



BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Keynote

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Aktuelle Entwicklungen im Datenschutz“

bei den 16. Praxistagen Datenschutz

Köln, den 9. Februar 2023

Es gilt das gesprochene Wort

Sehr geehrter Herr Hartz,
sehr geehrte Damen und Herren,
ich danke Ihnen für die Einladung.

Wir befinden uns aktuell mitten in der 5. Jahreszeit. Ab der nächsten Woche erreicht der Karneval seinen Höhepunkt. Insbesondere für die Rheinländer unter uns steht damit wieder eine „jecke Zick“ bevor. Und wie heisst es doch so schön im Kölschen Grundgesetz: „Et hätt noch immer jot jejange“.

I. Einleitung

Diesen Glaubenssatz würde ich nur allzu gern auf den Datenschutz übertragen. Leider geht dies aber an der Lebenswirklichkeit so ziemlich vorbei. Und auch das Credo, dass man aus den Fehlern der Vergangenheit lernen soll, wird mir im Datenschutz noch viel zu selten umgesetzt.

Die Corona-Krise hat viele Versäumnisse aufgedeckt. Neue Technologien drängen auf die Märkte. Aber auch politische Bestrebungen und die immer weiter steigende Macht internationaler Technologiekonzerne sind Treiber für Veränderungen.

Viel zu spät hat man dabei einen Blick auf die hinkende Digitalisierung bei uns geworfen:

- in der Wirtschaft
- in den Verwaltungen
- am Arbeitsplatz
- im Bildungsbereich.

Die Mängel waren dabei schon lange vorher erkennbar. Sie wurden aber unterschätzt und als unbequem zur Seite geschoben. Investitionen wurden verschoben. Auch weil die für eine erfolgreiche Digitalisierung notwendige Arbeit in den Maschinenräumen abseits des Sonnendecks wenig Glamour und auch keine schnelle Umsatzrendite bietet. Die so verschleppte Digitalisierung rächt sich nun.

Und dann gibt es da ja auch noch den Datenschutz. Der wird gerne mal von den Verantwortlichen zu Beginn vergessen und am Ende zum Sündenbock gemacht. Die Ausrede Datenschutz stimmt dabei vermutlich genauso häufig wie die in Witzen verwendete Schutzbehauptung, der Hund habe die Hausaufgaben aufgefressen.

Das alles bräuchte ich Ihnen als Datenschutzexpertinnen und –experten eigentlich gar nicht zu erzählen. Aber wir müssen uns gemeinsam diesen Vorurteilen und den damit verbundenen Herausforderungen stellen.

Lassen Sie uns also gemeinsam einen Blick auf die aktuellen Entwicklungen im Datenschutz werfen. Fangen wir mit dem großen Ganzen an.

II. Europäische Digitalrechtsakte

Erst in der letzten Woche war ich zum Abschluss meines Vorsitzes der Datenschutzkonferenz Gastgeber der Veranstaltung zum Europäischen Datenschutztag 2023 in Berlin. Das Thema war: „Der Data Act und die Zukunft des Datenschutzes“

Neben dem Data Act und den auf ihn folgenden spezifischen Regelungen, wie z.B. dem European Health Data Space, sind noch eine ganze Reihe weiterer europäischer Digitalrechtsakte Teil der EU-Datenstrategie. Wir denken hier an den Data Governance Act, den Digital Markets Act, den Digital Service Act und die Regulierung beim Einsatz künstlicher Intelligenz, sprich dem Artificial Intelligence Act.

Dieser bunte Strauß an Regulierungsansätzen wird die Unternehmen, die Bürgerinnen und Bürger, die Politik und die Datenschutzbeauftragten sowie die Aufsichtsbehörden künftig fordern.

Bis jetzt hat noch keiner wirklich ein genaues Verständnis dafür, wie die Interaktion der einzelnen Rechtssetzungsakte untereinander, der entstehenden Aufsichtsbehörden und –gremien, aber auch die Interaktion mit der Datenschutzgrundverordnung, gelingen soll. Und was es bringen wird an Veränderungen, an Verschiebungen und neuen Handlungsfeldern.

Aus meiner Sicht steht dieses Regelungspaket auch mit einem neuen Narrativ der Europäischen Union im Raum. Es geht um die breite Nutzung von Daten. Qualitativ sowie quantitativ. Es geht um Massendatenverarbeitung. Es geht um Daten, eben auch personenbezogene Daten, die als Rohstoff und Grundlage für wirtschaftliches Wachstum genutzt werden sollen.

Die wirtschaftspolitische Zielsetzung ist klar. Die Datenwirtschaft in der EU soll schon im Jahre 2025 mit über 800 Milliarden Euro fast 6 Prozent der Wirtschaftsleistung ausmachen.

Wenn Bürgerinnen und Bürger mit ihren personenbezogenen Daten als Rohstoff für Wirtschaftswachstum fungieren sollen, dann müssen die Aufsichtsbehörden umso konsequenter die Persönlichkeitsrechte schützen können.

Wir sehen neben den wirtschaftspolitischen Zielen der EU auch die Gemeinwohlaspekte, die hinter den Digitalrechtsakten stehen. Daten können helfen, existentielle Herausforderungen zu bewältigen. Zum Beispiel in den Bereichen Bildung, Forschung, der Klimakrise und der Gesundheitsversorgung.

Erfreulich ist, dass die EU-Institutionen bisher datenschutzpolitisch Flagge gezeigt haben, allen voran das EU-Parlament. Bekenntnisse zur DSGVO und dem damit erreichten Schutzniveau werden bisher weitgehend durchgehalten.

Was uns als Datenschutzaufsichtsbehörden natürlich ebenfalls brennend interessiert, ist die Aufsichtsstruktur. Wir wollen nicht, dass das, was wir als Aufsicht und Durchsetzung aus der DSGVO kennen, unter die Räder kommt. Diese Entwicklung gilt es weiter kritisch zu beobachten und zu begleiten.

III. Internationaler Datenverkehr

Bleiben wir auf dem internationalen Parkett.

In einer global vernetzten Welt muss es ungeachtet der Unterschiede in den nationalen und regionalen Rechtsordnungen und den Unterschieden in den Datenschutzregelungen einen freien, sicheren und vertrauenswürdigen Datenverkehr geben, zumindest zwischen den liberalen Demokratien dieser Welt als gemeinsamer digitaler Innovationsraum.

Das ist Voraussetzung für Vertrauen in die digitale Transformation, in digitale Dienste und Geschäftsmodelle, damit diese genutzt werden oder überhaupt erst entstehen können. Ohne einen solchen gemeinsamen Raum sinkt aber eben auch der Innovationsdruck. Dann hätten Verbraucherinnen und Verbraucher sowie Unternehmen weniger Wahlmöglichkeiten.

Deshalb arbeiten wir auch über die europäische Ebene hinaus mit internationalen Datenschutzaufsichtsbehörden an einem hohen Schutzniveau.

Hierzu wurde der sog. G7-Roundtable der Datenschutzbehörden ins Leben gerufen. Im Rahmen dieses Roundtable haben wir eine engere Zusammenarbeit zwischen den Datenschutzbehörden der G7 Staaten im digitalen Zeitalter vereinbart. Im letzten Jahr hatte ich parallel zu Deutschlands G7-Präsidentschaft den Vorsitz des Roundtable

übernommen und gebe diesen dieses Jahr an die Kollegin in Japan weiter.

Von besonderer Bedeutung war und ist dabei das Leitthema "Data Free Flow with Trust" – kurz DFFT. Eine gemeinsame Sichtweise der Datenschutzaufsichtsbehörden in Europa, Japan und Nordamerika ist dafür eine gute Grundlage. Daher habe ich mich sehr gefreut, dass unsere Kolleg:innen aus den USA, u.a. der FTC, unsere Sichtweise, dass Datenminimierung und Zweckbindung, Verhältnismäßigkeit staatlicher Zugriffe auf Daten und eine unabhängige Kontrolle unbedingte Voraussetzung ist, massiv unterstützen und von sich aus zum Thema für die Abschlusserklärung gemacht haben. Das gleiche gilt für die Kolleg:innen aus Japan und Kanada. Damit setzen wir denen, die die europäische Sichtweise auf Datenschutz als Wirtschaftshemmnis darstellen, klare Fakten entgegen.

Technologische Entwicklungen, Innovationen und der immer bedeutendere internationale Datentransfer müssen mit der Einhaltung hoher Datenschutzstandards einhergehen.

Dazu brauchen wir nicht nur übergreifende Regulierungsansätze zwischen Datenschutz- und anderen Behörden, wie z.B. Wettbewerbs- und Kartellbehörden. Wir brauchen vor allem eine Verständigung darüber, in welchem Ausmaß Zugriffe von Sicherheitsbehörden auf Daten in den globalen Kommunikationsnetzwerken als verhältnismäßig zu tolerieren sind. Dabei müssen stets die Rechte der Betroffenen eine wichtige Rolle spielen.

Z.B. durch eine unabhängige Kontrolle und gerichtliche Überprüfbarkeit der staatlichen Zugriffe. Denn davon hängt maßgeblich das Vertrauen der Menschen und der Wirtschaft in neue Technologien und die globale Digitalwirtschaft ab.

Wie die G7-Digitalminister werde ich intensiv dafür, dass zwischen Unternehmen und Einrichtungen in den demokratisch regierten Staaten dieser Erde personenbezogene Daten unter Beachtung der jeweils geltenden nationalen Regeln frei ausgetauscht werden können. Um wirtschaftlichen Wohlstand zu ermöglichen, wissenschaftlichen Austausch zu fördern und auch ein Gegenmodell zu China & Co. zu schaffen.

IV.OZG und Registermodernisierung

Lassen Sie uns nun einen Blick auf die neuesten Entwicklungen auf nationaler Ebene werfen.

Die Digitalisierung unserer Arbeits- und Lebenswelt hat bekanntlich nicht erst zu Pandemiezeiten begonnen. Aber unser Land hat hier seine Lektion erstmals bitter lernen müssen. Und zwar wie weit wir in Deutschland in Sachen Digitalisierung – insbesondere auch im öffentlichen Bereich – hinterherhinken.

Ich spreche hier nicht von ratternden Faxgeräten oder händisch geführten Excel-Tabellen in den Gesundheitsämtern. Die sind auch das Ergebnis der drastischen Einsparungen in diesem Bereich.

Ich spreche vielmehr von den gesteckten Zielen und deren tatsächlicher Umsetzung: Beispiel Onlinezugangsgesetz (OZG).

Bund, Länder und Kommunen haben sich 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, nach Schulnoten-Mathematik müsste man ein "ungenügend" geben, es reichte noch nicht einmal für ein „mangelhaft“.

Und wie steht es mit der Registermodernisierung?

Die Registermodernisierung ist bekanntermaßen eng mit dem OZG verknüpft. Denn für eine digitale Bereitstellung von Verwaltungsleistungen braucht es elektronische geführte Datenbestände und die Vernetzung bestehender Registerstrukturen.

Die aktuellen Regelungen zur Umsetzung der Registermodernisierung unter Rückgriff auf die Steuer-ID als übergreifendes Ordnungsmerkmal sind nach wie vor mit erheblichen datenschutz- und verfassungsrechtlichen Risiken verbunden. Der Gesetzgeber muss hier das Risiko der missbräuchlichen Zusammenführung personenbezogener Daten aus unterschiedlichen Registern begrenzen.

Wenn die Digitalisierung der Verwaltung erfolgreich vorangetrieben werden soll, dann muss sie auf einem rechtssicheren Fundament stehen. Ein universeller Identifikator wie die Steuer-ID, der mit dem

hohen Risiko behaftet ist, nach einem jahrelangen Prozess vom Bundesverfassungsgericht verworfen zu werden, hat das Potential, die digitale Verwaltung in Deutschland womöglich wieder um Jahre zurückzuwerfen.

Dieses Damoklesschwert schwebt aktuell über der Registermodernisierung. Ich sehe hier daher erheblichen gesetzlichen Nachbesserungsbedarf. Dies wird aktuell, auch unter Beteiligung meines Hauses, nochmal geprüft. Ich empfehle dringend, es den seit so vielen Jahren erfolgreichen deutschen Biathleten nachzumachen, wir sind ja noch mitten im Winter: Wenn die ersten Schüsse danebengingen und nun viele Strafrunden oder –minuten drohen, dann muss man einmal mit dem Gewehr absetzen, durchschnaufen und dann wieder neu zielen, abdrücken und ... treffen.

V. Datenschutz als Wettbewerbsvorteil

Wir haben also gerade gesehen, dass wir in Deutschland bei der Digitalisierung arg zurückliegen.

Lassen Sie uns daraus eine Chance machen. Die Chance nämlich, dass wir bei den zu entwickelnden, notwendigen Prozessen und Softwarelösungen den Datenschutz – und natürlich die IT-Sicherheit – von Anfang an mitdenken und „einbauen“. Das wäre wirtschaftlich und das wäre vorausschauend.

Ich bekenne mich dazu, Datenschutz als Innovationsförderer zu verstehen. Eine – wie ich weiß – nicht ganz unumstrittene Position. Aber ich möchte an dieser Stelle dafür werben.

Erfolgreiche Digitalisierung setzt Vertrauen voraus. Wir sollten den europäischen Datenschutz als gute gestalterische Leitplanken für einen fairen Interessenausgleich in einem globalen Datenökosystem schätzen.

Unser Ziel sollte es sein, weltweit Marktführer bei sicheren und datenschutzkonformen Produkten und Dienstleistungen zu werden. Datenschutzkonforme Produkte „Made in Europe“ könnten sich als positives Differenzierungsmerkmal am Markt etablieren.

Warum? Mit Blick auf den Datenschutz haben wir in Europa einen Erkenntnis-, einen Regelungs- und damit Wettbewerbsvorteil. Diese Potenziale müssen wir nutzen und positiv vermarkten. Wir verfügen mit der Datenschutzgrundverordnung und unserem nationalen Datenschutzrecht über einen innovativen Rechtsrahmen mit klaren Leitplanken und Handlungsanweisungen. Um diesen Rechtsrahmen werden wir beneidet. Die Datenschutzgrundverordnung wird weltweit als Referenz und Blaupause für eigene Rechtsvorgaben herangezogen, in Korea, Japan, Mexiko, Indien und in US-Bundesstaaten, eventuell bald auch auf Bundesebene der USA. Zuletzt sogar in China, wenn auch aus anderen Gründen.

Datenschutz und Datensicherheit müssen als wichtige Erfolgsfaktoren wahrgenommen werden.

Beides sind großartige Qualitätsmerkmale im globalen Markt. Datenschutz muss daher von Anfang an als Teil der „DNA“ eines jeden Produkts und einer jeden Dienstleistung mitgedacht werden. Es kann doch nicht sein, dass jetzt die US-Unternehmen, mehr oder weniger glaubwürdig, damit anfangen, Datenschutz als Unterscheidungsmerkmal zur Konkurrenz zu benutzen, während die deutsche Wirtschaft darüber klagt, dass sie ein Grundrecht einhalten muss.

Es ist daher umso wichtiger, dass wir dieses Potential erkennen. Lassen Sie uns daher am Ball bleiben und für den Datenschutz als Wettbewerbsvorteil werben!

VI. Beschäftigtendatenschutz

Auch in das Thema Beschäftigtendatenschutz kommt derzeit Bewegung rein.

Als Mitglied des unabhängigen und interdisziplinären Beirats zum Beschäftigtendatenschutz habe ich mich stets für weitgehende Regelungen im Beschäftigtendatenschutz eingesetzt. Mit dem Abschlussbericht von Januar 2022 hat der Beirat im Ergebnis die Notwendigkeit eines eigenständigen Beschäftigtendatenschutzgesetzes festgestellt.

Auch die Datenschutzkonferenz fordert seit Jahren die Schaffung eines Beschäftigtendatenschutzgesetzes. In ihrer EntschlieÙung von April 2022 hat sie klargestellt, dass gerade jetzt gesetzgeberischer Handlungsbedarf besteht.

Lassen Sie mich drei Aspekte hervorheben, warum das so ist:

1. Die immer schnellere Digitalisierung der Arbeitswelt ist Realität. Der aktuelle Rechtsrahmen wird dem leider nicht mehr gerecht. Es braucht die Schaffung klarer und bestimmter Rechtsgrundlagen, die den Beschäftigten einen hinreichenden Schutz ihrer Persönlichkeitsrechte bieten. Denn im Beschäftigungs- und Bewerberverhältnis fallen sehr viele aussagekräftige Daten an. Die Beschäftigten sind wegen ihres Abhängigkeitsverhältnisses in vielen Fällen besonders schutzbedürftig.
2. Es besteht massive Unsicherheit, welche technischen Neuerungen im Beschäftigungsverhältnis in welcher Weise rechtlich zulässig sind und welche nicht. Und wo liegen die Grenzen? Denken wir hier etwa an den Einsatz algorithmischer Systeme, einschließlich künstlicher Intelligenz.
3. Und drittens: Um die Chancen moderne Technik am Arbeitsplatz angemessen nutzen zu können, müssen die damit einhergehenden weitreichenden Möglichkeiten der Leistungs- und Verhaltenskontrolle begrenzt werden.

Auch die Bundesregierung hat im Koalitionsvertrag festgelegt, dass sie Regelungen zum Beschäftigtendatenschutz schaffen will, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen.

Nach Auskunft der Bundesregierung soll nunmehr ein Referentenentwurf erarbeitet werden. Im Vorfeld werden dazu derzeit Eckpunkte erarbeitet.

Ich bin zuversichtlich, dass sich in diesen Eckpunkten und den sich anschließenden gesetzlichen Regelungen nicht nur die Inhalte des Beiratsberichts, sondern auch die Punkte wiederfinden werden, die die Datenschutzkonferenz in ihrer Entschließung aus April 2022 aufgeführt hat.

Die technische Entwicklung und die Digitalisierung der Arbeitswelt macht eine Reform des Rechtsrahmens erforderlich.

Nicht nur auf Seiten der Beschäftigten, der Gewerkschaften und der Betriebsräte, sondern auch von Seiten der Unternehmerinnen und Unternehmer nehme ich ein Bedürfnis für klare und nachvollziehbare und rechtssichere Neuregelungen zum Beschäftigtendatenschutz wahr. Aus meiner Sicht besteht in dieser Legislaturperiode erstmals die große Chance, dies auch umzusetzen.

VII. TTDSG-Novelle

Bleiben wir bei den erfreulichen Entwicklungen. Erst kürzlich hat der Europäische Datenschutzausschuss (EDSA) seinen Abschlussbericht der Task Force Cookie-Banner vorgelegt. Die Ergebnisse entsprechen zum größten Teil dem, was wir in Deutschland bereits auf nationaler Ebene in der Orientierungshilfe Telemedien der DSK festgehalten haben, auch wenn wir etwas umfangreicher gearbeitet haben.

Wir erinnern uns: Ende 2021 ist das Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Das Gesetz regelt unter anderem den Schutz der Vertraulichkeit und Privatsphäre bei der Nutzung von Webseiten, Messengern oder auch Smart-Home-Geräten.

Der Einsatz von Cookie-Bannern gehört für uns mittlerweile zum durchaus ärgerlichen Alltag. Bei den meisten Webseiten springt uns beim Öffnen ein Cookie Banner entgegen, das für die Verarbeitung unserer personenbezogenen Daten unsere Einwilligung will, selbst bei Notfall-Infoseiten der Bundesregierung, zumindest bis der BfDI eingreift.

Eine gut gemachte und faire Internetseite benötigt aus meiner Sicht kein Cookie-Banner, weil sie nur technisch notwendige Cookies verwendet. Wollen Werbetreibende aber unbedingt auch personenbezogene Daten sammeln, dann dürfen sie sich eine Einwilligung dafür nicht mit unfairen Mitteln erschleichen.

Auch nach draußen: Cookie-Banner heißt, da will jemand mehr über sie wissen als für die Funktionalität der Webseite/Dienstleistung notwendig ist.

Umso mehr freue ich mich, dass ich mich mit meinen Kolleginnen und Kollegen im EDSA nun auf eine einheitliche Linie in der Aufsicht einigen konnte. Anbieter, die weiterhin nicht diese Anforderungen erfüllen, werden mit empfindlichen Geldbußen rechnen müssen. Und ich darf in diesem Fall darauf hinweisen, dass es automatische Tools zur Entdeckung solcher Verstöße gibt.

Aber dem nicht genug. Der EDSA hat im letzten Monat außerdem einen Bericht zu seiner ersten koordinierten Durchsetzungsmaßnahme veröffentlicht. Es ging dabei um die datenschutzkonforme Nutzung von Cloud-Diensten bei öffentlichen Einrichtungen. Fast 100 öffentliche Einrichtungen aus dem europäischen Raum wurden in die Nachforschungen einbezogen, darunter etliche deutsche Einrichtungen auf Bundes- und Landesebene. Auch damit schaffen wir eine europaweit einheitliche Linie.

Ich kann es gar nicht oft genug betonen – und ich werde hier auch nicht müde - aber auch und gerade bei Cloud-Projekten muss der Datenschutz von Anfang an mitgedacht werden. Ich berate die Bundesregierung beispielsweise zum Thema souveräne Cloud, unter anderem in den Gremien des IT-Rats und des IT-Planungsrats. Gerade mit Blick auf die Schwierigkeiten des internationalen Datentransfers bei Cloud-Projekten ist der Datenschutz ein wichtiger Grundpfeiler. Die Anforderungen an eine souveräne Cloud gehen dabei natürlich über eine DSGVO-Konformität hinaus.

Alles in allem nähern uns hier also insgesamt einer noch einheitlicheren Aufsicht in diesen Bereichen, national, auf EU-Ebene und – zumindest ansatzweise – auch auf internationaler Ebene. Die ersten Zertifizierungen auf nationaler und europäischer Ebene helfen dabei auch sehr.

VIII. Orientierungshilfen

Jetzt habe ich eine ganze Reihe von aktuellen Datenschutzthemen angesprochen. Einen wesentlichen Aspekt möchte ich allerdings noch hervorheben. Bei den ganzen verschiedenen Themen bemühen wir uns, immer auch die Praxis im Blick zu haben.

Und damit wollen wir Sie im Blick behalten: die Datenschutzbeauftragten aus allen Bereichen der Wirtschaft und der öffentlichen Verwaltung, die Anwenderinnen und Anwender, die Datenschutzexpertinnen und –experten. All diejenigen, die die Themen an vorderster Front an den Mann bzw. die Frau bringen und umsetzen müssen.

Wir Aufsichtsbehörden lassen Sie bei dieser Aufgabe nicht allein. Wir arbeiten mit Hochdruck an Orientierungshilfen, Leitlinien, Entschliefungen oder FAQs, die Sie in Ihrer täglichen Arbeit unterstützen. Und das sowohl auf nationaler wie auch auf internationaler Ebene. Und das mit Bezug auf aktuelle Themen, die Ihnen gerade unter den Nägeln brennen.

Lassen Sie mich ein paar Beispiele nennen:

Da gibt es zum Beispiel die schon erwähnte Orientierungshilfe Telemedien. Ich habe gerade bereits über die aktuellen Entwicklungen beim Betrieb von Webseiten gesprochen. Die DSK hat in diesem Kontext ein öffentliches Konsultationsverfahren durchgeführt. Aufgrund der Bewertung der eingegangenen Stellungnahmen haben wir die Ursprungsversion der Orientierungshilfe Telemedien angepasst.

Sie haben Fragen zu Facebook Fanpages? Dann werfen Sie doch mal einen Blick in die FAQs zu Facebook Fanpages der DSK. Da finden Sie Antworten auf Fragen, wie etwa: Was brauche ich für einen datenschutzkonformen Einsatz von Facebook Fanpages? Bestehen die gleichen Probleme auch bei anderen Social-Media-Diensten, wie zum Beispiel Instagram, Twitter, TikTok? Gelten die Hinweise der DSK nur für öffentliche Stellen? Und, und, und ...

Sie wollen wissen, ob Sie Microsoft 365 in Ihrem Unternehmen oder Ihrer Behörde überhaupt noch datenschutzkonform betreiben können? Dann ist vielleicht die Festlegung der DSK zu Microsoft 365 etwas für Sie. Ähnliches haben wir auch zu Windows, hier Windows 10, erarbeitet.

Vielleicht haben Sie aber auch Fragen zur Auftragsdatenverarbeitung? Hier hat der EDSA Leitlinien als Auslegungshilfen zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO veröffentlicht.

Ich lade Sie daher herzlich dazu ein: Nutzen Sie die zahlreichen Angebote! Die Unterlagen stehen Ihnen auf den jeweiligen Webseiten der Institutionen frei zur Verfügung.

Und sagen Sie uns, was noch wo fehlt.

IX. Datenschutzsensibilisierung

Ich bin der Überzeugung, dass man mit der Sensibilisierung für Datenschutzthemen nicht früh genug anfangen kann. Bereits in unserer Kindheit manifestieren sich Wertvorstellungen. Wertvorstellungen, die Teil unseres Handelns bleiben. Wertvorstellungen, die unsere Entscheidungen beeinflussen. Wertvorstellungen, die uns für gewisse Themen sensibilisieren können.

Unsere Kinder und Jugendlichen bewegen sich heute schon sehr früh im Netz. Sie spielen, surfen oder schauen Videos an. Zuerst auf den Geräten der Eltern, aber auch schnell auf den eigenen. Ca. 50 Prozent der Achtjährigen sind bereits online. Ab zwölf Jahren sind es ganze 100 Prozent. Damit sie verantwortungsvoll mit den Möglichkeiten im Netz umgehen können, braucht es eine frühe Sensibilisierung dahingehend, wie wichtig der Schutz der eigenen Daten ist.

Aber das muss altersgerecht geschehen. Und da kommen als ein neuartiger Baustein die Pixi-Bücher meiner Behörde ins Spiel. Wir haben mittlerweile mehrere eigene Publikationen von Pixi-Büchern herausgebracht. In jedem einzelnen Buch werden Datenschutzthemen in alltäglichen Situationen mit viel Witz kindgerecht erklärt. Gleichzeitig haben wir zu den Büchern nun auch Pixi-Videos auf unserer Webseite veröffentlicht.

Die Nachfrage ist riesig. Sowohl von Privatpersonen als auch von Institutionen und Bildungseinrichtungen. Wir kommen mit der Bestellaufnahme der Pixi-Bücher kaum hinterher, es geht in die hohen

Hunderttausende. Das ist erfreulich, denn es zeigt, dass das Thema Datenschutz in unserer Gesellschaft einen immer größeren Stellenwert einnimmt. Datenschutzensensibilisierung funktioniert!

Datenschutzensensibilisierung hört aber natürlich im Erwachsenenalter nicht auf. Auch hier bietet meine Behörde Ihnen ein breites Spektrum an verschiedenen Broschüren oder Flyern mit Spezialwissen zu den verschiedensten Themen an. Sei es zum Datenschutz im Jobcenter, zum Datenschutz bei der Polizei oder zur Informationsfreiheit. Dabei stellen wir derzeit auf sogenannte hybride Flyer um, mit übersichtlichen Infos in der Druckversion und weitergehenden Informationen im digitalen Teil des Angebots.

Meine Bitte an Sie: Tun Sie es mir und meinen Kolleginnen und Kollegen in den Aufsichtsbehörden in den Ländern gleich: Sensibilisieren Sie weiter für den Datenschutz! Sie sind nah dran, Sie erreichen die richtigen Adressaten.

X. Schlussbemerkung

Es liegt noch eine Menge Arbeit vor uns. Für uns als Aufsichtsbehörden und für Sie als Datenschutzexpertinnen und –experten aus allen Bereichen der Praxis.

Uns wird nicht langweilig werden.

Danke, dass Sie mit uns für dieses wichtige Thema, für dieses Grundrecht kämpfen. Bleiben Sie am Ball. Wir brauchen mehr, nicht weniger Datenschutz für eine freie digitale Gesellschaft.

Ich danke Ihnen für Ihre Aufmerksamkeit.