DEUTSCHE TELEKOM GROUP PRIVACY ACTIVITY REPORT 2017 FOR THE GROUP BOARD OF MANAGEMENT

Deutsche Telekom AG

Version 1.0, March 23rd 2018

ERLEBEN, WAS VERBINDET.

CONTENTS

FOREWORD BY THE GLOBAL DATA PRIVACY OFFICER 3

2. DEVELOPMENT OF DATA-PRIVACY LEGAL FRAMEWORK 5

3. IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR) 6

4. CONSULTING HIGHLIGHTS 7

4.1 CUSTOMER DATA PRIVACY 7

4.2 EMPLOYEE DATA PRIVACY 8

4.3 DATA PRIVACY SOLUTIONS FOR THE ICT INFRASTRUCTURE AND FOR PRODUCTS AND SERVICES FOR MAJOR BUSINESS CUSTOMERS 11

4.4 PRIVACY INSPECTIONS 14

5. RECORD OF PROCESSING ACTIVITIES 14

6. IN-HOUSE DEVELOPMENT OF AN INTERNATIONALLY USABLE PSEUDONYMIZATION AND ANONYMIZATION SOLUTION 15

7. GROUP DATA PRIVACY AUDIT 15

8. GLOSSARY AND ABBREVIATIONS 17

FOREWORD BY THE GLOBAL DATA PRIVACY OFFICER

Data privacy creates value for companies. So, it becomes much more than simply fulfilling statutory requirements. An embraced data privacy culture rather underpins trusting cooperation between companies on the one hand, and customers and employees on the other. Our aspiration is to be the leading telecommunications company, and also to be the brand and the company which customers trust most.
Besides the best infrastructure, suitable rate plans and very latest devices, data privacy is therefore a key aspect of our success. Together with security, data privacy ensures, on the one hand, the technical protection of our customers' and employees' data. On the other, however, it also makes sure that customer and employee data in the company is handled carefully and conscientiously. Data privacy has an external and internal impact.

"THINK FROM THE CUSTOMER'S PERSPECTIVE"

How does the Deutsche Telekom data-privacy organization contribute to the Group's success?
The data-privacy organization is the sparring partner for the operating units. By involving the data-privacy organization early in the company's planning, it ensures that the idea of Privacy by Design is considered from the start, and the solutions ultimately represent a balanced result, which meets customer and employee needs, as well as the company's operating requirements.

One example: In the digital world, an enterprise needs high-quality information about its customers so it can offer them suitable products and services. Attractive products and services are the key to business success. Yet where does a business obtain the necessary information?
Possibly by purchasing data from social networks, from credit card companies or from online retailers. All of which seems to be a simple way of doing it. Yet Deutsche Telekom does not use these solutions. Why not?
When purchasing data, you naturally have to ask yourself from a data-privacy perspective whether the data was collected lawfully and can be passed on lawfully. But that is not all.
There is then also the question of whether the data, which is analyzed without the customer's express consent, can provide a suitable basis at all from a quality perspective for designing new products and services. This is something the data-privacy organization looks at when it shares information with the operating units in the Group. Looking outside the box and retaining an overview is what it is all about:
In every social context, online individuals may assume a different identity. So, companies struggle to draw the right conclusions from data obtained "surreptitiously." In my role as customer, I would say that tracking mechanisms and big data analytics have not yet provided me with a single offering that gives me what I want. Why? Because every online aspect covers only a part of my personality, and the whole of my personality is more than the sum of its parts. And not to mention that many users despair about having their activities monitored all the time and so lay false trails. By streaming music, they do not actually like, buying certain products offline, not using their reward cards, simply not posting certain things, etc., etc., etc. ...
The analysis systems still cannot work out an individual's personality from relevant information. If, say, I stream a whodunit movie, that does not necessarily mean I dislike romances or biographies. Analysis systems, artificial intelligence (AI) included, can – at least today – only work with what is there and do what they were programmed or trained to do.
So ideally, high-quality data for successful business models comes from customers themselves. And customers will provide the company with this high-quality data of their own accord if they can trust the company to handle this data properly in their interests. Deutsche Telekom's data-privacy organization helps promote this trust.

Looking into the future also forms part of the data-privacy organization's remit. Back in 2016, we provided an outlook of upcoming developments with our White Paper "Data Privacy in the Digital World." In 2017, we set up a competition aimed at generating ideas for a privacy bot and received lots of interesting entries. The best five participants presented their solution to an international jury in Berlin and received their prizes.

We are also setting up collaboration projects to further develop data privacy, such as the Privacy Guard project where we are helping develop a data-privacy scanner. This scanner should provide customers with a quick, clear insight into how an application processes their data, and show them what decision-making leeway they have based on this – promoting digital sovereignty at the same time.
This solution means one day customers will no longer have to read pages of data-privacy information. Rather the data-privacy scanner will provide them with the key information so they can then decide what configuration they prefer. Over time the data-privacy scanner will also learn via AI to take into account the customer's personal preferences.

We have also accompanied and will accompany other groundbreaking ideas. These include the data cockpit, which will offer our customers a standardized user interface to manage their data simply. The Privacy Exchange solution has not quite got that far, but is equally promising. It provides cross-enterprise and cross-industry transparent data sharing. Naturally based on customer consent.
The Deutsche Telekom data-privacy organization ensures that all these solutions are implemented for the benefit of the company and for the benefit of our customers. For stable systems, and for transparency as well as choice for customers.

This report covers the essential aspects we focused on in 2017. But one thing is for certain: 2017 was more than just the year of the General Data Protection Regulation.

Kind regards,

CD Ulmer

2. DEVELOPMENT OF DATA-PRIVACY LEGAL FRAMEWORK

The General Data Protection Regulation (GDPR) will come into effect on May 25, 2018. The GDPR will introduce standard data-privacy requirements in the European Union (EU), which will emphasize the implementation responsibility of enterprises. With a few exceptions, this will not entail any new basic requirements for our Group, since we have already rolled out certain procedures over the past few years, which are now being introduced as generally binding through the GDPR. These include the Privacy & Security Assessment process (PSA) which already meets the data-protection impact assessment required under the GDPR for assessing and documenting risks associated with IT systems.
But we have also taken the new regulation as an opportunity to implement the existing data-privacy tools, such as the PSA process, in a far more standardized and sustainable manner throughout Europe. As such, we are increasing the internal and external transparency and efficiency of our solutions. Generally binding processes and tools will also promote international collaboration and the acceptance of data privacy in the Group.

The GDPR is a milestone on the way to a genuine European single market in which the same rules apply to all participants, and products and solutions can be scaled more effectively. The new regulations ensure a high level of data privacy in Europe, while also paving the way for new digital business models. This fulfills Deutsche Telekom's basic demand for a level playing field for all market participants in the EU. The new data privacy legislation also closes a regulatory gap in relation to providers that offer their products and services in the EU from outside the EU. The GDPR will also apply in future to non-European market participants (e.g. Google, Facebook or Apple), thus rounding off the level playing field – standard legislation applies not only to European enterprises; it also applies to the region of Europe.
To preserve the level playing field achieved with the General Data Protection Regulation, the EU member states, within the framework of their remaining legislative leeway, must only make national special arrangements regarding the General Data Protection Regulation where such arrangements are necessary. With the revision of the new Federal Data Protection Act (*Bundesdatenschutzgesetz – BDSG new*) which comes into effect on May 25, 2018, the German legislator has addressed some of the criticisms leveled at the initial drafts, and reduced the special arrangements for the non-public sector. Now the other EU states must adhere to the "imperative of regulatory economy." Some initial laws are a step in the right direction.
But, unfortunately, the approach to designing a level playing field has not been not adopted systematically. Sector-specific special arrangements still apply without any plausible reason. The regulations for telecommunications providers are subject, for instance, to separate, more stringent regulation, i.e. the e-Privacy Regulation and the relevant implementation laws. No substantial improvement is likely either from the current revision of the telecommunications regulations. Under the existing regulatory drafts, the competitive disadvantage for telecommunications providers in Europe remains in sub segments. Including the over-the-top service providers (such as WhatsApp and Skype) in future is only part of the solution. Compared with the General Data Protection Regulation, telecommunications providers face much tighter constraints on processing data. As a result, the telecommunications sector will have fewer opportunities to exploit big data applications than other sectors of the economy. After all, metadata can only be processed with the customer's consent under the current draft of the planned e-Privacy Regulation. Unlike in the General Data Protection Regulation, data cannot be further processed using pseudonyms for compatible purposes. As such, various service models, which the user could find useful, but which are not feasible with anonymous data, cannot be offered: These may include products for looking for a parking space, accident prevention services, on-demand TV programming or telemonitoring services in the health care segment.
Against this backdrop, Group Privacy together with Group Public & Regulatory Affairs promoted in 2017 the idea of regulation that is balanced across all sectors. These activities will continue in 2018. The aim is to provide business models that will allow Deutsche Telekom to utilize its high level of expertise in technical solutions.

3. IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Group Privacy has set up a pan-European steering project that will control and monitor the implementation of the requirements from the GDPR in the Group. Through the uniform enterprise-wide approach we can also help ensure that the new requirements are interpreted uniformly and correctly, and are implemented uniformly.
In this respect, we also had to analyze the current situation of the companies to determine the implementation status of existing data privacy requirements. The additional implementation requirements identified as a result were incorporated into the overall project.
Relevant subprojects were set up in the Group companies to ensure the required adjustments were made in each company. All IT systems and processes were verified in this way, shortcomings were prioritized individually and eliminated. The overall project has been up and running since the enactment of the GDPR in 2016. It will be finalized as part of the "GDPR Readiness Check" due to be completed this year on the cutoff date of May 25, 2018.

The project is divided up specifically into three phases:

- In the first phase, we developed a binding internal interpretation of the GDPR's substantial implications. The GDPR contains a number of rules that are open to interpretation, and that we thus had to clarify for our own purposes. We provided this clarification with input from our Data Privacy Advisory Council. This clarification process produced binding interpretations for the whole Group. We have published this information on our website https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection under "More Transparency."
- In phase two, we divided up responsibilities to implement the binding interpretations operationally. This entailed defining specific requirements, communicating those requirements to our various departments, and, of course, finally implementing those requirements within our systems and processes. For example, we had to make editorial adjustments to various parts of our data privacy information, i.e. the information we provide in the form of notices, at Telekom Deutschland. Group Privacy as the governance unit made the editorial adjustments, while the operating companies, accompanied by Group Privacy, were responsible for implementation.
- Phase 3 involves completing the Readiness Checks for control purposes in 2018. At the same time, Group Audit also verifies the implementation.

Special structural adjustments were and are not required as part of the GDPR, since we could already use as our base the existing data privacy governance structures and a Privacy and Security Assessment process (PSA), which has been established and further developed for many years, as a privacy impact assessment. During the project, it, however, turned out that the large number of systems and areas of action (e.g. data privacy information) pose a challenge. These had to be examined to establish where adjustments were necessary. Any necessary adjustments were then made. To do this, the Group had to provide far more HR and financial resources than originally expected.

4. CONSULTING HIGHLIGHTS

4.1 CUSTOMER DATA PRIVACY

Transparency took center stage in 2017. Easily accessible information that everyone can understand forms the basis for data privacy at Deutsche Telekom. Our customers should be able to find out at any time to what extent their data is processed whenever they use Deutsche Telekom services and products. For this we are on hand personally for our customers; Group Privacy answered directly or in writing more than 13,500 customer inquiries relating to data privacy in 2017. We also developed new easier-to-understand texts which describe data processing clearly. Under the heading "Your data at Deutsche Telekom" you can find out what we mean by "Personal data," "Phone usage data" or "Location data." The texts are available on the website www.telekom.com and on www.telekom.de, under "Data Transparency." Together with the privacy information developed with customers, these texts supplement the more detailed, product-specific data privacy information that is included via links.

FURTHER INFORMATION ON DATA PRIVACY ON OUR WEBSITE

This year we developed further information for and together with our customers on our website https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection.
Here you will find a detailed description of how we protect our customers' data and tips on what customers can do themselves to protect their data. We focused particularly on the issue of anonymization and pseudonymization. Wherever we require customer data, but a reference to an individual is not necessary or not necessary directly, we protect the customer data, e.g. through anonymization and pseudonymization. Two easily understandable videos on our website also explain what that means exactly and how it works.

To improve transparency of our internal processes, we provided online training on the GDPR. This was developed in-house specifically for our employees worldwide and is freely available on our website. The training course can be found under "More Responsibility."

We have also published the key internal data-privacy regulations, along with details of the political positioning papers relating to data privacy that we have incorporated into the political debate. These are also available on our website under "More Transparency."

We understand security and data privacy as a design criterion for all our products and services. To this end we developed in 2009 the PSA process which we used to conduct a special risk assessment with a focus on customer and employee data. Based on this analysis, targeted measures to protect data are defined and incorporated into the products from the outset. We further developed this process over the years and once again modified it specifically to the requirements of the General Data Protection Regulation in 2017. More information on the PSA process is also available on the website https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection.

INFORMATION FOR THE PROCUREMENT PROCESS

Deutsche Telekom does not rely just on customers reading the data privacy information. The customer is also informed when purchasing a product if the required product has specific requirements associated with data processing. This applies whenever Deutsche Telekom has to pass on data to another service provider so the service can be provided. This is the case when incorporating the Amazon Alexa voice control function with Magenta Smart Home. Here Amazon needs customer data to make the service work. After all, Amazon is ultimately the operator of the offered solution. Before the customer contracts the product, their attention is clearly drawn to this process.
The same applies to booking the StreamOn add-on option. Here we point out separately that the customer's data traffic is verified to ensure the service runs smoothly.

INTERNATIONALE FUNKAUSSTELLUNG

The international trade fair "Internationale Funkausstellung" (IFA) 2017 demonstrated that customers like the new data privacy information. Deutsche Telekom Data Privacy had a booth at the IFA to listen to customers' views and advise them on data privacy issues. In addition to texts, the prototype of a data privacy app was also presented, the Data privacy scanner. The Data privacy scanner app informs consumers how other apps handle their personal data. The Data privacy scanner also points out adjustments that can be made to tailor the way apps process data based on the user's own privacy preferences. This should help consumers exercise their right to decide how their personal data is used. The app is being developed as part of a research project, which is funded by the Federal Ministry of Education and Research *(Bundesministerium für Bildung und Forschung – BMBF)* within the publication "Self-determined and secure in the digital world." The partners mediaTest digital, InfAI e.V., Quadriga Hochschule Berlin and SRIW e.V. make up the research consortium. Deutsche Telekom supports new consumer-friendly data privacy solutions such as the Data privacy scanner and presented the app at the IFA.

Data privacy also plays a major role with another app, namely the games app Sea Hero Quest. Deutsche Telekom is supporting international research into dementia with Sea Hero Quest. The mobile game provided a huge amount of diagnostic data for research within a matter of months. Group Privacy supported implementation of the project, ensuring that only anonymous data is used. Users get a simple explanation of how the game data on the user's navigation behavior and orientation skills help with scientific research.

COOPERATION WITH SUPERVISORY AUTHORITIES

Various authorities supervise data privacy at Deutsche Telekom, making cooperation between Group Privacy and these authorities crucial. Besides the Federal Network Agency *(Bundesnetzagentur – BNetzA)*, the German Federal Commissioner for Data Protection and Freedom of Information *(Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – BfDI)* is responsible for Deutsche Telekom, while the various country data privacy officers are responsible for the telemedia services and employee data privacy. Last year a series of topics were discussed with the individual authorities and some of these are mentioned below.

The Motionlogic service, which the Deutsche Telekom subsidiary Motionlogic GmbH offers, receives anonymized traffic data from Telekom Deutschland GmbH mobile communications customers in order to provide traffic volume analysis. Once the BfDI deemed the anonymization process to be viable, the Berlin Commissioner for Data Protection and Freedom of Information got involved in 2017 on behalf of a major Berlin-based customer that wanted to use the service. As part of this involvement, the issues surrounding the anonymization process are once again being discussed. The discussions will presumably be completed in early 2018.

BfDI and Federal Network Agency have asked Deutsche Telekom for their opinion on a SAP system in which the erasure periods were implemented incorrectly. This is a SAP platform with various finance and logistics modules. All modules process a huge number of data records. The platform also forms part of an interactive network with other systems. This means that the erasure process must be preceded by complex check mechanisms to maintain the integrity of the data that is still held. As part of a large project the erasure function is now being established after Deutsche Telekom submitted the planned procedure to the BfDI and the latter deemed this procedure to be plausible.

As part of another consulting and inspection visit, Deutsche Telekom presented to the BfDI the data processing with Wi-Fi hotspots. The visit involved the Deutsche Telekom hotspots and the hotspot functions where Deutsche Telekom acts as a wholesale provider (e.g. with McDonalds). The BfDI suggested improvements to the data privacy information, but found the data processing to be sufficiently economical and correct overall.

4.2 EMPLOYEE DATA PRIVACY

With employee data privacy, the key topics related to consulting and the support of internal organizational issues, the use of digital services by employees, and measures relating to the training and awareness of data privacy legislation.

INTERNAL ORGANIZATION

Deutsche Telekom operates in a dynamic market environment and constantly faces challenges which also require restructuring and reorganization measures in the Group.
Group Privacy has therefore created the data privacy requirement *Data privacy measures in organizational projects*. The requirement is designed as a guide for simplified, structured handling of organizational changes. The document examines various reorganizational measures and defines requirements that must be met. Implementation suggestions are basically made for the fulfillment of the requirements. These are specifically described technical and organizational solutions for fulfilling the requirements.

At the initiative of Group Privacy, the management self-service for managers was further developed. The SAP HR tool provides Deutsche Telekom managers with a management self-service function. Here they can complete those management tasks that can be mapped in the IT systems. In the "Data privacy-compliant migrations" project a solution was devised and implemented which allows managers to consult their employees' data in compliance with data privacy regulations. This provides more efficient use of the management self-service under the need-to-know principle enshrined in data privacy law.

DIGITAL SERVICES

As part of their day-to-day work our employees have a number of communication tools for disparate applications. Employees are already familiar with and use these tools privately. As such, the business use of freely available communications tools greatly simplifies matters.

Group Privacy realizes that a different approach is needed when using new and external digital services. In the past, employees were not allowed to use external communications tools that were not approved for business communications. The company provided communication tools at work that were verified beforehand with regard to data privacy. With increasing digitalization, this "all-round carefree approach" had to be reconsidered. The company data privacy organizations cannot thoroughly verify all the available digital services that may be useful for specific areas.
Completely banning these services seems inappropriate though if the practical benefits clearly do not pose any relevant risks. At the same time, employees involved closely with the rapid changes associated with digitalization require leeway for making their own decisions based on opportunities and threats.
To facilitate the sensible use of freely available tools, the comprehensive ban was therefore lifted. Instead, the Group relies more on the employees' own responsibility.
To support our employees, we developed rules which provide clear guidelines of what is allowed and what not. In this way, only certain specially protected and verified tools may still be used for highly confidential information and personal customer data. The decision should, however, largely rest with the employee when it comes to internal information only.
Nobody should be forced to use these kinds of digital services. The "basic provision" of work communications tools will continue for all employees (e-mail, internal social network *you and me*, mobile and location-based telephony offerings, collaboration platforms such as Sharepoint, etc.).

TRAINING AND AWARENESS

Every two years, all Group employees receive training on the statutory and Group-internal provisions of data privacy and information protection, and are obliged to comply with data and telecommunications secrecy. A regular renewal of the commitment in conjunction with training or awareness measures ensures that all Deutsche Telekom employees are permanently obliged to comply with data privacy provisions. The training involves an online course. Successful participation in a training course is audit-proof documented. The training is also available via our websites (see above under Customer data privacy).
In 2017, the commitment course focused on the new General Data Protection Regulation, which is due to come into effect in May 2018. The training concept has a practical focus: participants accompanied the fictional character Tom, a Deutsche Telekom employee, throughout the day. For instance, on the way to

work, taking part in a meeting, and during the lunch break. Each situation includes a specific topic relating to data privacy law.
One of the key tasks of the data privacy officer is to familiarize employees with the provisions governing data privacy law and the specific requirements of data privacy. Group Privacy therefore creates training courses on various data privacy topics, which employees can complete on their own on the intranet. Group Privacy also offers classroom-based training on basic and topical issues.
Besides these courses, colleagues from Group Privacy have also been lecturing for several semesters on a series of bachelor's and master's degree courses at the Leipzig University of Applied Sciences (HfTL). Their involvement includes lectures and teletutorials in data privacy law as well as also supervising bachelor's dissertations in individual cases. While these lectures are held as part of the "IT law" module on the business Information Systems or ICT courses of study, there is also a separate certificate program "Data Protection and Security in Information Systems" in the master's degree courses at the HfTL. Starting from the summer semester 2017, Deutsche Telekom employees could attend these lectures as part of a certificate program. These courses are aimed at experts with existing master's or diploma qualifications, who are working, for instance, in developing products and processes and want to hone their skills with in-depth data protection expertise. Participants that have completed all modules in the certificate program and at least have a "University of Applied Sciences" degree, can obtain a master's degree as an additional academic qualification by submitting a master's thesis. In cooperation with the Chair of "Data Protection and Security in Information Systems," Prof. Dr. Erik Buchmann, Group Privacy designed the legal modules for this certificate program and ran the relevant lectures at the HfTL. The certificate program will also be continued over the coming semesters.

4.3 DATA PRIVACY SOLUTIONS FOR THE ICT INFRASTRUCTURE AND FOR PRODUCTS AND SERVICES FOR MAJOR BUSINESS CUSTOMERS

DATA-DRIVEN BUSINESS MODELS

Data privacy is no obstacle to the successful marketing of data-based business models; on the contrary, the competent use of data privacy-compliant solutions gives customers confidence, as a key prerequisite for the successful marketing of data-driven business models.

We consider aspects of data privacy law in conjunction with business models that use analysis techniques, existing data and/or freely available data and/or purchased data to add value and create new knowledge. Marketing this newly created knowledge is the basis for our business models.
Topics such as the Internet of Things (IoT) and automation play a pivotal role here, because they create mass data. Big data technologies, modern data analysis techniques and artificial intelligence for evaluating, interpreting and refining data are the principal tools used in data-driven business models.
Big data analyses draw data from a wide range of sources. Much of this data touches on the personal sphere and allows a wide range of conclusions to be drawn, both directly and indirectly, about the circumstances and behavior of data subjects. The key is to strike the right balance between the interests of individuals in protecting their personal data, and the interests of companies or authorities in using new analysis techniques. This presupposes that companies and authorities operate transparently and in compliance with data privacy regulations.
On the one hand, Deutsche Telekom uses big data itself, e.g. to organize its processes more efficiently and optimize its customer service. On the other, it is keen to offer its customers products and services using its own data or customers' data for big data analyses. Whether used internally or for external marketing it is important to strike the permissible balance between protecting privacy and using the opportunities afforded by big data.
Group Privacy has been involved closely with the requirements of the legally compliant design of data-driven business models as part of a project and exchanged ideas with the responsible business areas as part of workshops and discussions. As a result, Group Privacy presented a White Paper on the data privacy-compliant design of data-driven business models in late 2017.
This internal paper consists of an extensive legal appraisal, highlights specific design approaches and thus provides sustainable guidance for the Group's business units on how to develop current and future business models. Deutsche Telekom's positioning is clear in this respect: maximum transparency for our customers through Privacy by Design.

DATA PRIVACY-COMPLIANT USE OF CUSTOMER DATA FOR TROUBLESHOOTING

Deutsche Telekom increasingly uses big data technologies to determine the likelihood of its network components failing, and to support troubleshooting. These initiatives aim to provide greater availability of network and other services, as well as reducing faults in the entire communications infrastructure. To ensure data-privacy conformity of these kinds of analyses, the individual measures were coordinated closely with Group Privacy.
Basically, the analyses tend to involve assessing technical parameters of products and of the individual components in the local loop. This kind of data is not associated with any given individual and is assessed in accordance with certain fault patterns to enable conclusions to be drawn on the infrastructure vitality; this data can, however, not provide any statement on the failure probability or fault in the customer-related portion of the local loop.
Customer traffic and usage data is accessed solely on the basis of § 100 German Telecommunications Act (*Telekommunikationsgesetz – TKG*) to eliminate errors and faults, taking into account the current version of the draft Regulation on Privacy and Electronic Communications (Art. 6 (1b)).
The first step involves verifying whether the purpose behind processing this data complies with the legal provisions and the data is used to eliminate errors and faults. The second step involves providing an analysis based on pseudonymized data, or where specific faults reported by customers exist, based on plain data. Big data analyses are therefore completed in this context with

- Technical parameters without any association with a given individual,
- Anonymized data, or
- Pseudonymized data, or
- Plain data (where specific customer-related faults exist)

We are currently working on a solution to re-identify pseudonymized data at the end of the analysis process, say if a specific fault pattern points to the failure of a component in the customer-related portion of the local loop. In this respect, however, certain legal issues are still under discussion and, in particular, this procedure will need to be coordinated with the responsible supervisory authority.

OPEN TELEKOM CLOUD (OTC)

In 2016 and 2017, Group Privacy was involved decisively in designing and developing cloud solutions in line with data privacy law. A cloud solution was developed, the Open Telekom Cloud, which stores, processes and administers personal data solely within the European Union. No maintenance or support access to the Open Telekom Cloud comes from third countries outside the European Union. As such, the Open Telekom Cloud constitutes an affordable alternative to classic IT outsourcing for customers that do not want foreign security authorities to have the option of accessing their data. The business model was coordinated from the outset with Group Privacy. Group Privacy verified all partner contracts, the customer-related contracts, and terms and conditions of business in respect of data privacy law. The technical implementation of the business model was supervised as part of the PSA process.
In addition, Group Privacy supported Deutsche Telekom in its plan to actively become a data trustee for another large cloud provider.

PAN-NET

Pan-Net is an innovative, brand-new pan-European production and business model for the telecommunications company of the future. Services, products and data are no longer provided on individual platforms in each individual national company. They are bundled Europe-wide in an agile, standardized infrastructure cloud, which is distributed across a handful of data centers in Europe. The production is moving from traditional hardware platforms to a virtual environment, which is based on the very latest IP, software-defined network and virtualization technologies. Pan-Net units set up specially for the purpose operate the pan-European network. Deutsche Telekom Pan-Net s.r.o. Bratislava (Slovakia) pushes forward the business transformation, while Group Privacy provides intensive data privacy law support as part of a key account.
The Pan-Net international business and production model is unrivaled to date and highly demanding in relation to data privacy law. The data privacy officers in the participating Deutsche Telekom national companies audited and assessed the complex technical and legal issues associated with the business model and the future technical production platform (data centers, Operations/DevOps). This involved assessing different statutory legal norms, scrutinizing and harmonizing national requirements from 13 countries, and implementing these uniformly in the production and business model.

Pan-Net Privacy Governance was developed and established, and new data privacy law provisions (processes) drawn up. The Privacy Governance includes a Privacy Contractual Framework, which regulates the contractual bases of the business model and is based on the specimen contracts developed specially for Pan-Net. These take into account all national regulations of the participating national companies.

To ensure the data privacy requirements are met in the technical production platform, the PSA process is used for all parts of the infrastructure and for services in the agile development environment. The level of complexity increases here considerably, since, in addition to the existing high Deutsche Telekom standards, the national requirements must also be implemented technically.
With regard to the applicability of the GDPR in May 2018, a great deal of work was done in 2017 on the GDPR Readiness of the Pan-Net.

PROCESSING HEALTH DATA

The processing of personal health data must be deemed critical from a data privacy law perspective as it tends to involve highly sensitive data. Very close cooperation exists between the business unit Deutsche Telekom Healthcare and Security Solutions, which develops and operates relevant business models, and Group Privacy to ensure the data privacy conformity of all business activities.

Partnerships between health care institutions and T-Systems International and its associated subsidiary Deutsche Telekom Healthcare and Security Solutions (DTHS) are the preferred business model for operating relevant platforms to process health data securely.

Besides operating centralized platforms, the provision of integrated IT-based communication between the players in the respective health region is a key element of business operations. The aim is to leverage our offering of intensive business model consulting to map the increasingly interdisciplinary approach to patient care and specialization on the part of the care provider at a maximum data privacy law level through secure platforms and communication solutions.

Data privacy does not always meet the requisitioners' wishes. Group Privacy prescribes, for instance, the sole use of selected and adequately secure device hardware whenever the doctor's offices access the centralized platforms. The use of the physician's own, uncontrolled hardware constitutes an extremely high security risk from the perspective of data privacy and security. This is why approaches which include this hardware in the data processing are not approved. The incorporation of a Gematik-certified telematics infrastructure into the solution concepts is always verified.

This systematic approach is maintained not only with our cooperation partners. It also plays an important role in the political debate. Compelling data privacy and security concepts help solution providers gain funding to test new technologies in the health care sector.

4.4 PRIVACY INSPECTIONS

REDESIGN OF ORGANIZATIONAL INSPECTIONS

The completion of organizational inspections in the Group was reviewed. As part of organizational inspections, we looked at to what extent the audited units were suitably placed (responsibilities, resources, etc.) to guarantee compliance with data privacy requirements. The approach for organizational inspections was reviewed to establish a uniform approach for national and international organizations, to further standardize the completion of organizational inspections, and to compare the audit results.

To this end, a universal, regular self-assessment was introduced. This has a uniform structure for national and international units. It includes a standardized set of questions on the issues of data privacy governance and data privacy-relevant processes, based on Deutsche Telekom's Binding Corporate Rules Privacy (BCRP).

The on-site organizational inspections also involve verifying the results of the self-assessment. The units for the on-site inspections are selected on the basis of the established data privacy criticality index (DCI). For the on-site control, a new standardized test guide Privacy Inspection Controlset is also available, which is based on the themes addressed in the self-assessment from the areas of data privacy governance and processes.

DATA PRIVACY INSPECTIONS

Based on the newly designed process for organizational inspections, initial data privacy inspections were conducted both nationally and internationally in 2017. In Germany, Telekom Mobility Solutions GmbH, congstar GmbH and Detecon International GmbH were audited, T-Systems Nederland B.V. was audited as an international player. It is increasingly clear that data privacy issues do not receive sufficient resources.

5. RECORD OF PROCESSING ACTIVITIES

Under Art. 30 (1) GDPR each controller shall maintain a record of all processing activities under its responsibility. Due to the similar regulation in the previous Federal Data Protection Act *(Bundesdatenschutzgesetz – BDSG)* Deutsche Telekom can use the corporate IT architecture and IT compliance documentation tool, which Deutsche Telekom IT managed and accordingly modified. The tool already provides substantial parts of the required information since this information was used to create the internal process directories in the German Group companies. In 2017, Group Privacy defined and implemented, in cooperation with colleagues from the Greek Group subsidiary OTE and Deutsche Telekom IT, the additional requirements for the process directory arising out of the GDPR. Since January 2018, the GDPR-compliant version of the process directory has been available throughout the EU to all Group companies.

6. IN-HOUSE DEVELOPMENT OF AN INTERNATIONALLY USABLE PSEUDONYMIZATION AND ANONYMIZATION SOLUTION

Group Privacy developed the "Enkroder" software in-house for pseudonymizing and anonymizing personal data.
Data is pseudonymized through the automated, cryptographically strong substitution of individual data with strings while maintaining formats. This substitution can be fully reversed provided the used key exists. As such, the Enkroder is ideal for pseudonymization processes.
The Chair of IT Security at the Ruhr University Bochum examined the process independently. The resulting cryptographic expert report confirms the strength of the algorithm used in the process.
The software was also presented to the Deutsche Telekom Data Privacy Advisory Board. The Board recommended the solution be marketed both internally and externally. In addition, the project was included in 2017 in the Deutsche Telekom internal intrapreneur program UQBATE Scholarship.

The main applications include:
Data warehouse
Generation of test data
Fraud detection
Data in and from tables (e.g. Excel)

The process is already being used at several places in the Group (e.g. Data Warehouse Telekom Germany in the acquisition layer).
It basically receives the underlying character set (alphabet) and the word length of the data. This supports the receipt of simple structures, such as telephone numbers, IP addresses, ID structures, thus increasing the amount of data that can be analyzed.
Among other things, the ability to process a wide range of international character sets (including Greek, Cyrillic, etc.) ensures that the Enkroder is also suitable for international use.

7. GROUP DATA PRIVACY AUDIT

RESULTS OF THE 2017 GROUP DATA PRIVACY AUDIT

Group Privacy has succeeded in establishing the Group data privacy audit as a permanent and recognized data privacy tool. In 2017, 30% of the Group workforce worldwide was surveyed online.
The goal of the audit is to measure the general level of data privacy practiced at Deutsche Telekom in Germany and at 36 of its international subsidiaries and associates. A further aim is to identify potential improvements in data protection and develop appropriate measures to achieve them.

The results of the 2017 audit show that data privacy at Deutsche Telekom is both functional and stable – and reconfirm its high levels of protection. The average score across the Group as a whole was 75% (2016: 70%) of the total points achievable (83% nationally, and 62% internationally). Compared with last year, the international units have improved in almost all items, substantially in some cases.

In order to reveal potential for improvement and initiate measures, the auditors will provide the units that took part in the audit with relevant reports. Group Privacy will monitor the need for action identified in the units as well as oversee the implementation of improvement measures, providing support in the form of information, advice, and reviews.

In all units whose award score is below the Group average, the directors and managers, together with the relevant data privacy contacts, will also agree additional measures to enhance data privacy.

8. GLOSSARY AND ABBREVIATIONS

TERM OR ABBREVIATION	DEFINITION
BCRP	Binding Corporate Rules Privacy
BDSG	Federal Data Protection Act
BfDI	German Federal Commissioner for Data Protection and Freedom of Information
GPR	Group Privacy
PSA	Privacy and Security Assessment process
GDPR	General Data Protection Regulation
OTC	Open Telekom Cloud
PSA	Privacy & Security Assessment
DTHS	Deutsche Telekom Healthcare Solutions
HfTL	Leipzig University of Applied Sciences (HfTL)
GPDA	Group data privacy audit
TCDP	Trusted Cloud data privacy profile
Telecommunications Act	Telecommunications Act
Telemedia Act	Telemedia Act
NatCos	National Companies
OTE	Hellenic Telecommunications Organization S.A.
DT-IT	Deutsche Telekom IT

PUBLISHED BY:

Deutsche Telekom AG
Group Privacy – Dr. Claus-Dieter Ulmer, Global Data Privacy Officer
53113 Bonn, Germany

Last revised 12/2017 | Subject to change and correction

ERLEBEN, WAS VERBINDET.