Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

„Datenschutz by design - Projekte richtig aufsetzen“

bei Ringvorlesung zum Datenschutzzertifikat, Universität Frankfurt

online, 30. Mai 2023

Es gilt das gesprochene Wort

Sehr geehrte Frau Quintus,

sehr geehrte Damen und Herren,

I. [Einleitung]

ich freue mich, auch in diesem Jahr einen Beitrag zur Ringvorlesung „Datenschutz, Datensicherheit und ihre gesellschaftlichen Auswirkungen“ leisten zu können.
Ich will mich dabei in diesem Jahr einmal mehr auf die praktische Seite konzentrieren und anhand von Beispielen aus unserer Beratungs- und Kontrollpraxis aufzeigen, was in Sachen Digitalisierung in Deutschland gut oder schlecht läuft. Und was Sie beachten sollten, damit dieses Pendel in die richtige Richtung ausschlägt.

II. Unser Credo

Datenschutz und Datensicherheit müssen bei der Entwicklung von neuen Produkten, egal ob Hard- oder Software, von Anfang an mitgedacht und mitumgesetzt werden. Das ist das Credo meiner Behörde, das wiederhole ich in jedem Vortrag und bei jedem Gespräch und ich werde dies solange tun (müssen), bis es allen Entwicklern, Unternehmen und Verwaltungen in Fleisch und Blut übergegangen ist, bis sie es für ihr eigens Credo, für ihre eigene Idee halten. Warum?

Digitale Produkte, die ohne oder mit zu wenig Datenschutzstandards entwickelt werden, die einfach nur unter Wiederverwendung veralteter Module oder Verfahrensweisen entstehen, haben kurz vor oder nach der Inbetriebnahme immer dasselbe Problem: sie müssen nachgesteuert werden. Weil sonst Auflagen durch die Datenschutzbehörden bis hin

zum Stopp des Systems oder empfindliche Bußgelder drohen. Weil man sonst auch schadensersatzpflichtig werden kann.

Dies führt nicht nur zu zeitlichen Verzögerungen, sondern in aller Regel auch zu erheblichen Mehrkosten, eben weil es schwieriger und aufwendiger ist, „Nachzubessern“.

Wer nun glaubt, dass diese Erkenntnis, diese Tatsache dazu führt, dass der Datenschutz und die Datensicherheit vermehrt von Anfang mitbedacht und eingebaut werden, der irrt leider. Es ist erschreckend, wie oft wir bei Beratungen und Kontrollen feststellen müssen, dass selbst datenschutzrechtliche Standards, die seit über zwanzig Jahren gelten und eingehalten werden müssten, ignoriert und vergessen und vernachlässigt werden.

Wenn wir dann darauf hinweisen, dass Recht und Gesetz auch bei der Digitalisierung einzuhalten sind, fällt schnell der Spruch
„der Datenschutz ist schuld,
- dass wir nicht schneller sind
- Deutschland bei der Digitalisierung zurückfalle
- dass es teurer wird
- dass Täter nicht verfolgt werden können
- dass Kinderschutz im Netz nicht funktioniert
- dass Daten nicht besser in der Forschung genutzt werden können.“

Was soll ich sagen? Nichts davon stimmt, aber die plakativen Beschuldigungen klingen für Medien und zumindest Teile der

Öffentlichkeit vermeintlich plausibel. Ich habe auch nach über vier Jahren in meinem Amt noch kein einziges Beispiel vorgelegt bekommen, bei dem der Datenschutz etwas verhindert, verboten oder abgeschafft hat, was unseren europäischen Wertevorstellungen entspricht, obwohl ich unsere Kritiker immer wieder auffordere, mir Beispiele zu nennen. Fast immer geht es beim Datenschutz und der Datensicherheit auch nicht um das „Ob“, sondern um das „Wie“

Ich will also mal meinerseits einige Positiv- und Negativbeispiele anführen, um deutlich zu machen, worum es geht.

III. Digitalisierung im Gesundheitswesen und Elektronische Patientenakte

Das erste Beispiel, dass mein Haus jetzt bereits seit Jahren intensiv beschäftigt ist die elektronische Patientenakte, kurz ePA.
Als ich im Jahr 2003 als junger Bundestagsabgeordneter dafür gestimmt habe, eine elektronische Patientenakte einzuführen, habe ich mir nicht einmal im Traum vorstellen können, dass wir 20 Jahre später immer noch keine funktionierende ePA haben würden.

Theoretisch gibt es die ePA seit zwei Jahren, faktisch wird sie so gut wie nicht genutzt. Das liegt z.B. daran,
- dass noch immer nicht alle Arztpraxen und Krankenhäuser angeschlossen sind,
- dass noch immer nicht alle Daten, die darin gespeichert werden sollen,

mit dem System kompatibel sind,
- dass die Daten immer noch unstrukturiert als PDF gespeichert werden
- dass die gespeicherten Dokumente dann alle den gleichen Namen haben – „Dokument“
- dass noch immer nicht geklärt ist, welche älteren Patientendaten darin gespeichert werden und wie, obwohl das ja überaus sinnvoll wäre
- dass Patient:innen ohne Smartphone nicht auf die Daten zugreifen können

Das ist der Stand des Softwareprojektes nach zwanzig Jahren, die ersten fünfzehn Jahre davon übrigens ohne DSGVO ... Mich ärgert das so, weil eine gute ePA ein Riesengewinn für alle im Gesundheitsbereich wäre.

Ähnliches gilt für das **elektronische Rezept**. Die Krankenkassen haben es aber auch bis heute nicht geschafft, ihren Versicherten eine PIN für die elektronische Gesundheitskarte zukommen zu lassen, mit der sie sich in den Apotheken sicher autorisieren könnten. Stattdessen sollte Zwischenlösung genutzt werden, mit der die Daten aller anderen gesetzlichen Versicherten von über 18.000 Zugriffspunkten ohne Probleme hätten ausgelesen werden können. Weil die uns zur Prüfung vorgelegte Softwarelösung Authentifizierungszertifikate nicht einmal signiert hatte ...

Zusammen mit dem Digitalgesetz, in dem die ePA und das eRezept geregelt werden sollen, wird auch ein Forschungsdatennutzungsgesetz

auf den Weg gebracht werden. Mit diesem Gesetz soll geregelt werden, dass die Patientendaten aus der ePA anonymisiert auch für die Forschung genutzt werden können. Super-Idee eigentlich: Denn bisher scheitert eine solche Forschung in Deutschland daran, dass die Daten nicht bundesweit genutzt werden können, weil in jedem Land eigene Krankenhausgesetze gelten und die gesammelten Daten oft nicht kompatibel sind, weil keine Standards für Datenformate und Übertragen vorgegeben sind und jedes System sich abkapselt. Darum, und nicht um Anforderungen des Datenschutzes, geht der Lobbykampf im Hintergrund. Wir Datenschützer hatten bereits 2004 ein solches Gesetz vorgeschlagen.

Ich will aber nicht nur jammern, auch im Gesundheitsbereich haben wir durchaus auch positive Entwicklungen, wenn Projekte von Anfang an durch den Datenschutz begleitet werden. So ist sowohl beim Implantateregister als auch beim Organspenderegister gelungen datenschutzfreundliche Pseudonymisierungverfahren zu etablieren. Pseudonymisierung (und Anonymisierung) sind so entscheidend für gute IT-Projekte. Bei den Registern führt das dazu, dass weitere Daten zu einer Person hinzugefügt werden können und Erkenntnisse aus Forschung an Patient:innen zurückfließen können. Gleichzeitig können Forschende nicht direkt auf einzelne Personen zurückschließen und ein Abfluss der Daten an Dritte, die re-personalisieren könnten, unterbleibt.

Faustformel: Pseudonymisierung geht öfters als man denkt und ist sehr hilfreich

IV. Digitalisierung der Verwaltung

Ich könnte Ihnen unzählige Beispiele nennen, wo man unseren Rat nicht befolgt hat. Wo der Karren schon gegen die Wand gefahren wurde. Und da brauche ich mich nur in meinem privaten Umfeld umzuschauen.

Nehmen wir das Beispiel Digitalisierung von Prozessen und Formularen. Karren passt in diesem Kontext auch ganz gut. Einige von Ihnen kennen das sicher. Der lästige Gang zur KFZ-Anmeldestelle. Erst wartet man wochenlang auf einen Termin. Dann muss man sich als Berufstätiger schlimmstenfalls mit einem Zeitfenster mitten während der Arbeitszeit abfinden oder sich gar extra freinehmen. Und dann zieht man vor Ort brav seine Wartenummer und wartet und wartet und wartet....

Da kommt das weit angepriesene Angebot der Verwaltungen doch wie gerufen, diesen lästigen und zeitintensiven Papierkram online zu erledigen. Wunderbar habe ich mir gedacht, dann kann ich mein neues E-Auto bequem von zu Hause aus anmelden ... Hätte vielleicht auch funktioniert, wenn man bei den digitalen Anmeldeformularen auch berücksichtigt hätte, dass man ein Kennzeichen mit einem E am Ende haben will. Das funktioniert nämlich nicht, die Lösung wurde seit 2015 nicht angepasst. Ich glaube ja übrigens, dass das Problem dabei wieder so ein handgestrickter Schutz gegen Einschleusen von Code über Textfelder war. 90% der Softwareprojekte, die wir sehen, nutzt dabei nicht die sicheren, längst entwickelten Standards und gefährdet damit Systeme und sensible Daten.

Seien Sie bitte anders: Nutzen Sie den Stand der Technik

Wer denkt, dass das ein Ausnahmefall ist und die Digitalisierung in anderen Fällen von Anfang an mitgedacht wurde, den muss ich leider enttäuschen.

Wer beispielsweise ein Führungszeugnis beantragen möchte, der wird auch relativ schnell über die sogenannten digitalen Angebote der Verwaltung stolpern. Anstelle nämlich die Vorteile digitaler Lösungen vollumfänglich umzusetzen, hat man teilweise stupide analoge Formulare einfach in ein digitales Format übertragen. Gibt man beispielsweise bei dem Formular an, dass man keine weitere Staatsbürgerschaft eintragen lassen will, dann bekommt man noch zweimal die gleiche Frage gestellt. Grund ist nur, dass es im analogen Format drei Zeilen zur handschriftlichen Eingabe gab.

Bei Digitalisierung muss man sowohl den Verwaltungsvorgang als auch die Interaktion mit Bürger:innen und Unternehmen neu denken, um die Vorteile nutzen zu können. Als Bonbon kann man oft viel weniger Daten einsammeln und durch Einmalerhebung und richtige Identifizierung falsche Daten vermeiden.

Nutzen Sie das! Hinterfragen Sie den Prozess und bilden nicht einfach nur analoge Prozesse digital nach. Denn, „wer analog denkt, wird die

Vorteile der Digitalisierung nie verstehen“, las ich kürzlich und damit sind die Probleme bei der Digitalisierung der Verwaltung schon ziemlich genau beschrieben.

Das Zauberwort lautet in diesem Zusammenhang Onlinezugangsgesetz (OZG). Danach hatten sich Bund, Länder und Kommunen vorgenommen, auf der Grundlage des 2017 in Kraft getretenen OZG bis Ende 2022 rund 600 Verwaltungsleistungen für Bürgerinnen und Bürger online anzubieten. Dieses Ziel wurde krachend verfehlt, am Ende 2022 waren es gerade 101 Leistungen, die tatsächlich mehr oder weniger digital nutzbar waren.

Die Bundesregierung hat in der letzten Woche das Nachfolgegesetz OZG 2.0 vorgestellt, mit dem jetzt alles schneller und besser werden soll. Zentraler Bestandteil soll die Bund-ID als zentrales Bürgerkonto werden, mit der sich die Bürgerinnen und Bürger bei allen Verwaltungen von Kommunen, Ländern und dem Bund einloggen und mit ihnen kommunizieren können sollen.

Sie als Studentinnen und Studenten kennen die Vorstufe wahrscheinlich durch das Portal einmahlzahlung200.de, das auf dem gleichen Prinzip beruht. Es war so traurig: Im Jahr 2023 kriegt man statt aktueller Standards wirklich noch bei der Anlage eines digitalen Kontos Sicherheitsfragen wie „In welcher Stadt haben sich ihre Eltern kennengelernt“ ...

Deutschlandweit soll die ID privaten Nutzern über ein Bürgerkonto die Tore zur digitalen Verlängerung des Personalausweises oder der An- und Ummeldung eines Kraftfahrzeugs öffnen. Bis 2024 sollen mindestens 15 weitere Verwaltungsakte vollständig digital nutzbar sein, etwa Ummeldung, Baugenehmigung und Elterngeld.

Mit der gesetzlichen Verankerung des Once-Only-Prinzips sollen Nachweise für einen Antrag – zum Beispiel eine Geburtsurkunde – zukünftig auf elektronischem Wege bei den zuständigen Behörden und Registern mit Einverständnis des Antragstellers abgerufen werden können

Und durch die Gesetzesänderung sollen zukünftig alle Leistungen rechtssicher einfach und einheitlich mit der Onlineausweisfunktion des Personalausweises digital beantragt werden können; es ist keine händische Unterschrift mehr notwendig.

Problematisch an diesem Gesetzentwurf ist m.E. vor allem, dass wieder keine festen Fristen gesetzt werden, bis wann welche Leistungen umgestellt sein müssen. Das öffnet dem Verschiebebahnhof zwischen Bund, Ländern und Kommunen, wer bis wann umgestellt haben sollte, wieder das Tor, an dem schon das alte OZG gescheitert ist.

Ich lasse mich aber gerne diesmal vom Gegenteil überzeugen

Internetseiten des Bundes

Im Mai 2022 habe ich ein Verfahren zur Abhilfe wegen datenschutzrechtlicher Probleme im Zusammenhang mit dem Betrieb der Facebook-Fanpage für die Bundesregierung gegen das Bundespresseamt eingeleitet.

Bei der Fanpage (auch „Facebook-Seiten“) handelt es sich um eine Art Homepage, die durch Facebook publiziert wird. Der Inhalt stammt nicht von Facebook, sondern von den Betreiberinnen und Betreibern der Fanpage. Bei dem Besuch einer Facebook-Fanpage werden umfassend personenbezogene Daten über das Surfverhalten der Nutzerinnen und Nutzer gesammelt, um diese Informationen über Werbung zu monetarisieren oder sogar noch für andere Zwecke zu verwenden.

Diese Überwachung trifft nicht nur angemeldete Nutzerinnen und Nutzer von Facebook, sondern auch Personen, die kein Facebook Konto haben.

Mir ist die Bedeutung sozialer Netzwerke für die Öffentlichkeitsarbeit der Bundesbehörden (und natürlich auch privater Unternehmen) bewusst. Gleichwohl sind Behörden besonders gefordert, rechtskonform zu handeln. Die wichtige Aufgabe der Öffentlichkeitsarbeit kann nicht die Profilbildung und Verarbeitung personenbezogener Daten zu Marketingzwecken rechtfertigen. Daher und aufgrund ihrer Vorbildfunktion nehmen wir Datenschutzaufsichtsbehörden diese nun vorrangig in die Pflicht. Aber seien sie sicher. Auch Ihrem Start-Up würden wir so etwas nicht durchgehen lassen. „Ich verwende diese

Anwendung aber so gerne“ oder „die nutzen doch alle“ oder „ich kann mit diesen Daten aber so viel anfangen“ sind keine rechtliche Grundlage, personenbezogene Daten zu verarbeiten.

Mit Blick auf die Vorbildfunktion der öffentlichen Stellen des Bundes habe ich nach zwei Jahren Beratung mittlerweile eine erste Abhilfemaßnahme vorgenommen und mit Bescheid vom 17. Februar 2023 dem Bundespresseamt (BPA) bis auf weiteres die Verarbeitung personenbezogener Daten im Rahmen der von der Bundesregierung betriebenen Facebook-Fanpage innerhalb von vier Wochen nach Bekanntgabe dieses Bescheids durch Einstellen ihres Betriebs untersagt. Das BPA hat am 17. März 2023 gegen den Bescheid fristgerecht Klage vor dem Verwaltungsgericht Köln eingereicht. Die Klage hat aufschiebende Wirkung, sodass das BPA die Fanpage vorläufig bis zum Ausgang des gerichtlichen Verfahrens weiter betreiben kann. Auch Facebook selbst hat gegen den Bescheid Klage erhoben, wir warten also gespannt auf den Ausgang des Verfahrens.

Es sind aber nicht nur die Facebook-Fanpages der Bundesregierung, die ich kritisiere, sondern auch die „normalen“ Informations- und Aktionsseiten der Bundesministerien, über die wir uns täglich ärgern. Trotz immer neuer Bitten und Ermahnungen, auf Analyse-Tools und sonstige Tracker doch möglichst ganz zu verzichten, die Cookie-Banner datenschutzkonform auszugestalten, ändert sich am Grundproblem wenig bis nichts.

Bestehende Websites werden zwar mehr oder wenig nachgebessert, aber alle Relaunches werden offensichtlich auf die alten Seiten aufgesetzt oder mit den gleichen rechtswidrige Ergebnisse erzielenden Baukästen zusammengeklickt, sodass die bemängelten Punkte einfach immer weiter mitgeschleppt werden, statt einmal eine datenschutzgerechte Neugestaltung aufzusetzen und diese zu nutzen. Und die Qualität, die private Dienstleister:innen dabei erzielen, ist eher noch schlimmer als das, was in den Behörden selbst entsteht.

Überprüfen Sie ihre Baukästen, SDKs und Bibliotheken. Bereinigen Sie sie von datenschutzrechtswidrigen Elementen. Sie tun auch sich selbst einen Gefallen damit.

Wir werden nämlich in Zukunft verstärkt darauf achten, dass schon bei den Ausschreibungen für Aktionen und Wettbewerbe datenschutzrechtliche Standards eingehalten werden.

Was wir nicht mehr hinnehmen: Erst kürzlich mussten wir uns über einen Schulwettbewerb eines Ministeriums ärgern, in dem auch 8 – 13jährige Kinder dazu aufgefordert wurden, ihre Ergebnisse über Instagram oder TikTok zu posten, obwohl ein Bundesministerium wissen müsste, dass diese Dienste eigentlich erst ab 14 Jahren genutzt werden dürfen.

Es geht auch besser: Das Bundesinnenministerium hat angekündigt, dass es zukünftig Videos nicht mehr über Youtube sondern über einen eigenen Kanal einspielen möchte. Auch ist ein eigener „Bundesshop“

geplant, in dem die Apps der Bundesministerien heruntergeladen werden können, die Menschen also nicht mehr über den Google- oder Apple-Store gehen müssen. Was geht es auch Google oder Apple an, welche Apps, z.B. auch Apps, die bei bestimmten Erkrankungen helfen, heruntergeladen hat.

Solche Beispiele lassen mich hoffen, dass wir die Prozesse in den Griff kriegen.

P20

Um mal auf ein ganz anderes Feld zu schauen, dass eine solche Chance bietet: der BfDI begleitet beratend das Projekt P20 (Polizei 2020), ein IT-Großprojekt der Polizeibehörden des Bundes und der Länder.

Ein Entwicklungsschwerpunkt des letzten Jahres lag– wie auch im Vorjahr – darin, die unzähligen, zum Teil total veralteten Fallbearbeitungs-, die Vorgangsbearbeitungs-, und die Verbundsysteme zu vereinheitlichen. Aber auch zu dem gemeinsamen „Datenhaus“ der Polizeibehörden des Bundes und der Länder gibt es Projektfortschritte.

Zunächst liegt hier der Fokus auf der Auswahl einer geeigneten Technologie. In diesem Zusammenhang haben bereits erste Produkttests stattgefunden. Bis zum Ende des Jahres 2022 sollten drei Testinstallationen mit fiktiven Datensätzen befüllt werden. Ende 2024 ist dann die Verwendung von Echtdaten beabsichtigt. Mit dem Datenhaus wird auch ein Altdatenqualifizierungsdienst entwickelt. Dieser dient unter

anderem dazu, den Grundsatz der hypothetischen Datenneuerhebung umzusetzen bzw. automatisiert zu unterstützen. Das ist total spannend: Hätten die Daten für den Ermittlungszweck mit den gleichen Methoden erhoben werden dürfen, wie sie ursprünglich gewonnen wurden. Software unterstützt Grundrechte ...

Verzeichnis von Verarbeitungstätigkeiten

Meiner Beratungs- und Kontrollaufgabe unterliegt nicht nur P 20, sondern auch die anderen Anwendungen im BKA. Seit 2019 hatte ich das BKA um das Verzeichnis von Verarbeitungstätigkeiten gebeten. Da ein solches nicht vorgelegt wurde, habe ich gegenüber dem BMI als Fachaufsichtsbehörde eine Beanstandung ausgesprochen.

Für Sie gilt: Systeme, die personenbezogene Daten verarbeiten, müssen in ein solches Verarbeitungsverzeichnis, am besten direkt von Anfang an

Insgesamt ist P 20 ein Beispiel dafür, an welcher Stelle schon vor der Entwicklung eines Produkts klar ist, dass der Grundsatz "privacy by design" von zentraler Bedeutung ist und dass dies auch vom BMI nach langen Beratungen verstanden wurde. Wir sind jedenfalls nach wie vor zuversichtlich, dass hier am Ende eine datenschutzgerechte Lösung gefunden wird.

V. Wirtschaft

Zum Beispiel Mobilitätsdaten:

Die Europäische Kommission wie auch die Mitgliedstaaten der EU setzen große Hoffnungen auf die Wertschöpfungsmöglichkeiten in einer datengetriebenen digitalen Ökonomie. Die EU-Kommission hat dazu im Februar 2022 einen Verordnungsentwurf über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Data Act“) vorgelegt, um die wirtschaftliche Verwertung von Daten rechtssicher zu ermöglichen.

Gemeinsam mit meinen europäischen Kollegen habe ich dazu im Europäischen Datenschutzausschuss kritisch Stellung bezogen. Ausdrücklich sind davon auch die Daten aus den vielen smarten Gerätschaften des „Internet of Things (IoT)“ umfasst, die eine Fülle personenbezogener Daten produzieren, wenn sie von Personen genutzt werden oder sich in privaten Haushalten befinden. Dazu zählen grundsätzlich auch moderne vernetzte Fahrzeuge.

Speziell für Fahrzeuge hat die Kommission für das zweite Quartal 2023 eine spezialgesetzliche Vorschrift angekündigt, mit der Hersteller verpflichtet werden, Wettbewerbern einen fairen Zugang zu Daten, Funktionen und Ressourcen in Fahrzeugen zu ermöglichen.
Die datengetriebene Wertschöpfung setzt vertrauenswürdige Datenräume voraus.

In diesen können Anbieter ihre Daten anderen Teilnehmern des Datenraums für wohlbestimmte Verarbeitungszwecke auf Vertragsbasis zur Verfügung stellen, ohne einen Missbrauch durch unbefugte Dritte befürchten zu müssen.

Wichtig zu verstehen ist, dass viele dieser Daten personenbezogen sind, z.B. wenn sie fest mit einem bestimmten Fahrzeug verbunden sind, dass meist von derselben Person verwendet wird. Diese Daten sind aber nur dann für eine freie Nutzung weiterverwertbar, wenn sie zuverlässig anonymisiert wurden.

Das ist nicht einfach. Eine Fülle unterschiedlicher Daten oder in dichter zeitlicher Folge erhobene Daten sind in der Regel nur schwer zu anonymisieren sind. Anonymisierung wird eine Schlüsselkompetenz für ITler in der Zukunft, bereiten Sie sich darauf vor.

Wenn Sie nicht anonymisieren können, dann brauchen die Bürger:innen eine volle Nutzungskontrolle auch bei Sensor- und Fahrzeugdaten, wie wir sie aus der Welt der Smartphones und Tablets kennen oder zumindest erwarten. Ob die Fahrzeugsensoren auch für den Parkplatzfinder des Fahrzeugherstellers oder eines anderen Dritten genutzt werden, darf sich nicht der Kontrolle durch die Fahrzeugnutzenden entziehen. AGBS oder Vertragsklauseln sind dafür nicht der richtige Ort. In den zu schaffenden Datenräumen muss dem Schutz der Interessen von Privatpersonen die gleiche Priorität eingeräumt werden wie dem Schutz von Geschäftsinteressen.

Beispiel Smart Zum Home:
Der Rollout intelligenter Messsysteme nach Messstellenbetriebsgesetz hat begonnen. Stromzähler werden dadurch bei Einhaltung höchster Cybersicherheits-Standards fernauslesbar. Auch wird dadurch eine unterjährige Verbrauchserfassung möglich, die Verbrauchenden jederzeit einen Überblick über ihren Stromverbrauch gewährt. Die intelligenten Messsysteme sind auch für die Gas-, Wasser- und Wärmezählung einsetzbar, jedoch besteht dazu nur in Einzelfällen eine gesetzliche Verpflichtung. Überdies wird es durch eine Übergangsregelung möglich, etwa für die Wärmezählung die Privacy-Management-Funktionen des intelligenten Messsystems zu umgehen.

Mit der Digitalisierung im Energiesektor ergeben sich auch dort neue Möglichkeiten für digitale Geschäftsmodelle. Bei der Energiezählung im Haushalt wird nun nicht mehr nur ein Jahresarbeitswert erhoben, sondern im Fall elektrischer Energie ein Arbeitswert im Viertelstundentakt, also etwa 36.500 Arbeitswerte jährlich. Aufgrund des dadurch entstehenden Risikos für den Schutz der Privatsphäre durch Nutzerprofile wurde 2016 mit dem Gesetz zur Digitalisierung der Energiewende das Messstellenbetriebsgesetz (MsbG) geschaffen, mit dem Belange der Cybersicherheit und des Datenschutzes mustergültig berücksichtigt wurden.

Insbesondere die sogenannten Smart-Meter-Gateways (SMGW), die eine Vernetzung der Energiezähler mit dem Internet ermöglichen, setzen nicht nur Maßstäbe für die Cybersicherheit, sie haben auch zugleich die Funktion eines Privacy-Information-Management-Systems (PIMS). Sie

gewähren Verbrauchenden die größtmögliche Kontrolle über die Verwendung der zuweilen im Millisekundentakt aus intelligenten Zählern (Smart Meter) verfügbaren Daten. Für den Bereich der Messung elektrischer Energie wird mit dem MsbG datenschutzrechtlich umfassend geregelt, welche Stelle welche Daten für welchen Zweck erhalten und verarbeiten darf. Insbesondere regelt das Gesetz, dass für die Fernauslesung der Stromzähler nur intelligente Messsysteme verwendet werden dürfen, bei denen intelligente Zähler über ein nach den strengen technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) zugelassenes Smart-Meter-Gateway kommunizieren.

Leider erstrecken sich die für Verbrauchende vorteilhaften Regelungen nicht auf andere Sparten im Energiesektor. Gesetzliche Vereinfachungen zur Beschleunigung der Energiewende dürfen und brauchen auch nicht zu Lasten des Datenschutzes und der Cybersicherheit vorgenommen werden. Das Smart-Meter-Gateway ermöglicht Verbrauchenden grundsätzlich ein hohes Maß an Kontrolle über in ihrer Privatsphäre erhobene Zählwerte.

Die Möglichkeiten zur Kontrolle über die Verwendung der Zählwerte müssen auch vor dem Hintergrund aktueller Bemühungen der EU-Kommission zur Nutzbarkeit der Daten von datenproduzierenden IoT-Geräten (Internet of Things) für die Wertschöpfung in der Digitalökonomie ausgebaut werden. Dahingehend werde ich die Bundesregierung auch bei der anstehenden Novellierung des MsbG zur Beschleunigung der Energiewende beraten.

Was für Sie wichtig ist: Verschlüsselung und Transparenz. Need to know. Das sind Prinzipien für Datenschutz und Datensicherheit by design.

Zum Beispiel Telekommunikation:
Eines der besten Beispiele dafür, wie teuer eine nachträgliche Implementierung von datenschutzgerechten Funktionalitäten sein kann, betraf die IT-Systeme eines großen Mobilfunkanbieters. Diese IT-Systeme waren systemseitig nicht auf die rechtskonforme Löschung personenbezogener Daten ausgelegt. Misslich: Einer der eklatantesten Punkte betraf die Löschung der Bestandsdaten ehemaliger Kunden. Die Firma konnte - weil die Systeme vorher kreuz und quer verbunden waren -, nicht einmal nachvollziehen, ob Kundendaten tatsächlich gelöscht worden waren, weil sie an anderer Stelle dann doch wieder auftauchten.

Diese Funktionalität musste dann teuer, sehr teuer nachimplementiert werden. Diesen Prozess hat mein Haus fast zehn Jahre lang begleitet, bis tatsächlich alles so funktionierte, wie es sollte. Meine Rede: Nachbessern ist teuer und zeitaufwendig.

Hätte die Firma sich nicht an die Auflagen gehalten, hätte ich das System stillgelegt. Wegducken und totstellen funktioniert gegenüber Datenschutzaufsichtsbehörden also nicht.

Zum Beispiel KI
Künstliche Intelligenz (KI) dringt mit großer Entwicklungsgeschwindigkeit

in viele Wirtschafts- und Lebensbereiche vor. Hierbei nimmt aktuell die sog. generative KI eine Vorreiterrolle ein. Das muss ich gegenüber Zuhörer:innen wie Ihnen kaum erwähnen.

Angesichts vielfacher potentieller Lenkungs- und Entscheidungswirkungen generativer KI auf den Einzelnen als Individuum sowie die Gesellschaft als Ganzes verlangt sie allerdings zum Schutz der Freiheitlich Demokratischen Grundordnung, speziell zum Schutz der Grundrechte und des demokratischen Gemeinwesens, nach einem vorausschauenden Rechtsrahmen. Der übrigens mehr ist als DSGVO und AI Act.

Dieser Rechtsrahmen muss Innovation ermöglichen und schützen, kritische Verarbeitungen allerdings wirkungsvoll reglementieren und im Einzelfall sogar ausschließen. Dies gilt besonders auch zum Schutz des Grundrechts auf informationelle Selbstbestimmung.

Generative KI kann durch die Verarbeitung personenbezogener Daten erhebliche Auswirkungen haben. Ich habe zuletzt einmal Chat GPT gebeten, mir meinen Lebenslauf aufzuschreiben und war durchaus überrascht, was ich so alles in den letzten Jahrzehnten gemacht haben soll. Denn abgesehen von meiner aktuellen Tätigkeit lag die KI bei wirklich allen Punkten daneben: vom falschen Geburtsort über das vermeintliche Jura-Studium bis hin zum nie existenten Landtagsmandat – alles frei assoziiert, dafür aber mit enormer Detailverliebtheit ausgeschmückt! Dass ich einmal selbst in einer KI-

Forschungseinrichtung gearbeitet hatte, verschwieg das Programm dagegen lieber.

In meinem Fall sorgt das eher für Erheiterung. Was aber ist bei falschen Assoziationen bei Informationsauswertung in Sicherheitsbehörden oder einer falschen Zusammenfassung der Lebensläufe und Fähigkeiten von Bewerberinnen und Bewerbern um einen Job? Oder eine Versicherung? Oder eine Wohnung? Von der Gefahr einer Aufdeckung sensibler Daten aus dem Trainingssatz des Systems durch gezielte Fragen an das System selbst und andere Risiken ganz zu schweigen.

Generative KI braucht daher eine grundrechtliche Folgenabschätzung, gerade auch aus Datenschutzsicht. Von der Datenakquise bis zur Nutzung. Mit unterschiedlichen Haftungen auf den unterschiedlichen Ebenen, vom Anbieter des Fountain Modells bis hin zu den Anwendenden.

Die Regelungen der Datenschutzgrundverordnung sind ein guter Ausgangspunkt für einen sachgerechten, wenn auch ausbaufähigen Rechtsrahmen für die Verarbeitung von personenbezogenen Daten im Kontext von KI. Angesichts erheblicher Grundrechtsgefährdungen bedarf es spezifischerer Vorgaben, einschließlich einer grundrechtsbezogenen Kritikalitätsbetrachtung, die auch Platz und Freiheit schafft für unbedenkliche Anwendungen.

Die Überwachung dieser Vorschriften im Bereich der Verarbeitung personenbezogener Daten sollte übrigens sachgerecht bei den

Datenschutzbehörden liegen. Ich bin zuversichtlich, dass wir mit unserer Expertise hier einen entscheidenden Beitrag liefern können. Wir wollen KI rechtssicher und sicher nutzbar machen helfen.

Ich erwähne dass auch, um Ihnen zu zeigen, welche spannenden Jobs es bei uns gibt: KI-Aufsicht, Beratung im Gesundheits- und Telekommunikationssektor, Einblick in den Maschinenraum von Polizeibehörden und Geheimdiensten. Und das mit einer durchaus anständigen Bezahlung und flexiblen Arbeitsmöglichkeiten.

VI. Schlussbemerkung

Ich habe heute einmal bewusst auch ein paar Beispiele aus der Beratungspraxis meines Hauses ausgewählt, die nicht so sehr im Mittelpunkt der Berichterstattung stehen, die uns aber alle betreffen oder betreffen werden.

Ich hoffe, dass ich damit deutlich machen konnte, warum unser Credo „Datenschutz von Anfang an mitdenken“ so wichtig für eine gute gesellschaftliche aber auch wirtschaftliche Entwicklung ist und ich würde mich freuen, wenn wir Sie alle dabei jetzt und in Zukunft als aktive Mitstreitende an unserer Seite habe.

Ich danke Ihnen für Ihre Aufmerksamkeit und freu mich auf eine angeregte Diskussion.