Glossary.

Audit. Audits are examination and review procedures that assess whether and to what extent requirements and guidelines have been met. Specially trained auditors carry out the audits.

Awareness. As it relates to data protection, awareness signifies the sense of responsibility the employees of a company have in dealing with data.

Certification. Procedure that is used to verify compliance with certain standards for products or services and their respective manufacturing processes.

Cloud computing. In cloud computing, data is no longer processed and services are no longer performed on the users' computers, but via a network service which the users can access from their respective terminals, including mobile devices. The applications and data are no longer located on the user's local computer or in the company's data center, but in the (figurative) cloud.

Company-level controls (CLCs). Company level controls are Group-wide test criteria and audits that are derived from the U.S. Sarbanes-Oxley Act (S-OX) and the German Accounting Law Modernization Act (BilMoG).

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

Computer Emergency Response Team (CERT). A team established to handle computer security incidents and emergencies.

e-learning. All forms of learning in which electronic or digital media are used to present and distribute learning materials or to support interpersonal communication.

Federal Data Protection Act (BDSG – Bundesdatenschutzgesetz). 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 are processed in IT systems or manually. It was last amended in 2009.

German Accounting Law Modernization Act (BiLMoG – Bilanzrechtsmodernisierungsgesetz). The Accounting Law Modernization Act is a German law passed to reform accounting law.

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

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

Location-based service (LBS). Location-based services provide users location-specific information via a mobile device.

Nearshore. From a central European perspective, the relocation of processes and functions of a company to eastern European countries.

Offshore. From a central European perspective, the relocation of processes and functions of a company to foreign countries (overseas).

Outbound call center. An outbound call center creates active market contacts, meaning it calls people. One example is direct marketing. In contrast, an inbound call center operates passively, meaning it receives calls from people. One example is an advice hotline.

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 uniformly governs the internal requirements regarding the handling of personal data in the Deutsche Telekom Group.

Radio frequency identification (RFID). Radio frequency identification offers the possibility to read and store data via electromagnetic waves.

Sarbanes-Oxley Act (S-OX). The Sarbanes-Oxley Act is a U.S. law passed in response to accounting scandals and is intended to improve the reliability of corporate reporting. The aim of the Act is to restore investor confidence in the accuracy and reliability of companies' published financial data. The Act applies to U.S. and foreign firms whose securities are traded on U.S. stock exchanges and to their subsidiaries.

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

Publication information.

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

www.telekom.com

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

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

Photographs:
Deutsche Telekom AG
plainpicture

Translation:
Corporate Language Management DTAG

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

Printing:
Broermann Offset-Druck GmbH, Troisdorf-Spich

KNr. 642 100 129 (German)
KNr. 642 100 135 (English)

Contact.

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

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

www.telekom.com