DEUTSCHE TELEKOM KONZERNDATENSCHUTZ TÄTIGKEITSBERICHT 2017 FÜR DEN KONZERNVORSTAND

Deutsche Telekom AG

Version 1.0
Stand 12.03.2018

ERLEBEN, WAS VERBINDET.

INHALT

VORWORT DES KONZERNDATENSCHUTZBEAUFTRAGTEN

Datenschutz ist ein wertbildender Faktor für Unternehmen. Er darf daher nicht nur eine Frage der Erfüllung gesetzlicher Anforderungen sein. Eine gelebte Datenschutzkultur ist vielmehr die Grundlage des vertrauensvollen Zusammenspiels zwischen Unternehmen einerseits sowie Kunden und Mitarbeitern andererseits. Es ist unser Anspruch, nicht nur das führende Telekommunikationsunternehmen zu sein, sondern auch die Marke und das Unternehmen, dem die Kunden am meisten vertrauen.
Neben der besten Infrastruktur, passenden Tarifen und aktuellen Endgeräten ist daher der Datenschutz ein zentraler Aspekt unseres Erfolges. Gemeinsam mit der Sicherheit sorgt der Datenschutz zum einen für den technischen Schutz der Daten unserer Kunden und Mitarbeiter. Zum anderen kümmert er sich aber auch um den sorgfältigen und wertschätzenden Umgang mit den Daten von Kunden und Mitarbeitern im Unternehmen. Datenschutz wirkt nach außen und nach innen.

„VOM KUNDEN HER DENKEN“

Wie trägt die Datenschutz-Organisation der Deutschen Telekom zum Erfolg des Konzerns bei?
Die Datenschutz-Organisation ist der Sparrings-Partner der operativen Einheiten. Durch die frühzeitige Einbeziehung der Datenschutz-Organisation in die Planungen des Unternehmens sorgt sie dafür, dass die Idee des „Privacy by Design“ von Anfang an berücksichtigt wird und die Lösungen letztendlich ein ausgewogenes Ergebnis darstellen, das sowohl den Kunden und Mitarbeitern, wie auch den operativen Anforderungen des Unternehmens gerecht wird.

Ein Beispiel: In der digitalen Welt benötigt ein Unternehmen qualitativ hochwertige Informationen über seine Kunden, um ihnen entsprechende Angebote machen zu können. Attraktive Angebote sind der Schlüssel zum wirtschaftlichen Erfolg. Doch woher nimmt ein Unternehmen die benötigten Informationen? Die kann es etwa über den Ankauf von Daten aus sozialen Netzwerken, von Kreditkartenunternehmen oder von Online-Kaufhäusern beziehen. Das scheint ein einfacher Weg zu sein. Die Deutsche Telekom bedient sich dieser Lösungen allerdings nicht. Warum ist das so?
Beim Ankauf von Daten stellt sich aus Datenschutzsicht zum einen natürlich die Frage, ob die Daten zulässig erhoben wurden und in zulässiger Weise weitergegeben werden können. Doch das ist nicht alles. Zum anderen stellt sich auch die Frage, ob die Daten, die ohne ausdrückliches Einverständnis des Kunden ausgewertet werden, qualitativ überhaupt eine taugliche Grundlage für die Gestaltung von neuen Produkten und Angeboten sein können. Auch damit beschäftigt sich die Datenschutz-Organisation in ihrem Austausch mit den operativen Einheiten im Konzern. Die Devise ist, über den Tellerrand hinaus zu schauen und den Blick auf das Ganze zu haben:
In jedem sozialen Kontext hat der Online-Mensch möglicherweise eine andere Identität. Deshalb tun sich Unternehmen sehr schwer damit, aus „heimlich“ abgegriffenen Daten die richtigen Schlüsse zu ziehen. Ich für mich selbst in meiner Rolle als Kunde behaupte, dass ich über Tracking-Mechanismen und Big Data Analytics noch nicht ein einziges passendes Angebot zu meinen Interessen erhalten habe. Warum? Weil jeder Online-Aspekt eben nur einen Teil meiner Persönlichkeit abdeckt und die Persönlichkeit als Ganzes mehr als die Summe seiner Teile ist. Ganz zu schweigen davon, dass viele Nutzer in ihrer Verzweiflung über das andauernde Monitoring ihrer Aktivitäten falsche Spuren legen. Zum Beispiel auch Musik streamen, die sie eigentlich nicht interessiert, bestimmte Produkte offline einkaufen, ihre Bonus-Karten nicht nutzen, bestimmte Dinge gerade nicht posten und, und, und...
Zudem sind die Analysesysteme noch nicht so weit, selbst aus zutreffenden Informationen die Persönlichkeit einer Person umfassend zu bestimmen. Wenn ich beispielsweise einen Krimi als Film streame, heißt das nicht, dass ich mich nicht auch für Romanzen oder Biographien interessiere. Analysesysteme, künstliche Intelligenz (KI) eingeschlossen, können eben – zumindest heute noch – nur mit dem umgehen, was da ist und auf was sie programmiert oder trainiert wurden.
Hochwertige Daten für erfolgreiche Geschäftsmodelle kommen also am besten vom Kunden selbst. Und der Kunde gibt dem Unternehmen diese hochwertigen Daten dann freiwillig, wenn er darauf vertrauen

kann, dass es damit in seinem Sinne ordentlich umgeht. Und dass er darauf vertrauen kann, dafür sorgt die Datenschutz-Organisation der Deutschen Telekom.

Der Blick in die Zukunft ist ebenfalls Teil des Auftrags der Datenschutz-Organisation. Bereits im Jahr 2016 haben wir mit unserem Whitepaper „Datenschutz in der digitalen Welt“ einen Ausblick auf die kommenden Entwicklungen gegeben. 2017 haben wir einen Wettbewerb zu Ideen für einen Privacy Bot ausgeschrieben und sehr interessante Beiträge erhalten. Die besten fünf Teilnehmer haben ihre Lösung in Berlin einer internationalen Jury vorgestellt und wurden prämiert.

Wir setzen auch auf Kooperationen, um den Datenschutz weiterzuentwickeln. Etwa beim Projekt Privacy Guard, mit dem wir die Entwicklung eines Datenschutzscanners unterstützen. Der soll dann dem Kunden schnell und übersichtlich verständlich machen, wie eine Anwendung seine Daten verarbeitet und ihm auf dieser Grundlage Entscheidungsspielräume eröffnen – eben die digitale Souveränität fördern.
Mit dieser Lösung werden Kunden eines Tages keine langen Datenschutzhinweise mehr lesen müssen, sondern vom Datenschutzscanner über das Wichtigste informiert werden und danach entscheiden können, welche Gestaltung sie bevorzugen. Mit der Zeit wird der Datenschutzscanner über eine KI auch lernen, die persönlichen Präferenzen des Kunden zu berücksichtigen.

Auch andere zukunftsweisende Ideen haben wir begleitet und werden wir begleiten. Genannt seien hier u.a. das Datencockpit, das unseren Kunden eine einheitliche Bedienoberfläche zur einfachen Verwaltung ihrer Daten anbieten wird. Noch nicht ganz so weit, aber ebenso vielversprechend ist die Lösung „Privacy Exchange“, mit der der unternehmens- und branchenübergreifende, transparente Austausch von Daten möglich wird. Selbstverständlich auf Grundlage des Einverständnisses der Kunden.
Dass dies alles zum Nutzen des Unternehmens und zum Nutzen unserer Kunden umgesetzt wird, dafür setzt sich die Datenschutz-Organisation der Deutschen Telekom ein. Für stabile Systeme einerseits und Transparenz sowie Wahlmöglichkeiten für den Kunden andererseits.

Was uns 2017 im Wesentlichen beschäftigt hat, haben wir in diesem Bericht zusammengestellt. Soviel sei schon einmal verraten: 2017 war nicht nur das Jahr der Datenschutz-Grundverordnung.

Herzliche Grüße, Ihr

CD Ulmer

2. ENTWICKLUNG DATENSCHUTZRECHTLICHER RAHMENBEDINGUNGEN

Am 25. Mai 2018 kommt die Datenschutz-Grundverordnung (DSGVO) zur Anwendung. Mit der DSGVO werden in der Europäischen Union (EU) einheitliche Datenschutzanforderungen eingeführt, die mehr Gewicht auf die Umsetzungsverantwortung in den Unternehmen legen. Dies bringt für unseren Konzern bis auf wenige Ausnahmen keine grundsätzlich neuen Anforderungen mit sich, da wir in den letzten Jahren bereits einige Verfahren eingeführt haben, die nun über die DSGVO allgemeinverbindlich eingeführt werden. Dazu gehört zum Beispiel das Privacy & Security Assessment Verfahren (PSA) das bereits der von der DSGVO geforderten Datenschutz-Folgenabschätzung zur Bewertung und Dokumentation von Risiken bei IT Systemen entspricht.
Die neue Regulierung haben wir aber zum Anlass genommen, die bestehenden Datenschutzinstrumente, wie eben das PSA-Verfahren, europaweit wesentlich einheitlicher und nachhaltiger umzusetzen. Damit steigern wir die interne und externe Transparenz und Effizienz unserer Lösungen. Allgemeinverbindliche Prozesse und Tools werden zudem die internationale Zusammenarbeit und die Akzeptanz des Datenschutzes im Konzern fördern.

Die DSGVO ist ein Meilenstein auf dem Weg zu einem echten europäischen Binnenmarkt, in dem für alle Teilnehmer die gleichen Regeln gelten und sich Produkte und Lösungen besser skalieren lassen. Die neuen Regeln sichern ein hohes Datenschutzniveau in Europa und ermöglichen gleichzeitig neue digitale Geschäftsmodelle. Damit ist die Grundforderung der Deutschen Telekom nach einem „Level Playing Field“ für alle Marktteilnehmer in der EU erfüllt. Das neue Datenschutzrecht schließt zudem eine Regelungslücke bezogen auf Anbieter, die ihr Produkte und Dienstleistungen in der EU von außerhalb der EU anbieten. Die DSGVO gilt zukünftig nämlich auch für nicht europäische Marktteilnehmer (z. Bsp. Google, Facebook oder Apple), und arrondiert somit des „Level Playing Field” – einheitliches Recht nicht nur für europäische Unternehmen, sondern für die Region Europa.
Um das mit der Datenschutzgrundverordnung erreichte „Level Playing Field“ zu bewahren, ist es daher von besonderer Bedeutung, dass die Mitgliedstaaten der EU im Rahmen der ihnen verbliebenen Gestaltungsspielräume nationale Sonderreglungen zur Datenschutzgrundverordnung nur dort treffen, wo diese zwingend erforderlich sind. Der deutsche Gesetzgeber hat bei der Neufassung des ab dem 25. Mai 2018 geltenden neuen Bundesdatenschutzgesetzes (BDSG neu) der an den ersten Entwürfen geäußerten Kritik teilweise Rechnung getragen und die Sonderreglungen für den nichtöffentlichen Bereich reduziert. Nun ist es wichtig, dass auch die anderen EU-Staaten sich an das „Regelsparsamkeitsgebot“ halten. Einige erste erlassene Gesetze deuten bereits in die richtige Richtung.
Leider wird der Ansatz zur Gestaltung eines „Level Playing Field“ aber nicht konsequent durchgehalten. Sektorspezifische Sonderregelungen werden weiter ohne sachlich nachvollziehbaren Grund aufrechterhalten. Die Regelungen für Telekommunikationsanbieter unterliegen beispielsweise einer gesonderten, schärferen Regulierung; der e-Privacy-Richtlinie und den entsprechenden Umsetzungsgesetzen. Auch im Rahmen der derzeit erfolgenden Überarbeitung der Telekommunikationsregeln ist keine wesentliche Besserung zu erwarten. Nach den bislang vorliegenden Verordnungsentwürfen bleibt der Wettbewerbsnachteil für Telekommunikationsanbieter in Europa in Teilbereichen bestehen. Da hilft es zunächst nur wenig, wenn zukünftig auch die „Over The Top Dienstleister“ (etwa WhatsApp und Skype) erfasst werden. Aufgrund der gegenüber der Datenschutzgrundverordnung deutlich restriktiveren Möglichkeiten der Weiterverarbeitung von Daten für Telekommunikationsanbieter werden Big-Data-Anwendungen im Telekommunikationsbereich auch in Zukunft kein vergleichbares Potential entfalten können wie in anderen Wirtschaftsbereichen. Denn die Weiterverarbeitung von Metadaten ist nach dem derzeitigen Entwurf der geplanten e-Privacy-Verordnung nur nach Einwilligung des Kunden möglich. Anders als in der Datenschutzgrundverordnung gibt es nach derzeitigem Stand keine Möglichkeiten, Daten unter Verwendung von Pseudonymen zu kompatiblen Zwecken weiter zu verarbeiten. Damit würden verschiedene Dienstleistungsmodelle, die dem Verbraucher nützlich sein können, die aber mit anonymen Daten nicht umsetzbar sind, nicht angeboten werden können:

Dies können Angebote zur Parkplatzsuche, Services zur Unfallvermeidung, bedarfsgerechte TV-Programmgestaltung oder Telemonitoring-Dienste im Gesundheitsbereich sein.
Vor diesem Hintergrund hat sich der Konzerndatenschutz gemeinsam mit der politischen Interessenvertretung in 2017 für ein sektorübergreifend ausgeglichenes Regulierungswerk eingesetzt. Diese Aktivitäten werden 2018 weiter fortgesetzt. Ziel ist es, Geschäftsmodelle zu ermöglichen, mit denen die Deutsche Telekom ihre hohe Kompetenz in technischen Lösungen zum Tragen bringen kann.

3. UMSETZUNG DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Der Konzerndatenschutz (Group Privacy) hat ein europaweites Steuerungsprojekt aufgesetzt, mit dem die Umsetzung der Anforderungen aus der DSGVO im Konzern gesteuert und gemonitort wird. Durch den übergreifend einheitlichen Ansatz können wir zudem darauf hinwirken, dass die neuen Anforderungen einheitlich und richtig interpretiert sowie einheitlich implementiert werden.
In diesem Zusammenhang war es auch erforderlich, den aktuellen Status Quo der Gesellschaften zum Umsetzungsstand der bereits bestehenden Datenschutzanforderungen festzustellen. Die dabei identifizierten zusätzlichen Umsetzungsbedarfe wurden in das Gesamtprojekt mit eingebunden.
In den Konzerngesellschaften wurden entsprechende Unterprojekte eingerichtet, um die konkrete Umsetzung der Anpassungsbedarfe in den jeweiligen Gesellschaften sicherzustellen. Alle IT-Systeme und Prozesse wurden auf diese Weise überprüft und Defizite werden individuell priorisiert abgearbeitet. Das Gesamtprojekt läuft seit dem Erlass der DSGVO in 2016 und findet seinen Abschluss im „GDPR-Readiness Check“ der dieses Jahr zum Stichtag 25.05.2018 durchgeführt wird.

Konkret unterteilt sich das Projekt in drei Phasen:

- Die erste Phase war die intern verbindliche Interpretation der Inhalte der DSGVO. Die DSGVO enthält einige interpretierungswürdige Regelungen, für die wir Klärung schaffen mussten. Diese Klärung haben wir mit Beteiligung unseres Datenschutzbeirates durchgeführt. Im Ergebnis dieses Klärungsprozesses sind für den gesamten Konzern verbindliche sogenannten „Binding Interpretations“ entstanden, die wir auf unserer Webseite http://www.telekom.com/datenschutz im Bereich „Mehr Transparenz“ veröffentlicht haben.
- Phase zwei ist die arbeitsteilig operative Umsetzung der Binding Interpretations, also die Definition von konkreten Anforderungen, die Vermittlung der Anforderungen an die Fachseiten und letztlich natürlich die konkrete Umsetzung in Systemen und Prozessen. Z.B. waren bei der Telekom Deutschland die Datenschutzhinweise in verschiedenen Teilen redaktionell anzupassen. Die redaktionelle Anpassung erfolgte hier durch Group Privacy als Governance-Einheit und die Umsetzung erfolgt bei den operativen Gesellschaften, begleitet von Group Privacy.
- In der Phase 3 werden im Jahr 2018 Readiness Checks zur Kontrolle durchgeführt. Parallel dazu wird die Konzernrevision ebenfalls die Umsetzung prüfen.

Besondere strukturelle Anpassungen waren und sind im Rahmen der DSGVO nicht erforderlich, da wir bereits auf die bestehenden Governance Strukturen des Datenschutzes und ein seit Jahren etabliertes und weiterentwickeltes Privacy and Security Assessment Verfahren (PSA) als Datenschutzfolgeabschätzung aufsetzen konnten.
Im Laufe des Projektes hat sich aber herausgestellt, dass eine besondere Herausforderung die große Anzahl an Systemen bzw. Handlungsfelder (z.B. Datenschutzhinweise) sind. Diese mussten sowohl auf Anpassungsbedarfe hin untersucht und ggf. auch angepasst werden. Dafür musste der Konzern deutlich mehr personelle und finanzielle Ressourcen zur Verfügung stellen als ursprünglich erwartet.

4. BERATUNGSHIGHLIGHTS

4.1 KUNDENDATENSCHUTZ

Transparenz stand im Jahr 2017 im Mittelpunkt. Gut zugängliche und für jedermann verständliche Informationen sind die Grundlage für den Datenschutz bei der Deutschen Telekom. Unsere Kunden sollen sich jederzeit darüber informieren können, in welchem Umfang ihre Daten verarbeitet werden, wenn sie die Dienstleistungen und Produkte der Deutschen Telekom nutzen. Dafür stehen wir unseren Kunden zum einen persönlich zur Verfügung, so hat Group Privacy im Jahr 2017 mehr als 13.500 Kundenanfragen zum Thema Datenschutz direkt oder schriftlich beantwortet. Zum anderen haben wir zur weiteren Verbesserung der Verständlichkeit neue Texte entwickelt, welche die Datenverarbeitung anschaulich beschreiben. So wird unter der Überschrift „Ihre Daten bei der Telekom“ erklärt, was unter „Personendaten“, unter „Nutzungsdaten“ oder unter „Standortdaten“ zu verstehen ist. Die Texte sind sowohl auf der Internetseite www.telekom.com als auch auf der www.telekom.de, dort unter „Datentransparenz“, zu finden. Diese zusammen mit Kunden entwickelten Datenschutzhinweise ergänzen die detaillierteren, produktspezifischen Datenschutzhinweise, auf die jeweils verlinkt ist.

WEITERE INFORMATIONEN ZUM DATENSCHUTZ AUF UNSERER INTERNETSEITE

Auf der Internetseite www.telekom.com/datenschutz haben wir dieses Jahr weitere Informationen für und gemeinsam mit unseren Kunden entwickelt. Dort wird ausführlich beschrieben, wie wir die Daten unserer Kunden schützen und wir erklären, was der Kunde selbst zum Schutz seiner Daten tun kann. Einen besonderen Fokus haben wir dabei auf das Thema Anonymisierung und Pseudonymisierung gelegt. Dort, wo wir zwar Kundendaten benötigen, ein Personenbezug aber nicht oder nicht direkt erforderlich ist, schützen wir die Kundendaten z.B. durch Anonymisierung und Pseudonymisierung. Was das genau ist und wie das funktioniert, haben wir ebenfalls auf unserer Webseite leicht verständlich mit zwei bereitgestellten Videos erklärt.

Für mehr Transparenz über unsere internen Prozesse haben wir die eigens für unsere Mitarbeiter weltweit zur Verfügung gestellte Onlineschulung zur DSGVO auf unserer Webseite für Jedermann zur Verfügung gestellt. Die Schulung ist im Bereich "Mehr Verbindlichkeit" zu finden.

Ebenso haben wir die wichtigsten internen Regelungen zum Datenschutz publiziert und auch, welche politischen Positionspapiere zum Thema Datenschutz von uns in die politische Diskussion eingebracht wurden. Diese sind ebenfalls auf unserer Internetseite im Bereich "Mehr Transparenz" abrufbar.

Wir verstehen Sicherheit und Datenschutz als Design-Kriterium für alle unsere Produkte und Dienstleitungen. Wir haben dafür im Jahr 2009 das PSA-Verfahren entwickelt, mit dem wir ein spezielles Risikoassessment mit Fokus auf die Kunden- und Mitarbeiterdaten durchführen. Basierend auf dieser Analyse werden gezielte Maßnahmen zum Schutz der Daten definiert und von Anfang an in die Produkte eingebaut. Wir haben dieses Verfahren über die Jahre weiterentwickelt und 2017 nochmals speziell an die Anforderungen der Datenschutzgrundverordnung angepasst. Zum PSA-Verfahren sind ebenfalls mehr Informationen auf der Internetseite www.telekom.com/datenschutz hinterlegt.

INFORMATIONEN BEIM EINKAUFSPROZESS

Der Deutschen Telekom reicht es aber nicht darauf zu vertrauen, dass die Kunden die Datenschutzhinweise lesen. Zusätzlich wird der Kunde im Rahmen des Einkaufsprozesses informiert, wenn das gewünschte Produkt bei der Datenverarbeitung Besonderheiten hat. Dies gilt zum Beispiel dann, wenn Daten von der Deutschen Telekom an einen anderen Dienstleister weitergegeben werden müssen, damit der Dienst erbracht werden kann. Dies ist zum Beispiel bei der Einbindung der Sprachsteuerung „Amazon Alexa“ bei Magenta Smart Home der Fall. Hier müssen Kundendaten an Amazon gegeben werden, damit der Dienst funktioniert. Denn Amazon ist letztlich der Betreiber der angebotenen Lösung. Bevor der Kunde das Produkt beauftragt, bekommt er einen gut sichtbaren Hinweis auf diesen Vorgang.

Gleiches gilt für die Buchung der Zusatzoption „StreamOn“. Hier weisen wir gesondert darauf hin, dass der Datenverkehr des Kunden geprüft wird, um den reibungslosen Ablauf des Dienstes zu ermöglichen.

INTERNATIONALE FUNKAUSSTELLUNG

Dass die neuen Datenschutzhinweise bei den Kunden gut ankommen, hat sich auf der Internationalen Funkausstellung (IFA) 2017 gezeigt. Der Datenschutz der Deutschen Telekom war auf der IFA mit einem Stand vertreten, um die Meinung der Kunden zu hören und bei Fragen zum Datenschutz zu beraten. Neben den Texten wurde auch der Prototyp einer Datenschutz-App vorgestellt, der „Datenschutzscanner“. Der „Datenschutzscanner“ ist eine App, die Verbraucherinnen und Verbraucher darüber informiert, wie andere Apps mit ihren persönlichen Daten umgehen. Darüber hinaus zeigt der „Datenschutzscanner“ Handlungsmöglichkeiten auf, mit denen die Datenverarbeitungen von Apps entsprechend der eigenen Datenschutzpräferenzen angepasst werden können. Dies soll den Verbraucherinnen und Verbrauchern helfen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Die Entwicklung der App erfolgt im Rahmen eines Forschungsprojekts, das vom Bundesministerium für Bildung und Forschung innerhalb der Bekanntmachung „Selbstbestimmt und sicher in der digitalen Welt“ gefördert wird. Am Forschungskonsortium sind die Partner mediaTest digital, InfAI e.V., Quadriga Hochschule Berlin und SRIW e.V. beteiligt. Die Telekom unterstützt neue verbraucherfreundliche Datenschutzlösungen wie den „Datenschutzscanner“ und hat die App deshalb auf der IFA vorgestellt.

Datenschutz spielt auch bei einer anderen App eine große Rolle, bei der Spiele-App „Sea Hero Quest“. Mit „Sea Hero Quest unterstützt die Deutsche Telekom die internationale Demenzforschung. Das mobile Spiel lieferte innerhalb weniger Monate ein enormes Potential an Diagnosedaten für die Forschung. Group Privacy unterstützte das Projekt bei der Realisierung und sorgte dafür, dass ausschließlich anonyme Daten verwendet werden. Dem Nutzer wird verständlich erklärt, wie die Spiel-Daten über das Navigationsverhalten und Orientierungsvermögen des Nutzers der wissenschaftlichen Forschung dienen.

ZUSAMMENARBEIT MIT AUFSICHTSBEHÖRDEN

Datenschutz bei der Deutschen Telekom unterliegt der Aufsicht verschiedener Behörden. Daher ist die Zusammenarbeit von Group Privacy mit diesen Behörden enorm wichtig. Neben der Bundesnetzagentur, ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die Deutsche Telekom zuständig, zusätzlich für die Telemediendienste und den Beschäftigtendatenschutz aber die verschiedenen Landesdatenschutzbeauftragten. Im letzten Jahr gab es mit den einzelnen Behörden eine Reihe von Themen, die diskutiert wurden und von denen nachfolgend einige beispielhaft genannt werden.

Der Dienst „Motionlogic“, den die Deutsche Telekom-Tochter „motionlogic GmbH“ anbietet, erhält anonymisierte Verkehrsdaten der Mobilfunkkunden der Telekom Deutschland GmbH, um daraus Analysen zum Verkehrsaufkommen zu machen. Nachdem die BfDI das Anonymisierungsverfahren als tragfähig erachtet hatte, fand im Jahr 2017 im Interesse eines Berliner Großkunden, der den Dienst nutzen möchte, auch eine Abstimmung mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit statt. Mit dieser werden die Fragestellungen zum Anonymisierungsverfahren erneut erörtert. Die Diskussionen werden voraussichtlich zu Beginn des Jahres 2018 abgeschlossen werden können.

BfDI und Bundesnetzagentur haben die Deutsche Telekom um Stellungnahme zu einem SAP–System gebeten, in dem die Löschfristen nicht ordnungsgemäß umgesetzt waren. Dabei handelt es sich um eine SAP-Plattform mit verschiedenen Modulen zum Finanz- und Logistikwesen. Alle Module verarbeiten eine sehr hohe Anzahl an Datensätzen. Außerdem befindet sich die Plattform in einem interaktiven Verbund mit anderen Systemen. Das bedeutet, dass dem Löschvorgang jeweils komplexe Prüfmechanismen vorausgehen müssen, damit die Integrität, der noch zu haltenden Daten bestehen bleibt. Im Rahmen eines großen Projekts wird die Löschfunktion nun etabliert, nachdem die Deutsche Telekom der BfDI das geplante Vorgehen vorgestellt hat und es von dieser als plausibel erachtet wurde.

Im Rahmen eines weiteren Beratungs- und Kontrollbesuchs hat die Telekom der BfDI die Datenverarbeitung bei den W-Lan-Hot Spots vorgestellt. In dem Besuch ging es um die Telekom Hot Spots und um die Hot-Spot-Funktionen, bei denen die Deutsche Telekom als Vorleister auftritt (z.B. bei

McDonalds). Die BfDI hat Verbesserungen bei den Datenschutzhinweisen angeregt, befand die Datenverarbeitung aber als ausreichend sparsam und insgesamt richtig.

4.2 BESCHÄFTIGTENDATENSCHUTZ

Im Beschäftigtendatenschutz lagen die Schwerpunktthemen in der Beratung und bei der Unterstützung interner Organisationsthemen, der Nutzung von digitalen Diensten durch Mitarbeiter sowie im Bereich der Maßnahmen zu Schulungs- und Awareness datenschutzrechtlicher Themen.

INTERNE ORGANISATION

Die Deutsche Telekom ist in einem dynamischen Marktumfeld tätig und stetig mit Herausforderungen konfrontiert, die auch Umbau– bzw. Reorganisationsmaßnehmen im Konzern erfordern.
Group Privacy hat daher die Datenschutzanforderung *Datenschutzmaßnahmen in Organisationsprojekten* erstellt. Die Anforderung ist als Leitfaden für eine vereinfachte und strukturierte Handhabung von organisatorischen Veränderungen konzipiert. Das Dokument greift verschiedene Reorganisationsmaßnahmen auf und definiert einzuhaltende Anforderungen. Für die Einhaltung der Anforderungen werden grundsätzlich Umsetzungsvorschläge gegeben. Diese sind konkret beschriebene technische und organisatorische Lösungen zur Erfüllung der Anforderungen.

Auf Initiative von Group Privacy wurde der Management Self Service für Führungskräfte weiterentwickelt. Das Tool SAP HR stellt den Führungskräften der Deutschen Telekom ein Management Self Service bereit. Dort können sie ihre Führungsaufgaben, soweit sie in der EDV abbildbar sind, erledigen. Im Projekt „Datenschutzkonforme Migrationen“ wurde eine Lösung erarbeitet und implementiert, die es Führungskräften datenschutzkonform erlaubt, die Daten ihrer Mitarbeiter zu sehen. Dadurch ist eine effektivere Nutzung des Management Self Service im Rahmen des datenschutzrechtlichen „Need to Know Prinzip“ möglich.

DIGITALE DIENSTE

Im heutigen Alltag unserer Mitarbeiter gibt es etliche Kommunikationstools für die unterschiedlichsten Anwendungsbereiche. Mitarbeiter kennen und nutzen diese Tools schon im privaten Bereich und sind mit ihnen vertraut. Daher bedeutet die dienstliche Nutzung frei verfügbarer Kommunikationstools eine große Vereinfachung.

Group Privacy hat erkannt, dass die Nutzung neuer, auch externer digitaler Dienste grundsätzlich einen anderen Umgang mit diesen Diensten erfordert. Bislang war die Nutzung von externen, nicht zur dienstlichen Kommunikation freigegebenen Kommunikationsmitteln, nicht erlaubt. Das Unternehmen stellte dienstliche Kommunikationsmittel zur Verfügung, die zuvor eingehend aus Datenschutzsicht geprüft wurden. Mit der weiter fortschreitenden Digitalisierung musste dieser „rundum sorglos Ansatz“ überdacht werden. Die eingehende Prüfung aller verfügbaren und für spezifische Bereiche ggf. nützlichen digitalen Dienste ist nämlich von betrieblichen Datenschutzorganisationen nicht zu leisten. Ein komplettes Verbot dieser Dienste erscheint aber auch dann unangemessen, wenn dem praktischen Nutzen offensichtlich keine relevanten Risiken gegenüberstehen. Gleichzeitig brauchen Mitarbeiter im Umfeld der mit der Digitalisierung einhergehenden schnellen Veränderungen Freiräume für eigene, an Chancen und Risiken orientierten Entscheidungen.
Um eine sinnvolle Nutzung frei verfügbarer Tools zu ermöglichen, wurde daher das umfassende Verbot aufgehoben. Stattdessen setzt der Konzern stärker auf die Eigenverantwortung der Mitarbeiter.
Um unsere Mitarbeiter dabei zu unterstützen, haben wir Regeln entwickelt, die klare Leitplanken aufzeigen, was möglich ist und was nicht. So dürfen etwa für streng vertrauliche Informationen und personenbezogene Kundendaten auch weiterhin nur bestimmte, besonders geschützte und geprüfte Tools genutzt werden. Für lediglich interne Informationen soll die Entscheidung dagegen weitgehend beim Mitarbeiter liegen.
Dabei darf niemand gezwungen werden, solche digitalen Dienste zu nutzen. Die „Grundversorgung“ mit dienstlichen Kommunikationsmitteln wird allen Mitarbeitern weiterhin zur Verfügung gestellt (E-mail,

internes soziales Netzwerk „You and Me“, mobile und standortbezogene Telefonangebote, Zusammenarbeitsplattformen wie „sharepoint“, etc.).

SCHULUNG UND AWARENESS

Alle zwei Jahre werden alle Mitarbeiter und Mitarbeiterinnen konzernweit auf die gesetzlichen und konzerninternen Bestimmungen des Daten- und Informationsschutzes geschult sowie auf das Daten- und Fernmeldegeheimnis verpflichtet. Durch die regelmäßige Wiederholung der Verpflichtung in Zusammenhang mit einer Schulungs- bzw. Sensibilisierungsmaßnahme wird sichergestellt, dass alle Beschäftigten der Deutschen Telekom nachhaltig auf die Einhaltung der Bestimmungen zum Datenschutz hingewiesen und verpflichtet werden. Bei der Schulung handelt es sich um ein Online-Training. Die erfolgreiche Teilnahme an der Schulung wird revisionssicher dokumentiert. Die Schulung ist auch über unsere Internetseiten abrufbar (s. oben unter Kundendatenschutz).

Der Schwerpunkt der Verpflichtungsschulung im Jahr 2017 lag auf der neuen Datenschutzgrundverordnung, die im Mai 2018 zur Anwendung kommt. Das Konzept der Schulung ist praxisorientiert: die Teilnehmer begleiteten die Kunstfigur „Tom“, einen Mitarbeiter der Deutschen Telekom, durch den Tag. Beispielsweise auf dem Weg zur Arbeit, bei der Teilnahme an einer Besprechung und in der Mittagspause. Jede Situation beinhaltet ein spezielles datenschutzrechtliches Thema.

Eine der wesentlichen Aufgaben des Datenschutzbeauftragten ist es, Beschäftigte mit den Vorschriften des Datenschutzrechts und den besonderen Erfordernissen des Datenschutzes vertraut zu machen. Group Privacy erstellt daher Schulungen zu verschiedenen Themen des Datenschutzes, die die Beschäftigten selbständig im Intranet durchführen können. Außerdem werden von Group Privacy Präsenzschulungen zu grundsätzlichen und zu aktuellen Fragestellungen angeboten.

Neben diesen Schulungen übernehmen Kolleginnen und Kollegen aus dem Bereich Group Privacy seit einigen Semestern Dozententätigkeiten in einer Reihe von Bachelor- und Masterstudiengängen an der Hochschule für Telekommunikation in Leipzig (HfTL). Die Tätigkeit umfasst Vorlesungen und Teletutorien im Datenschutzrecht sowie in Einzelfällen auch die Betreuung von Bachelorarbeiten. Während diese Vorlesungen im Rahmen des Moduls „IT-Recht“ u.a. in den Studiengängen Wirtschaftsinformatik oder Informations- und Telekommunikationstechnologie stattfinden, gibt es an der HfTL in den Masterstudiengängen auch eine eigene Profilierungslinie „Datenschutz und Sicherheit in den Informationssystemen“. Seit dem Sommersemester 2017 können auch Beschäftigte der Deutschen Telekom an diesen Vorlesungen teilnehmen. Sie können dies im Rahmen eines Programms tun, das mit einem Zertifikat abschließt. Dieses Angebot richtet sich an Fachkräfte mit bereits vorhandenem Master- oder Diplomabschluss, die beispielsweise in der Entwicklung von Produkten und Prozessen tätig sind und ihre Kompetenzen mit einem profunden Datenschutz-Expertenwissen erweitern wollen. Teilnehmer, die alle Module des Zertifikatsprogramms absolviert haben und wenigstens über den Abschluss „Diplom FH“ verfügen, können über eine Masterarbeit sogar einen Masterabschluss als weiteren akademischen Abschluss erlangen. In Zusammenarbeit mit dem Lehrstuhlinhaber für „Datenschutz und Sicherheit in den Informationssystemen“, Prof. Dr. Erik Buchmann, hat Group Privacy die Rechtsmodule für diese Profilierungslinie konzipiert und die entsprechenden Vorlesungen an der HfTL gehalten. Das Zertifizierungsprogramm wird auch in den kommenden Semestern fortgeführt werden.

4.3 DATENSCHUTZLÖSUNGEN FÜR DIE IT/TK INFRASTRUKTUR UND FÜR PRODUKTE UND SERVICES FÜR GROßE GESCHÄFTSKUNDEN

DATENGETRIEBENE GESCHÄFTSMODELLE

Datenschutz ist kein Hemmschuh für die erfolgreiche Vermarktung von datenbasierten Geschäftsmodellen – ganz im Gegenteil: Durch die kompetente Anwendung datenschutzkonformer Lösungen entsteht Vertrauen bei Kunden – eine wichtige Voraussetzung für die erfolgreiche Vermarktung datengetriebener Geschäftsmodelle.

Wir betrachten datenschutzrechtliche Fragen im Zusammenhang mit Geschäftsmodellen, welche durch Verwendung von Analysemethoden, vorhandene Daten und/oder frei verfügbare Daten und/oder gekaufte Daten, einer Wertschöpfung unterziehen und dadurch neues Wissens schaffen. Die Geschäftsmodelle beruhen auf der Vermarktung dieses neu entstandenen Wissens.
Themen wie das „Internet der Dinge“ und „Automatisierung“ spielen dabei eine wichtige Rolle, weil in diesem Kontext massenhaft Daten generiert werden. „Big-Data-Technologien“, moderne Methoden zur „Datenanalyse“ und „Künstliche Intelligenz“ zur Auswertung, Interpretation und Veredelung von Daten sind die wichtigen Werkzeuge bei datengetriebenen Geschäftsmodellen.
Daten für Big-Data-Analysen können aus den unterschiedlichsten Quellen stammen. Viele dieser Daten berühren den persönlichen Bereich und ermöglichen – direkt oder indirekt – vielfältige Rückschlüsse auf Lebensumstände und Verhalten der von den Datenanalysen Betroffenen. Hier gilt es, einen ausgewogenen Ausgleich zwischen den Interessen der Menschen am Schutz persönlicher Daten und dem Interesse der Unternehmen oder Behörden an der Nutzung neuer Analysemöglichkeiten zu finden. Dies setzt voraus, dass Unternehmen und Behörden transparent und datenschutzkonform agieren.
Die Deutsche Telekom setzt einerseits selbst Big Data ein, um ihre Prozesse effizienter zu gestalten und z.B. ihren Kundendienst zu optimieren. Andererseits ist sie daran interessiert, ihren Kunden Produkte und Dienstleistungen anzubieten, für die eigene Daten oder die der Kunden zu Big-Data-Analysen genutzt werden. Sowohl für die eigene Nutzung, als auch in der Vermarktung nach außen muss die zulässige Balance zwischen dem Schutz der Privatsphäre und dem Nutzen der Chancen von Big Data gefunden werden.
Group Privacy hat sich im Rahmen eines Projektes intensiv mit den Anforderungen an die rechtskonforme Gestaltung datengetriebener Geschäftsmodelle beschäftigt und im Rahmen von Workshops und Gesprächen mit den verantwortlichen Geschäftsbereichen ausgetauscht. Im Ergebnis hat Group Privacy Ende 2017 ein „Whitepaper“ zur datenschutzkonformen Gestaltung datengetriebener Geschäftsmodelle vorgelegt.
Dieses interne Papier besteht aus einer umfassenden rechtlichen Bewertung, zeigt konkrete Gestaltungsansätze auf und gibt somit eine nachhaltige Orientierung für die Geschäftseinheiten des Konzerns bei der Entwicklung aktueller und zukünftiger Geschäftsmodelle. Die Positionierung der Deutschen Telekom ist dabei klar: Maximale Transparenz für unsere Kunden durch „Privacy by Design“.

DATENSCHUTZKONFORME NUTZUNG VON KUNDENDATEN ZUR FEHLERANALYSE

Die Deutsche Telekom setzt zur Erkennung von Ausfallwahrscheinlichkeiten ihrer Netzkomponenten und zur Analyse von Fehlersituationen zunehmend auf Big-Data-Technologien. Ziel dieser Initiativen ist eine höhere Verfügbarkeit der Netz- und Serviceleistungen sowie die Reduzierung von Störungen in der gesamten Kommunikationsinfrastruktur. Um die Datenschutzkonformität derartiger Analysen sicherzustellen, werden die einzelnen Maßnahmen eng mit Group Privacy abgestimmt.
Grundsätzlich werden bei den Analysen vorrangig technische Parameter der Produkte und der einzelnen Komponenten der Anschlussbereiche ausgewertet. Derartige Daten haben keinen Personenbezug und werden nach bestimmten Fehlermustern ausgewertet, um Rückschlüsse auf die Vitalität der Infrastruktur zu gewinnen, diese Daten können jedoch keine Aussage über die Ausfallwahrscheinlichkeit, bzw. Störung im kundenbezogenen Teil des Anschlussbereichs treffen.
Wird zu Zwecken der Beseitigung von Fehlern und Störungen auf Verkehrs- und Nutzungsdaten der Kunden zurückgegriffen, erfolgt dies ausschließlich auf Grundlage des § 100 TKG unter Einbeziehung des aktuellen Stands des Entwurfs der E-Privacy Verordnung (Art. 6 Abs. 1b).

Dabei erfolgt im ersten Schritt eine Prüfung, ob die Zweckbestimmung bei der Verarbeitung dieser Daten im Einklang mit den gesetzlichen Regelungen steht und die Verwendung der Daten zur Beseitigung von Fehlern und Störungen erfolgen wird. Im zweiten Schritt wird auf Basis pseudonymisierter Daten, oder bei Vorliegen von konkreten, von Kunden gemeldeten Störungen auf Basis von Klardaten analysiert. Big Data Analysen in diesem Kontext erfolgen also mit

- technischen Parametern ohne Personenbezug,
- anonymisierten Daten, oder
- pseudonymisierten Daten, oder
- Klardaten (bei Vorliegen konkreter kundenbezogener Störungen)

Wir arbeiten derzeit an einer Lösung, um eine Repersonalisierung von pseudonymisierten Daten am Ende des Analyseprozesses, etwa wenn ein konkretes Fehlerbild auf den Ausfall einer Komponente im kundenbezogenen Teil des Anschlussbereichs hinweist, durchführen zu können. Hierzu sind jedoch noch einige rechtliche Fragen in der Diskussion und nicht zuletzt wird diese Vorgehensweise mit der zuständigen Aufsichtsbehörde abgestimmt werden.

OPEN TELEKOM CLOUD (OTC)

In den Jahren 2016 und 2017 hat Group Privacy entscheidend bei der Gestaltung und datenschutzrechtskonformen Entwicklung von Cloud Lösungen mitgearbeitet. So wurde mit der Open Telekom Cloud eine Cloud Lösung entwickelt, die persönliche Daten ausschließlich innerhalb der Europäischen Union speichert, verarbeitet und administriert. Es erfolgen keine Wartungs- oder Supportzugriffe auf die Open Telekom Cloud aus sogenannten Drittländern außerhalb der Europäischen Union. Somit stellt die Open Telekom Cloud für Kunden, die einen potenziellen Zugriff von ausländischen Sicherheitsbehörden auf ihre Daten ausschließen möchten, eine kostengünstige Alternative zu dem klassischen IT-Outsourcing dar. Das Geschäftsmodell wurde von Anfang an mit Group Privacy abgestimmt. Sämtliche Partnerverträge sowie die kundenbezogenen Verträge und Geschäftsbedingungen wurden von Group Privacy datenschutzrechtlich geprüft. Die technische Umsetzung des Geschäftsmodells wurde im Rahmen des PSA-Verfahrens begleitet.
Darüber hinaus konnte Group Privacy die Deutsche Telekom bei ihrem Vorhaben unterstützen, für einen weiteren großen Cloudanbieter als sog. Data Trustee aktiv zu werden.

PAN-NET

Pan-Net ist ein innovatives, neuartiges paneuropäisches Produktions- und Geschäftsmodell für die Telco der Zukunft. Services, Produkte und Daten werden nicht mehr auf einzelnen Plattformen in jeder einzelnen Landesgesellschaft bereitgestellt, sondern europaweit in einer agilen, standardisierten Infrastruktur-Cloud gebündelt, die auf wenige Rechenzentren in Europa verteilt ist. Die Produktion wird von traditionellen Hardware-Plattformen in eine virtuelle Umgebung verlagert, die auf den neuesten Technologien rund um IP, Software definierten Netzwerken und Virtualisierung beruht. Betrieben wird das paneuropäische Netz von eigens hierfür gegründeten Pan-Net Einheiten. Die Geschäftstransformation wird von der Deutsche Telekom Pan-Net s.r.o. Bratislava (Slowakei) vorangetrieben und von Group Privacy im Rahmen eines Key-Accounts intensiv datenschutzrechtlich betreut.
Das internationale Business- und Produktionsmodell der Pan-Net ist bislang einzigartig und datenschutzrechtlich höchst anspruchsvoll. Komplexe technische und juristische Sachverhalte mit Schwerpunkt auf dem Geschäftsmodell sowie der künftigen technischen Produktionsplattform (Rechenzentren, Operations/DevOps), wurden in Zusammenarbeit mit den Datenschutzbeauftragten der teilnehmenden Telekom-Landesgesellschaften geprüft und bewertet. Unterschiedliche gesetzliche Rechtsnormen mussten bewertet, nationale Anforderungen aus 13 Ländern im Detail geprüft und harmonisiert, und im Produktions- und Geschäftsmodell einheitlich umgesetzt werden.

Eine Pan-Net Privacy Governance wurde entwickelt und etabliert sowie neue datenschutzrechtliche Vorgaben (Prozesse) erstellt. Ein Teil der Privacy Governance ist ein Privacy Contractual Framework, das

die vertraglichen Grundlagen des Geschäftsmodells regelt und auf eigens für Pan-Net entwickelten Vertragsmustern beruht. Diese berücksichtigen sämtliche nationalen Vorschriften der teilnehmenden Landesgesellschaften.

Zur Sicherstellung der Datenschutzanforderungen in der technischen Produktionsplattform, wird das PSA-Verfahren für alle Teile der Infrastruktur sowie Services im agilen Entwicklungsumfeld angewendet. Der Komplexitätsgrad steigt hier erheblich, da neben den bereits vorhandenen hohen Telekomstandards auch die nationalen Anforderungen technisch realisiert werden müssen.
In Hinblick auf die Anwendbarkeit der DSGVO im Mai 2018 wurde in 2017 bereits intensiv an der DSGVO-Readiness des Pan-Nets gearbeitet.

VERARBEITUNG VON GESUNDHEITSDATEN

Die Verarbeitung personenbezogener Gesundheitsdaten ist datenschutzrechtlich grundsätzlich als kritisch einzustufen; handelt es sich doch in der Regel um besonders sensible Daten. Zwischen der Geschäftseinheit Deutsche Telekom Healthcare and Security Solution, die entsprechende Geschäftsmodelle entwickelt und betreibt, und Group Privacy gibt es eine sehr enge Zusammenarbeit, um die Datenschutzkonformität aller Geschäftsaktivitäten sicherzustellen.
Partnerschaften zwischen Trägern im Gesundheitsbereich und der T-Systems International und deren Tochter Deutsche Telekom Healthcare and Security Solution (DTHS) sind das präferierte Geschäftsmodell zum Betreiben entsprechender Plattformen zur sicheren Verarbeitung von Gesundheitsdaten.
Neben dem Betrieb von zentralen Plattformen, ist die Sicherstellung einer integrierten IT-gestützten Kommunikation zwischen den Akteuren der jeweiligen Gesundheitsregion wesentliches Element der Geschäftstätigkeiten. Ziel ist es, durch unser Angebot einer intensiven Geschäftsmodellberatung, die zunehmende Interdisziplinarität der Patientenversorgung und die Spezialisierung auf Versorgerseite auf höchstem datenschutzrechtlichem Niveau durch sichere Plattformen und Kommunikationslösungen abzubilden.
Nicht immer kann der Datenschutz den Wünschen der Anforderer entsprechen. So gibt Group Privacy beispielsweise vor, ausschließlich ausgewählte und hinreichend sichere Endgerätehardware für den Zugriff auf die zentralen Plattformen durch die Arztpraxen zu verwenden. Die Verwendung arzteigener, unkontrollierter Hardware ist sowohl aus Sicht des Datenschutzes als auch der Sicherheit ein extrem hohes Sicherheitsrisiko, weshalb Ansätze, die diese Hardware in die Datenverarbeitung mit einbeziehen, nicht freigegeben werden. Zudem wird stets der Einsatz einer Gematik-zertifizierten Telematikinfrastruktur in die Lösungskonzepte geprüft.
Diese konsequente Haltung wird nicht nur gegenüber unseren Kooperationspartnern eingehalten, sondern spielt auch eine wichtige Rolle in der politischen Diskussion. Die Zuweisung von Fördermitteln zur Erprobung neuer Technologien im Gesundheitswesen wird durch überzeugende Datenschutz- und Sicherheitskonzepte begünstigt.

4.4 DATENSCHUTZKONTROLLEN

NEUKONZEPTION ORGANISATIONPRÜFUNGEN

Die Durchführung von Organisationsprüfungen im Konzern wurde einem Review unterzogen. Im Rahmen von Organisationsprüfungen wird die Frage untersucht, inwieweit die geprüften Einheiten ausreichend gut aufgestellt sind (Verantwortlichkeiten, Ressourcen, etc.), um die Erfüllung von Datenschutzanforderungen zu gewährleiten. Die Überarbeitung des Ansatzes für Organisationsprüfungen erfolgte mit dem Ziel, einen einheitlichen Angang für nationale und internationale Organisationen zu etablieren, die Durchführung der Organisationskontrollen weiter zu standardisieren und die Kontrollergebnisse einer Vergleichbarkeit zuzuführen.

Hierfür wurde flächendeckend ein regelmäßig durchzuführendes Self-Assessment eingeführt. Dies ist einheitlich ausgestaltet für nationale und internationale Einheiten. Es enthält ein standardisiertes Set an Fragen zu den Themenbereichen Datenschutz-Governance und Datenschutzrelevante Prozesse, basierend auf den Binding Corporate Rules Privacy (BCRP) der Deutschen Telekom.

Im Rahmen der Vor-Ort-Organisationskontrolle werden die Ergebnisse des Self-Assessments verifiziert. Die Auswahl der Einheiten für die Vor-Ort-Kontrollen erfolgt auf Basis des etablierten Datenschutzkontrollindexes (DKI). Für die Prüfungen Vor-Ort wird zudem ein neuer standardisierter Prüfleitfaden „Privacy Inspection Controlset“ bereitgestellt, der auf dem Themenkatalog des Self-Assessments mit den Bereichen Datenschutz-Governance und -prozesse aufsetzt.

DATENSCHUTZKONTROLLEN

Anhand des neu konzeptionierten Verfahrens für Organisationskontrollen wurden 2017 bereits erste Datenschutzkontrollen sowohl national als auch international durchgeführt. In Deutschland wurden die Telekom Mobility Solutions GmbH, congstar GmbH und Detecon International GmbH geprüft, international die T-Systems Nederland B.V.. Vermehrt zeigte sich hier, dass unzureichend Ressourcen für Datenschutzthemen bereitgestellt werden.

5. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Nach Art. 30 (1) DSGVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, zu führen. Die Deutsche Telekom kann aufgrund einer ähnlichen Vorschrift im bisherigen Bundesdatenschutzgesetz (BDSG) auf das von der Deutschen Telekom-IT geführte und entsprechend angepasste Dokumentationstool für die Unternehmens-IT-Architektur und IT-Compliance aufbauen. Dort sind bereits wesentliche Teile der erforderlichen Informationen abrufbar, da es schon bisher für die Erstellung der internen Verfahrensverzeichnisse in den deutschen Konzernunternehmen genutzt wurde. Group Privacy hat 2017 in Zusammenarbeit mit Kollegen der griechischen Konzerntochter OTE und der Deutschen Telekom–IT die sich aus der DSGVO ergebenden zusätzlichen Anforderungen an das Verfahrensverzeichnis definiert und umgesetzt. Seit Januar 2018 steht die DSGVO konforme Version des Verfahrensverzeichnisses allen Konzernunternehmen EU-weit zur Verfügung.

6. EIGENENTWICKLUNG EINER INTERNATIONAL EINSETZBAREN PSEUDONYMISIERUNGS- UND ANONYMISERUNGSLÖSUNG

Der „Enkroder“ ist eine von Group Privacy eigenentwickelte Software zur Pseudonymisierung und Anonymisierung von personenbezogenen Daten.
Die Pseudonymisierung wird mit der automatisierten und kryptografisch starken Ersetzung von Einzeldaten durch Zeichenketten unter Erhaltung von Formaten erzielt. Diese Ersetzung ist, solange der dafür benutzte Schlüssel existiert, vollständig umkehrbar. Daher ist der Enkroder ideal für Pseudonymisierungsprozesse geeignet.
Das Verfahren wurde am Lehrstuhl für IT-Sicherheit an der Ruhr-Universität Bochum unabhängig untersucht. Ein hieraus resultierendes kryptografisches Gutachten bestätigt die algorithmische Stärke des eingesetzten Verfahrens.
Die Software wurde zudem dem Datenschutzbeirat der Deutschen Telekom vorgestellt. Dieser sprach in einer Empfehlung aus, die Lösung sowohl intern als auch extern zu vermarkten. Darüber hinaus wurde das Projekt in 2017 in das Deutsche Telekom interne Förderprogramm UQBATE Scholarship aufgenommen.

Die Haupt-Anwendungs-Felder sind:
Data Ware House
Generierung von Testdaten
Missbrauchserkennung
Daten in und aus Tabellen (z.B. Excel)

Das Verfahren ist bereits an mehreren Stellen im Konzern im Einsatz (z.B. Data Warehouse Telekom Deutschland im Acquistion-Layer).
Das Verfahren erhält grundsätzlich den zugrundeliegenden Zeichensatz (Alphabet) und die Wortlänge der Daten. Dieses erlaubt den Erhalt simpler Strukturen wie z.B. Telefonnummern, IP-Adressen, ID-Strukturen und erhöht somit die Auswertbarkeit.
Unter anderem die Möglichkeit zur Verarbeitung verschiedenster internationaler Schriftzeichen (u.a. griechisch, kyrillisch, etc.) gewährleistet, dass der Enkroder auch für den internationalen Einsatz geeignet ist.

7. KONZERNDATENSCHUTZAUDIT

ERGEBNISSE DES KONZERNDATENSCHUTZAUDITS 2017

Group Privacy hat das Konzerndatenschutzaudit (KDSA) als stetiges und anerkanntes Instrument des Datenschutzes etabliert. 2017 wurden 30% der Beschäftigten im Konzern weltweit online befragt.
Ziel des Audits ist die Messung des allgemeinen Datenschutzniveaus der Telekom in Deutschland sowie von 36 internationalen Beteiligungsgesellschaften. Durch das Audit sollen grundsätzliche Verbesserungspotentiale erkannt und entsprechende Maßnahmen abgeleitet werden.

Das Konzerndatenschutzaudit 2017 zeigt, dass der Datenschutz bei der Deutschen Telekom funktioniert und stabil ist: Das Datenschutzniveau wird erneut auf hohem Wert bestätigt. Der Durchschnitt liegt konzernweit bei 75 % (70% in 2016) der erreichbaren Punkte (national 83%, international 62%). Im

Vergleich zum Vorjahr haben sich die Internationalen Einheiten in fast allen Punkten, teilweise auch deutlich, verbessert.

Um das Verbesserungspotential transparent aufzubereiten und Maßnahmen anzustoßen, werden den auditierten Einheiten entsprechende Ergebnisberichte zur Verfügung gestellt. Group Privacy wird den identifizierten Handlungsbedarf in den Einheiten und die Umsetzung von Verbesserungsmaßnahmen monitoren und mit Informationen, Beratung und Überprüfungen unterstützen.

In allen Einheiten, deren Awardwert unter Konzerndurchschnitt liegt, vereinbaren zudem die Geschäftsführer bzw. Führungskräfte gemeinsam mit dem jeweiligen Datenschutzansprechpartner eigenverantwortlich zusätzliche Maßnahmen zur Stärkung des Datenschutzniveaus.

8. GLOSSAR UND ABKÜRZUNGSVERZEICHNIS

BEGRIFF ODER ABKÜRZUNG	BEDEUTUNG
BCRP	Binding Corporate Rules Privacy
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
GPR	Group Privacy
PSA	Privacy and Security Assessment Verfahren
DSGVO	Datenschutz -Grundverordnung
OTC	Open Telekom Cloud
PSA	Privacy & Security Assessment
DTHS	Deutsche Telekom Healthcare Solutions
HfTL	Hochschule für Telekommunikation Leipzig
KDSA	Konzerndatenschutzaudit
TCDP	Trusted Cloud Datenschutzprofil
TKG	Telekommunikationsgesetz
TMG	Telemediengestz
NatCos	National Companies
OTE	Hellenic Telecommunications Organization S.A.
DT-IT	Deutsche Telekom IT

HERAUSGEBER:

Deutsche Telekom AG
Group Privacy – Dr. Claus– Dieter Ulmer, Konzerndatenschutzbeauftragter
53113 Bonn

Stand 12/2017| Änderungen und Irrtum vorbehalten

ERLEBEN, WAS VERBINDET.