DATA PRIVACY IN THE DIGITAL WORLD

The digitization of our society continues apace. Millions of machines are networked with each other and huge quantities of data are being processed. All of which gives rise to questions about our data protection standards, which traditionally tend to be high in Europe. How can we transfer these standards to a digital age? Is it enough to comply with laws or do we need rules which go beyond these in order to gain people's trust? Digital responsibility lies at the heart of all these issues. A responsibility which Deutsche Telekom also assumes, especially when it comes to data privacy.

The digital future.

In the digital world, new business models are generating more and more personal data and processing that data in disparate ways. The individual struggles to comprehend the complexity of the data flows. This trend is set to accelerate further over the next few years as devices and everyday objects are increasingly networked. Virtually every aspect of our lives will be affected. Whether it is shopping or at the doctor's office, at work or leisure: Data is being collected, networked and correlated everywhere.

Many people are worried about this development. Skepticism of new digital business models is rife. These business models in particular depend on customer trust and ultimately acceptance in society. Some people would even like to see us stop processing data altogether in order to allay these fears. But that is not an approach our society can embrace as it moves into the future. Today we have no alternative to data processing. Virtually all existing and upcoming business models are based on processing data and the associated information. Our society would grind to a halt without data processing. So we need to find ways and solutions that inspire people's trust in digital business models and bolster that trust long term. So while we do need data processing, it also needs to be compatible with data privacy. Because it is clear that if people do not trust us to use their data, then it is not only the economy that stands to lose out. Developments that are essential to society, such as in the medical field, would also be permanently jeopardized as a result.

The digital future and Deutsche Telekom.

Deutsche Telekom assumes responsibility for consistently fostering people's trust in data processing. This is the only way that digital business/processing models can be successfully further developed for the good of society and the individual.

The individual's digital sovereignty takes center stage. This autonomy is guaranteed through a high degree of transparency, decision-making freedom and the development of data privacy-friendly solutions. To this end, data privacy experts need to be involved from the start in the development of new products and services that process personal data.

The leading trend and future development gurus predict that the digital future cannot develop successfully without taking account of people's concerns. The futurist Matthias Horx talks about the megatrend of "mindfulness" for the next five to ten years and predicts a "rehumanization" of the Internet.

Deutsche Telekom is adapting early on to current and upcoming developments with its data protection solutions. For instance, we are the first company to set out principles for big data solutions and the Internet of Things.

But interaction with society is crucial here. No company, no institution and no legislator alone can provide answers to the questions surrounding digitization. That is why Deutsche Telekom is promoting a wide-ranging debate about the issues of digitization and has turned the issue of digital responsibility into its main theme.

www.telekom.com/digital-responsibility

Deutsche Telekom is already assuming its responsibility.

Our customers and shareholders, the regulatory authorities and the general public rightly expect that we handle the data entrusted to us by our business partners, customers and employees with the appropriate care. And we make every effort not just to satisfy these expectations, but to inspire yet more trust in our dependability. Data privacy is for us more than just a responsibility; we consider it a concern of particular importance to us.

By guaranteeing a high level of data privacy we are living up to our digital responsibility. A high level of data privacy does not simply mean setting requirements that are as high as possible. Rather, a high level of data protection means embracing data privacy in the business and integrating it into all operational areas.

This is the only way of achieving the best results for the business and for people.
Our data protection core principles determine how we act – day in, day out, product by product. So our customers can rely on us to deliver on the following:

More responsibility
We accept responsibility for how we handle our customers' data – wherever we operate – and have created, among other things, a uniform international framework for this in the shape of our Binding Corporate Rules Privacy. These define the purposes for which personal data may be collected, stored and processed. We endeavor to clarify any unresolved questions or issues without delay. We set ourselves principles early on for new business models, which make it clear to our customers, employees and business partners how we deal with these models and leave them in no doubt that we assume responsibility.

Greater commitment
Data protection is given top priority at Deutsche Telekom. We are the first company listed on the German stock exchange to create a separate Board of Management department devoted to this issue. Dr. Thomas Kremer is the Member of the Board of Management for Data Privacy, Legal Affairs and Compliance. As the Global Data Privacy Officer, Dr. Claus-Dieter Ulmer, together with his team is responsible for the Group's data protection requirements and for making sure that they are complied with. The team directly supports all Deutsche Telekom units in data protection matters. This applies to the fundamental orientation of our Group in data protection issues as much as it does to the development of new business models and to the development of data protection awareness among our employees.

Greater transparency
We speak openly about the aspects of data protection that are important to us: about potential solutions and our vision for the future, but equally about what is not functioning as we would like it to. We inform customers and interested partners simply and clearly about how we handle their data with our data protection information and principles on new business models. In response to our customers' questions and problems we provide rapid, direct assistance, whether over the phone, via e-mail or through social media.

More trust in products and services
We implement data privacy from the foundations up (following a "privacy by design" approach), whether we are working on our products, services or features. Our data privacy organization is directly involved in all the Group's centralized and decentralized development processes, supporting new solutions through the unit's

comprehensive expertise. “Privacy by design” is thus a practice that we live daily in the Group by deploying what we call our “Privacy and Security Assessment process.” We continue to develop data protection in line with customer, employee and market needs. That creates trust and makes our products more attractive to customers.

More tailored solutions

Data processing is becoming ever more important. New business models based on the smart processing of large data volumes are having a positive impact on our society. Such models involve, for instance, adapting production processes to actual demand and regulating traffic flows intelligently. Simply refraining from processing data is not a viable response to this trend. We prefer to rely on tailored solutions. When developing new business models and products, we gather only the data that is absolutely essential, and take every technical and organizational precaution to protect that data as well as ensuring transparency vis-à-vis the customer.

More digital sovereignty

We consider the digital sovereignty of every citizen to be crucial. This means customers must be able to understand easily what their data is being used for so that they can make an informed choice whether to accept that use or not. Beyond that, digital business models require effective anonymization and pseudonymization methods to ensure that individuals are not identifiable without their consent.

Closer to new developments

Group Privacy at Deutsche Telekom discusses the new trends thoroughly with the Group’s innovation units, the Telekom Laboratories and the Hochschule für Telekommunikation in Leipzig. The aim is to offer groundbreaking solutions to the business and people early on. We continually adapt our consulting, support and testing processes to actual, technical and process developments (design thinking, agile development processes).

Our Group has achieved a standard in data protection and security that cannot be taken for granted in the business community. Deutsche Telekom has become the benchmark against which other companies compare themselves in many areas. In addition to this, our data privacy management system has been certified by a team of independent auditors.

www.telekom.com/privacy

Deutsche Telekom will continue to be actively involved in the discussion in society as it has done in the past and, among other things, push forward the development toward more customer-oriented data privacy with simple, reliable solutions.

Can Deutsche Telekom change the world?

Deutsche Telekom sees itself as a pioneer when it comes to data privacy and the assumption of its responsibility. Data privacy is, however, not an issue that can be guaranteed solely by a single group in society or an institution.

Everyone involved has to assume their part of the responsibility.

Legislator and government: Government must ensure a suitable, balanced framework is put in place which underpins a data protection culture in society. Relevant laws need to be drafted that are essentially technology-neutral. It is not about regulating individual industries or practices. Rather as a society we need clear guidelines on how to handle data. Under these guidelines it must still be possible to develop new applications and technologies. The promotion of data privacy-friendly processing models can help reconcile business interests with the basic right to data protection. In addition to statutory provisions, government is also responsible for providing its citizens with educational opportunities so they can learn how to use technologies and their own data – and ideally start this learning process from a very early age. Syllabuses for schools and training institutions need to be urgently revised so we have enough time to prepare tomorrow's generation of leaders for future requirements.

Industry and commerce: Industry and commerce must ensure that the data privacy guidelines are implemented in a trustworthy way in their sphere of influence. Treating people with respect must not be compromised. The providers and users of data-based services are ultimately responsible for fostering the trust of their customers and their employees. This includes voluntarily bolstering the data subjects' digital sovereignty. In this way, people must be able to find out quickly and simply which of their data has been recorded and processed. New, simpler ways must be found for deleting data. Only if people trust businesses, they will continue to allow their data to be processed. Companies in their capacity as "trusted companions" must ensure that the rights of customers and employees are not undermined with increasing networking and, in turn, increasing complexity. This concerns contractual arrangements with partners and the exploitation of existing data down the line. People must always be able to identify and get in touch easily with the relevant managers and contacts.

The person as individual: In our capacity as customer, company employee or user of digital business models we must all ultimately play our part through our own responsibility and our responsibility to our fellow human beings. This is not limited to granting or revoking consent, but also includes social interaction in particular. Customers and users also need to systematically avoid providers that recklessly use the valuable personal data entrusted to them or make such practices transparent for others.

Data privacy "only in Europe"?

Data privacy cannot be just a "European solution" either. To meet the need to network the digital world, data protection must be developed and embraced internationally, on the basis of jointly accepted standards. Many countries around the world, be it in the Asia-Pacific region, in Central and South America or in Africa have now realized that "digital" is not feasible without rules. Even in the United States, surveys conducted by the National Telecommunications and Information Administration (NTIA) now show that citizens have concerns about the unregulated development of digital business models. These citizens tend to use the Internet less. Standards, which have to be developed jointly and internationally, help in this respect. If these come from industry, they are likely to be successful provided they suitably balance the own interests with the interests of the data subjects and, in turn, foster the necessary trust in standards.

The future of data privacy.

Data privacy does not stand still. Its structure therefore needs to be constantly developed even if the legal framework remains unchanged. Three factors will essentially be decisive for this development:

Simple.

Data privacy requires pragmatic solutions that are easy to understand. Standardized regulations are an important starting point in this respect. We now need to ensure that the interpretation and implementation of regulations is also geared to the principle of uniform, understandable standards. This applies, for instance, to the issues of customer information and system documentation, as well as to the development of certification mechanisms or pseudonymization solutions.

Customer-focused.

Data privacy must be geared to the needs of the people whose data is being processed. So we need to ask: How can we best ensure in a world of increasing digital networking the self-determination right regarding information, in other words people's digital sovereignty? How can consent models be structured sensibly? How can data processing be conveyed in a more transparent, more understandable way? Do we need to rethink consent models? The decision whether to use data ultimately rests with the data subject. We must therefore ensure that the consent mechanisms are geared to people's real-life needs and data usage, and not to purely technical aspects.

Balanced.

Data privacy must be balanced and in proportion to the other justified needs of society and holders of basic rights. Data privacy itself will not survive long term without protecting society against crime. The digital world has become too multilayered for it to continue to regulate itself. Provided strict checks and balances are applied, it must be acceptable to limit people's self-determination right regarding information in the interests of prosecuting criminal offences. We also need to clarify whether and to what extent companies acquire rights to the results of processed information. These and other general requirements must be negotiated between the various stakeholders in a democratic society.

Implementation paths - examples.

Data privacy information and icons.

Easy-to-understand data privacy information and icons are a first step in the right direction. To exercise their digital sovereignty, people need brief, clear and understandable information about how their data will be processed.

This can be done using a "one pager" – data-privacy information on a single page – and with icons.

Icons in particular - i.e. readily understandable visual symbols - should help people understand quickly how their data will be processed. One example is the familiar video surveillance pictogram. If indoor tracking is used to record the time customers spend and the route they take in a department store, customers informed by an icon in the entrance area can take action as soon as they enter the store - say by disabling their device or the relevant functions (such as Wi-Fi); or they willingly accept the offer and allow the system to

navigate them through the department store. Icons can therefore also make the long overdue **connection between the analog and digital world**.

Privacy apps.

Privacy apps, such as the Deutsche Telekom Privacy App governing the level of protection provided by the individual data privacy settings on Facebook, will soon be an important companion on the way to greater digital autonomy for the individual. Over the long term the aim is to merge these approaches to create a uniform solution that encompasses multiple services wherever possible.

Data dashboards and data cockpits.

Individual companies will take another step by providing the technical means so their customers and employees can access data relating to the specific individual above and beyond general information. This can be done using **data dashboards or data cockpits** in which the information is summarized on a single portal. A further expansion stage will allow the data subject to make changes to their data. These changes will be directly reflected in the company's systems.

Privacy bots.

When using digital services, the customer does not want to worry about every little detail, but wants to store their wishes and have these fulfilled. With the aid of **digital butlers or robots (privacy bots)** this will also apply in future to the customer's self-determination right.

Using the privacy bots the customer will store their needs and the bot will query these requirements for the customer and, where necessary, negotiate or apply them directly. The customer will also be able to set whether they are asked for their preferences each time a contract is concluded or a service used, or only where variances occur. In this way, the customer should be able to define, for instance, whether an opt-out is sufficient for them where data is transferred from the responsible entity to international service providers. If the data is transferred to third parties for profile creation purposes – whether in Europe or abroad – the customer can save the need for an opt-in. This function can and should take place on a cross-service basis.

On a smartphone, for instance, both for the operating system and the used apps.
If the customer wants to book a trip to a certain place and to find a hotel and a restaurant there at the same time, services for booking, means of transport, hotel search and

restaurant search are then activated. Plus a route planner, where necessary, to navigate their way from the hotel to the restaurant. For all these services, the data privacy profile of the person making the booking can be negotiated directly or integrated by the privacy bot as part of the booking.

Anonymization and pseudonymization solutions.

In the case of **mass data processing** it will be very difficult in future to receive reliable and hence usable results simply with consent-based solutions. **Anonymization and pseudonymization solutions** and transparency become all the more important where a company needs to process personal data. Transparency is the only way of guaranteeing that people will also trust the digital models of the future.

Encryption (homomorphic encryption).

Over the long term data will be transferred and stored in encrypted format, even though the content can still be processed (known as homomorphic encryption). Homomorphic encryption processes mean that encrypted data can be sent to a service provider. The data is **processed** there **in an encrypted state** and the (also encrypted) results sent back. Information no longer needs to be decrypted or re-encrypted to process the data. Only the user that originally encrypted the data knows the initial value and will have the result in plaintext. These solutions may lead, say in the area of **cloud computing**, to a substantial **increase in the level of security** over the next few years. The storage location of the data would then no longer be as relevant as it is today. However, homomorphic encryption processes still require further development before using them in live operations. The required computing capacity is still considerable. As such, practical solutions will only be feasible over the longer term.

What remains?

Hitherto the providers of services and products have had an advantage over the user because they are responsible for designing a solution. Given an increasingly complex digital world and the lack of standards, the result is a lack of clarity for the data subjects. As a result, they may potentially become weary of or reluctant to embrace digital business models over the long term. So providers must give people solutions where they once again see themselves as a partner in a fruitful relationship for both sides. Only with this partnership of equals will the digital world be a good and thus desirable world for all those involved over the long term.