sondern tatsächlich auch Leute, die unsere Sprache nicht verstehen, die vielleicht auch nur leichte Sprache verstehen, die sich nicht orientieren können im Raum vielleicht Hilfen brauchen beim Gehen, oder um irgendwo hinzukommen, oder die wissen müssen, wo ein Fahrstuhl ist, und so weiter. Wir haben ja viele „wirkliche" Integrationsprobleme, die man auch technologisch angehen kann. Und dass man versucht, auch einen guten Mix hinzubekommen, auch für diese Projekte kriegt man ja Fördermittel, und da gibt es auch Fördergeber, die man finden kann, zum Teil kriegt man auch Sponsoring. Das haben wir auch schon geschafft, als damals die große FI… 2016, da haben dann auch Leute u… wir dann gebaut haben, gesponso… chen bemüht, kann man eben auc… immer umzusetzen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Constanze Kurz: Na gut, es sind im Prinzip ähnliche Antworten. Eine gewisse Betonung, dass die Forschung nicht immer nur dem Profit und der Profilierung eines großen Tech-Konzerns dienen soll, sondern sehr viel mehr Facetten hat. Das wäre sozusagen eine der Antworten. Aber dann sind wir eigentlich schon wieder bei der forschungspolitischen Frage, weil wir ja einfach wissen, dass die Summen, die in maschinelles Lernen und angrenzende Bereiche investiert werden, von den Proportionen her sehr unterschiedlich sind. Im Bereich der universitären Forschung etwa, wenn man das mit Deutschland vergleicht, oder eben auch was die großen Konzerne vor allem in Asien eine riesengroße, auch schriftlich festgehaltene KI-Strategie haben, von fast monströsen Ausmaßen, oder eben, was die amerikanischen Konzerne da reinstecken. Vielleicht ist das der Punkt, an dem man – gerade weil die Bundesregierung in ihrem eigenen Strategiepapier, wo sie die „Spurinnovation" ja gern hätte – so … Aspekt betont, dass man ehr… diese albernen Summen, die sie … Tropfen auf den heißen Stein … muss man leider auch für das DFKI sagen, aber sicherlich auch für deine Forschungseinrichtung – fast keine Universität gibt, die nicht im Wesentlichen mit diesem Drittmitteleinwerben zu tun hat. Drittmittelgeber, wenn man sich das in Europa zumindest mal ansieht, sind natürlich auch in großem Maße amerikanische Tech-Konzerne. Das ist leider ein Fakt, der sich über die Jahre eher noch verstärkt als weniger wird. Ich glaube aber, dass es Forschungspolitik allein nicht sein kann …

FIfF-Konferenz 2018

Die DSGVO: Eine kommentierte Reise durch die (Un-) Tiefen des juristischen Feuilletons – eine launige Bilanz nach vier Monaten Geltung

Verschriftlichung des Vortrags von Kirsten Bock und Malte Engeler

Vom Foto-Verbot zum Ende strukturierter Visitenkartensammlungen. Vom großen Blogsterben zu Zahnärzten und ihren Datenschutz-Tonbandansagen. Von überforderten Aufsichtsbehörden zu jubelnden Silicon-Valley-Riesen: Die DSGVO hat all den bekannten Kontroversen des Datenschutzrechts neuen Diskussionsstoff gegeben. Die Twitter-Szene hat die großen, kleinen (und vermeintlichen) Aufreger dankend aufgegriffen. Kirsten Bock und Malte Engeler begeben sich anhand ausgewählter Tweets auf eine kommentierte Twitter-Reise durch die Untiefen des DSGVO-Wahnsinns.

Herzlichen Dank nochmal ans FIfF, wir freuen uns ganz besonders heute hier sein zu dürfen. Wir möchten kurz darauf hinweisen, dass wir privat hier sind und nicht für unsere jeweiligen Dienststellen hier stehen. Das gleiche gilt für die Tweets, die wir hier aufnehmen. Auch diese nehmen wir zur Anschauung, wir folgen denen nicht und bewerten sie auch nicht.

Hier heute beim FIfF zu sein, ist uns besonders wichtig, weil der Mensch im Mittelpunkt stehen soll. Das ist ein Aspekt der in den Diskussionen um die Digitalisierung häufig viel zu sehr in den Hintergrund gerät. Und wenn wir uns mit der DSGVO befassen, dann wollen wir das heute auch besonders vor diesem Hintergrund tun: Den Menschen nicht aus den Augen zu verlieren.

Wie haben wir uns das also vorgestellt? Wir sind beide sehr aktiv auf Twitter und haben uns angeguckt, was seit vier Monaten – seitdem gilt die Datenschutzgrundverordnung – eigentlich so in der Szene diskutiert wird. Dafür haben wir uns repräsentative Tweets herausgefischt. Natürlich ist das auch ein wenig Beispiel unserer eigenen Filterblase. Wir haben versucht, die Debatte ein bisschen divers aufzustellen, aber nochmals der Hinweis: Wir nehmen auf gar keinen Fall den Standpunkt ein, es sind einfach Spotlights in der Diskussion, nicht unbedingt unsere eigenen Auffassungen. Teilweise schon, aber nicht immer.

Da wir auf öffentlich gemachte Tweets von Personen zurückgreifen, haben wir uns tatsächlich auch die Frage gestellt: Dürfen wir das eigentlich, dürfen wir lauter Tweets mit Bildern, mit Namen, mit Twitter-Handles an die Wand werfen und hier in den Köpfen und im Stream speichern lassen? Wir haben uns ziemlich den Kopf zerbrochen, ob das überhaupt zulässig ist.

Also haben wir uns auf die Suche nach der berühmten Rechtsgrundlage gemacht. Das ist immer der erste Schritt, wenn man weiß, was für Daten man verarbeitet. Das hatten wir schnell eingegrenzt: Tweets mit Twitternamen und Fotos drauf. Was ist also die richtige Rechtsgrundlage? In so einem Zusammenhang fallen einem zwei Dinge ein, berechtigtes Interesse und Wissenschaft, denn wir untersuchen das und nehmen schon den wissenschaftlichen Hintergrund in Anspruch. Zu unserem Erstaunen haben wir dann festgestellt, dass Artikel 6 (1f) DSGVO die richtige Rechtsgrundlage für uns ist, denn es gibt keine Ausnahme für die For-

schung im Bereich der einfachen Daten. Es gibt eine im Bereich der besonderen Kategorien von Daten, also wenn mit DNA oder mit Gesundheitsdaten geforscht wird, aber eben nicht für ganz einfache Datenverarbeitung. Das ist vermutlich übersehen worden, uns gestern erst aufgefallen, so als spannender Nebeneffekt.

Es ist ja im Datenschutzrecht vieles beim alten geblieben, aber ein Bereich ist neu, nämlich die Verpflichtung, über die Datenverarbeitung zu informieren. Nach der Feststellung der Rechtsgrundlage folgt also die durch die DSGVO neu eingeführte Informationspflicht. Das stellte uns vor die Herausforderung, die Betroffenen bei Erhebung oder kurz danach zu informieren. Wie haben also alle angeschrieben und ihnen mitgeteilt, dass wir ihre Tweets verwenden, wir haben ihnen die Rechtsgrundlage, die Zwecke der Verarbeitung und zuständige Aufsichtsbehörde mitgeteilt.

Die Antworten fielen ganz unterschiedlich aus und waren sehr interessant, denn es waren ja alles ExpertInnen aus der Datenschutzszene. Einige haben einfach nur gelacht, weil die gemerkt haben, dass es im Grunde eine Nachricht mit einem gewissen Augenzwinkern war. Es kann natürlich nicht sein, dass wir hier für zwanzig Tweets stundenlang mit Juratext die Twitter-DMs oder die Impressumsadressen der jeweiligen Blogs verstopfen.

Andere ExpertInnen haben uns tatsächlich ihre Einwilligung mitgeteilt, dabei hatten wir gar nicht um Einverständnis gebeten, sondern nur informiert. Wir mussten ja nicht um Einverständnis bitten, das ist alles gesetzlich gedeckt. Wir hatten nur eine reine Informationspflicht. Anscheinend hatten einige den Unterschied Einwilligung als Rechtsgrundlage und Informationspflicht noch nicht ganz verstanden.

Einige haben sich tatsächlich nur bedankt und dachten, das wäre jetzt ein bisschen Werbung. Da haben wir auch überlegt, das ist eigentlich eine witzige Idee, das eigene Produkt zu bewerben, indem man sagt, wir müssen jetzt leider informieren über unsere Datenverarbeitung mit diesem fantastischen Produkt, das sie bei unserem Datenschutzcompliancemarketingmenschen erwerben können. Wir dachten, eigentlich wäre das eine witzige Idee, Datenschutz als Standortvorteil. Das bringt uns dann auch gleich zum ersten Tweet und der Frage, worum es eigentlich wirklich bei diesem Gebilde Datenschutz/Datenschutzrecht geht.

Worum geht es eigentlich: Schutzgut des Datenschutzes

Im ersten Tweet stellt der Twitternde diese ganz korrekte Frage und sagt, diese könne man nicht beantworten, ohne vorher das Schutzgut im Datenschutzrecht überhaupt zu klären. Es ist im Grunde das erste, was wir nach dem Geltungsbeginn der DSGVO gemerkt haben, dass nach wie vor – eine ewig alte Debatte – völlig unklar ist was eigentlich der Datenschutz ist. Die DSGVO will Artikel 8 der Grundrechte-Charta umsetzen; da steht so was drin wie Recht auf Schutz personenbezogener Daten. Was genau das aber ist, ist weitestgehend ungeklärt. Was machen also die JuristInnen? Die machen das, was sie immer machen, nämlich das, was früher schon gemacht wurde, und das ist besonders in Deutschland, in der deutschen Debatte natürlich das Volkszählungsurteil und die Debatte davor, und wenn man sich genauer anguckt was tatsächlich in der deutschen Diskussion vertreten wurde, merkt man, dass vom Steinmüller-Gutachten bis zum Bundesverfassungsgerichtsurteil sehr früh sehr viel Kritik an dem Ansatz formuliert wurde, das Ganze auf Privatsphäre und Privatleben zu stützen. Aber genau das ist aktuell der Stand in Deutschland, das ist auch bei vielen Experten, die das Thema diskutieren, immer noch in den Köpfen drin. Datenschutz ist Privatsphärenschutz, Datenschutz ist Schutz des Rechts auf Achtung des Privatlebens. Ob das richtig ist, kann kann man bestreiten; wir werden das an vielen Punkten merken, dass das eine falsche Wahrnehmung ist, weil das Recht auf Privatleben tatsächlich Datenschutz reduziert auf Selbstbestimmung – Datenschutz aber ein Grundrecht ist, das sämtliche Freiheitsrechte: Meinungsfreiheit, Versammlungsfreiheit, Asylfreiheit: alle Freiheitsrechte die die Charta oder das Grundgesetz schützen wollen, schützen will. Das heißt, es geht im Grunde darum, den Menschen im Rahmen des digitalen Wandels davor zu schützen, dass er durch die Datenverarbeitung Eingriffe in seine Rechte erlebt, nicht nur sein Recht auf unbeobachtet sein, auf Selbstbestimmung, und wir werden sehen, dass an vielen Stellen dieses alte Denken, dass es immer noch beim Datenschutz nur um Selbstbestimmung und Persönlichkeitsrechte geht, sehr viele Fehlschlüsse produziert. Worum geht es überhaupt beim Datenschutz? Wie weit reicht er eigentlich? Und das ist die nächste Frage: Kann man eigentlich der Datenschutz-Grundverordnung entkommen? Ist das Rechtsgebiet, dass wir betrachten, überhaupt anwendbar?

Sachliche Anwendbarkeit

Da kommen wir dann gleich zu dem ersten Bereich: die sachliche Anwendbarkeit, die Reichweite der Datenverarbeitung, und da gab es eben diese spannende Frage, was ist denn mit den Visitenkarten, die ich auf solchen Veranstaltungen wie hier bekomme und mit nach Hause trage. Gibt es da Informationspflichten, was folgt daraus? Da ist zuerst einmal zu sagen, die Datenschutz-Grundverordnung erfasst ja erst mal nur die automatisierte Datenverarbeitung, und im analogen Bereich das, was veraktet wird, was sortiert wird, also kann man sich erst einmal merken: Visitenkarten, einfach so in der Schublade als großer Haufen ungeordnet: Kein Problem; raus aus dem Anwendungsbereich. In dem Moment, in dem ich das einscanne, sortiere und vielleicht dann auch noch Drittanbietern zur Verfügung stelle, bin ich im Anwendungsbereich der Grundverordnung.

Die andere Frage, die sich immer stellt, ist, wie ist das eigentlich bei personenbezogenen Informationen, wenn die an die Öffentlichkeit gelangen? Das beste Beispiel dafür ist der Aushang der Krankheitstage im Betrieb. Dem Chef stinkt, dass Leute fehlen, und kurzerhand macht er sich kleine Zettel und schreibt darauf, wer alles krank gewesen ist und hängt das in den Flur. Er sagt, das ist zur Information der Mitarbeiter, damit die alle

wissen, wer da ist und wer nicht. Fällt das unter die Grundverordnung oder nicht? Es ist erstmal keine automatisierte Datenverarbeitung, und das ist ein Aspekt, den wir auch in der aufsichtsbehördlichen Praxis immer wieder zu bearbeiten haben. Datenschutz ist kein Geheimnisschutz, darum geht es erst mal nicht. Ausgenommen ist auch der gesamte Bereich der persönlichen Verarbeitung: alles was die Privatsphäre, betrifft, was ich zu Hause für mich mache, was ich nicht teile nach außen, das ist von der Grundverordnung ausgenommen in Artikel 2 und unterfällt der Grundverordnung nicht, aber es gibt natürlich viele Bereiche, in denen vermischt sich dieses private Häusliche: Mit meinem Handy, wenn ich zum Beispiel bei Whatsapp bin und da dann im Hintergrund ein Datenaustausch stattfindet. Was ist, wenn ich twittere? Unterfällt das der DSGVO?

Soziale Medien

Das ist tatsächlich eine der Fragen, die auch in der Szene heiß diskutiert werden: Wenn ich jetzt auf Twitter meine persönliche Meinung äußere, ist es eigentlich etwas, was der Datenschutz-Grundverordnung unterfällt? Das hätte ganz dramatische Folgen, da wäre ich nämlich verantwortlich für das was ich auf Twitter tue: Ich muss meinen Informationspflichten gerecht werden, unter anderem meinen Namen angeben, weil ich ja den Verantwortlichen der Datenverarbeitung benennen muss. Das würde im Umkehrschluss bedeuten, dass wir dank der DSGVO eine Klarnamenpflicht in der Nutzung von sozialen Medien haben. Die Frage ist unbeantwortet, es gibt unter den Aufsichtsbehörden die einen, die selber twittern, die sagen, das sei alles nicht so schlimm, und es gibt die, die das ein bisschen strenger sehen und sagen, eigentlich müsste man, wenn man die ganze Geschichte ernst nimmt, tatsächlich die Nutzung von Twitter darunter fassen, weil es eben eine Datenverarbeitung ist, die immer die Öffentlichkeit betrifft; das ist nichts, was im Privaten bleibt, in einer geschlossenen Nutzergruppe, sondern es ist für alle Öffentlichkeit sichtbar. Da hat der OGH eigentlich ziemlich klar gesagt, wenn es für die Öffentlichkeit sichtbar ist, unterfällt es der Grundverordnung. Das Problem ist im Grunde eines von vielen, wo man merkt: Die DSGVO stellt Anforderungen auf, aber so richtig vollziehen mag man sie doch nicht, weil das zu wahnsinnigen Verzerrungseffekten und im Grunde gesellschaftlich gar nicht hinnehmbaren Folgen führen würde, wenn wir das durchziehen würden, und das ist so ein Motto, dass man an vielen Stellen der Grundverordnung sieht: Wenn man sie ernst nehmen würde, würde sie nicht funktionieren.

Einwilligung

Der nächste Tweet, der so ein bisschen zeigt, wo die Debatte hinläuft, ist einer über eine Aussage von – unter anderem – Jan Albrecht, aber ist nur exemplarisch und das führt fort, was ich anfangs sagte: Die Unklarheit darüber, reden wir hier über Privatsphärenschutz, über Selbstbestimmung, reden wir über Datenschutz oder was ist überhaupt Datenschutz? Ein ganz ganz erheblicher Teil der klassischen Vertreter der Datenschutzszene fokussiert sich unglaublich stark auf die Einwilligung. Da gibt es Begriffe wie „Die Königin der Rechtsgrundlagen", „Kern des Datenschutzes" und „Grundprinzip des Datenschutzes", und das ist eine Aussage, die ist schlicht falsch. Die ist falsch aus zwei Gründen: Es gibt da dogmatische Gründe, da könnten wir jetzt juristisch darüber reden, was genau eigentlich Einwilligung soll. Ist sie eine Beschränkung von einem Grundrecht oder ist es eine Ausübung? Rein dogmatisch passt die Einwilligung überhaupt nicht dazu, dass wir hier von Privatsphäre und allgemeinem Persönlichkeitsrecht reden. Viel wichtiger ist aber, dass die Einwilligung, wenn man sich so sehr auf die Einwilligung fokussiert, zu zwei Dingen führt: Erstens entfaltet sie überhaupt keinen Schutz mehr; ich kann nicht mehr zählen, wie oft ich auf einer Website einfach nur noch blind OK klicke, bei diesen ganzen Cookie-Bannern. Ich soll zu *manage options* gehen und dann kann ich *performance cookies* definieren und *tracking cookies* und *necessary cookies* – kann ich alles machen, oder ich will einfach nur ein Zitat lesen auf der Webseite und sage: Ich nehme dafür nicht 15 Minuten feingranulare Einstellungen vor. Ich willige ein, aber ich willige nicht wirklich ein. Dass ist eine reine Fassade, ist im Grunde nur der Anschein von Rechtmäßigkeit, der nur dazu führt, dass die Einwilligung völlig entwertet wird, weil das für die Menschen keinen Schutz mehr hat, weil die Nutzer einfach nur sagen, ich will meinen Dienst nutzen. Das heißt, wer so sehr auf die Einwilligung fokussiert, entwertet die Einwilligung. Bei Datenverarbeitungen, die massenhaft identisch auftreten wie zum Beispiel im Internet: immer gleiche Sachverhalte, immer wiederholt durch Webseiten-Besucher, ist die Einwilligung überhaupt keine angebrachte Möglichkeit, Datenschutz sinnvoll zu regulieren.

Kopplungsverbot

Das wissen natürlich auch diejenigen, die so ein bisschen sehr sich auf die Einwilligung einstellen, und die versuchen, das dann zu retten mit etwas – das ist jetzt ein juristischer Begriff, der aber vielleicht auch schon mal außerhalb der juristischen Kreise Wellen geschlagen hat: Dem sogenannten „Kopplungsverbot". Das Kopplungsverbot – hier ein sehr schöner Tweet von einer Rechtsanwältin, die sich darüber beschwerte, dass das Kopplungsverbot die Privatautonomie einschränkt – was meint sie damit, erzähle ich gleich, aber das wichtigste, was alle im Saal einfach mitnehmen können: Es gibt in der Datenschutz-Grundverordnung kein Kopplungsverbot. Was ist das Kopplungsverbot? Das Kopplungsverbot ist die Idee, dass, wenn man mehr Datenverarbeitung als für den Vertrag gefordert ist, rechtfertigen will, also der Dienstanbieter mehr erfassen will, als er eigentlich aufgrund der vertraglichen Leistungen an Daten bräuchte, wenn er das über eine Einwilligung rechtfertigen will, dann muss man diese Einwilligung so ein bisschen genauer angucken, ob die freiwillig ist und man damit mehr macht als man eigentlich für den Vertrag braucht. Das ist unter dem Stichwort *Kopplungsverbot* genannt. Ein solches Kopplungsverbot, das dieses verbieten würde, gibt es in der Grundverordnung nicht; es ist nicht verboten, über eine Einwilligung mehr Datenverarbeitung zu rechtfertigen, als man für die Vertragserfüllung braucht. Ganz im Gegenteil: Wenn das

der Fall ist, muss man genauer hingucken, ob die Einwilligung freiwillig ist und was die Praxis daraus macht. Die muss trotzdem noch freiwillig sein, obwohl man sagt: Du kriegst den Dienst nur, wenn du einwilligst. Sie lösen das ganze darüber, dass sie die Einwilligung retten, indem sie sagen, dann biete eine Alternative an, die du bezahlst, wo diese Datenverbindung nicht so intensiv ist – und wozu führt das? Das führt dazu – was wir aktuell und damit im Bereich der Onlinemedien ganz häufig sehen – es gibt jetzt den Basistarif, also quasi wie immer, volles Tracking, aber man braucht ja eigentlich kein Tracking um eine Webseite aufzurufen. Man braucht keine Cookies, um eine Webseite zu lesen. Das ist also nicht wirklich erforderlich, also ist die Einwilligung, was die Freiwilligkeit angeht ein bisschen kritisch. Dann bieten wir eben, um die Freiwilligkeit zu retten – also quasi wieder als Fassade – nebenbei einen Premiumdienst an für alle die nicht getrackt werden wollen, um die Freiwilligkeit der Einwilligung für alle anderen zu erhalten. Das ist die Idee. Für alle anderen, die sagen, ich kann mir das gar nicht leisten, aber die haben ja theoretisch jetzt eine Wahl, und da sie eine Wahl haben, ist es wieder freiwillig. Wozu führt das in der Praxis? 99 % der Leute werden weiter genauso getrackt wie vorher und 0,03 % kaufen sich das Privacy-Add-on, werden damit zu einer datengeschützten Elite und für die anderen ändert sich überhaupt nichts. Das ist im Grunde das Problem, dass das Kopplungsverbot gesamtgesellschaftlich wahnsinnige Verzerrungswirkung haben kann. Das muss man noch mal sehen, wie sich das entwickelt, aber die Idee, den Fokus auf die Einwilligung zu retten über dieses komische Kopplungsverbot, da halte ich überhaupt nichts davon.

Globaler Exportschlager?

Wir haben also in der europäischen und auch in der deutschen Debatte aufgrund eines nicht ganz passenden Grundverständnisses von Datenschutz ein sehr schiefes Verständnis davon, worum es im Kern geht, um Einwilligung, und das schöne ist, das exportieren wir jetzt in die ganze Welt. Die Frage, ist die DSGVO der Exportschlager, der sie vorgibt zu sein? Ist Europa der neue Datenregulierer der ganzen Welt? Hat die Welt auf die DSGVO gewartet? Man kann sagen, die DSGVO hat sozusagen krakenartig ihre Fühler in die Welt herausgestreckt, über den Artikel 3, indem sie bestimmt, dass ein Unternehmen, das Datenverarbeitung auf dem europäischen Markt anbietet, auch wenn es in den USA sitzt, dann der Datenschutz-Grundverordnung unterfällt. Hat das dazu geführt, dass die DSGVO mehr Wirkung entfaltet? Das werden wir sehen, die Unternehmen versuchen sich zum Teil darauf zu fokussieren; wir wissen aus Umfragen, dass nach eigener Einschätzung der Unternehmen ca. 24 % datenschutzkonform agieren. Das ist also noch nicht so rasend viel. Was wir zur Kenntnis nehmen, ist, dass in einigen Drittstaaten es auch Datenschutzregulierung gibt, die sich auch in der Tat an der Grundverordnung orientiert. Das ist aber eigentlich keine Besonderheit, das gab es auch schon zu Zeiten der Richtlinie. Insbesondere im südamerikanischen Raum gibt es eine sehr lebhafte und eine sehr am europäischen Datenschutzrecht orientierte Regulierung.

Kalifornien – das war dann auch groß zu lesen – ist der DSGVO auch ein Stück weit gefolgt und hat einige Aspekte aufgegriffen, ist zum Teil ja aber auch sogar darüber hinausgegangen. Im Asia-Pacific-Raum haben wir immer schon datenschutzrechtliche Regeln gehabt, die sich aber mehr am US-amerikanischen Verständnis von Datenschutz orientiert haben. Da muss man wahrscheinlich auch noch ein bisschen abwarten, wie sich das tatsächlich entwickelt, inwieweit wir tatsächlich aus der DSGVO heraus einen globalen Standard bekommen. Was es aber zu fragen gilt, auch vor dem Hintergrund, dass wir das vielleicht auch politisch exportieren wollen, ist die Frage, was exportieren wir denn da eigentlich? Ist das nur die Einwilligung, ist das so ein diffuses Verständnis von Datensouveränität und was ist dann überhaupt der Gegenstandsbereich? Damit kommen wir dann zu einer der Kernnormen der DSGVO, ohne die genauen Rechtsgrundlagen.

Rechtsgrundlagen – bitte zu Ende lesen …

Die sind alle in einem Artikel geregelt, den müssen wir jetzt nicht nennen, aber das schöne ist, wenn wir die DSGVO zu Ende lesen würden – und das tun tatsächlich einige nicht so gerne – dann würden wir sehen, da stehen nach der Einwilligung noch eine ganze Menge anderer Rechtsgrundlagen. Wir dürfen Daten verarbeiten, wenn wir Verträge erfüllen müssen, wenn sie in unserem Interesse stehen, wenn dies zur öffentlichen Aufgabenerfüllung notwendig ist, es lebenswichtig ist, das ist alles möglich. Die Einwilligung ist eine von vielen Rechtsgrundlagen, wenn man das mit exportieren würde, das wäre zum einen ein Gewinn und da gab es – direkt am 25. Mai – einen mir sehr sehr nachvollziehbaren Tweet: Ich habe zwar selbst kein Auto, aber ich habe ins Lenkrad von meinem Fahrrad gebissen, als ich den halben Tag im Radio gehört habe, die DSGVO habe den Vorteil, dass jetzt BürgerInnen von Behörden und Unternehmen immer um Zustimmung gefragt werden müssen, bevor ihre Daten verarbeitet werden. „Lenkrad zeigt inzwischen Abdrücke meiner Zähne …" Ganz genau so ging es mir auch, das ist längst nicht der Fall, die Einwilligung ist überhaupt nicht der Kern der Grundverordnung, sie ist eine von 6-7 Rechtsgrundlagen, die alle auch geprüft werden müssen. Für Unternehmer ist das auch das Entscheidende: die Empfehlung, dass bitte auch zu tun, denn die Einwilligung ist jederzeit widerrufbar. Wenn wir ein Geschäft aufbauen und uns nur auf die Einwilligung verlassen, dann kann, wenn wir einen Datenschutzskandal haben, mal eben die Einwilligung für den Abo-Dienst widerrufen werden, und dann kann das ganze Geschäftsmodell in sich zusammenfallen, weil wir auf die Einwilligung gesetzt haben und dank dem Widerruf die ganze Datenverarbeitung ihre Rechtsgrundlage verliert. Deswegen in jedem Fall die Empfehlung: Bevor man sich auf die Einwilligung als Ultima Ratio verlässt: alle möglichen Rechtsgrundlagen prüfen: Vertragserfüllung, berechtigte Interessen, alles was man finden kann, um hier nicht am Ende auf einmal den Teppich unter den Füßen weggezogen zu bekommen.

Und eine ganz andere Frage: Was ist denn nun, wenn man sich auf die Einwilligung verlassen hat, zum Beispiel: Ich bin eine große Supermarktkette und sage, ich hätte gern Kundenkartenprogramme, und alle die wir hier sitzen, sagen, alles klar 3 % Rabatt bei jedem Einkauf, das mache ich mit, und macht es über eine Einwilligung. Irgendwann ist mein Geschäft vielleicht in Verruf und Sie sagen, ich widerrufe diese Einwilligung. Und dann sage ich: Moment mal, das hätte ich auch im Vertrag schreiben können, ich switche mal um auf eine andere Rechtsgrundlage. Und das ist im Grunde das Problem, dann ist nämlich die Folge, wenn man nicht vorher die Grundverordnung zu Ende liest, wenn man sich einmal auf die Einwilligung eingelassen hat, dann suggeriert man

ja so eine Art Gleichordnung und so eine Ebene, wo quasi zwei gleichrangige Parteien sich das so überlegt haben, wenn die dann sagen, da nehme ich mal wieder die Rechtsgrundlage, die im Gesetz steht, Vertragserfüllung, dann – vielleicht nicht herrschende Ansicht aber eine sehr starke Ansicht bei den Juristen – da ist der Rückgriff gesperrt, dann haben sie Pech. Dann ist die Einwilligung weg und etwas anders können Sie nicht nehmen. Deswegen ganz klare Empfehlung: In der Grundverordnung immer zu Ende lesen und sich nicht immer gleich auf die Einwilligung zu stürzen.

Soft Law oder harte Regulierung?

Der nächste Tweet betrifft Artikel 5, was bietet die DSGVO eigentlich noch als Rechtsgrundlage? Wir haben eine ganze Reihe von Regeln, und eine der Kernregelungen in der DSGVO ist Artikel 5, das sind die Grundsätze der Datenverarbeitung. Nun gibt es diesen Streit, wie verbindlich sind die eigentlich? Ist das eigentlich nur Gesetzgebungsprosa oder ist das auch verbindlich? Muss man das umsetzen, Soft Law oder Regulierung? Die DSGVO ist eindeutig mehr als Einwilligung, das haben wir gehört, mehr als Rechtsgrundlagen die Programmsätze, die Grundsätze werden in Absatz 1 beschrieben. Interessant für uns ist aber auch der Absatz 2, der häufig auch nicht mehr mitgelesen wird. Im Absatz 2 wird nämlich die Verantwortlichkeit festgeschrieben, und das ist auch deutlich stärker herausgearbeitet worden in der Grundverordnung im Vergleich zur Richtlinie: Dass die Verantwortlichen, sei es ein Unternehmen für sich oder gemeinsam mit anderen Unternehmen, oder auch eingebundene Auftragsverarbeiter rechenschaftspflichtig sind, und insofern wird der Artikel 5 Absatz 2 meines Erachtens etwas unterschätzt. Der sagt nämlich, der Verantwortliche muss nachweisen, dass er mit den Regelungen der Grundverordnung compliant ist. Daraus folgt der Anspruch, dass der Verantwortliche verpflichtet ist, Prüftransparenz herzustellen, und Prüftransparenz ist sozusagen die Baustelle im Datenschutzrecht und in der Datenschutzumsetzung. Jedenfalls aus aufsichtsbehördlicher Sicht und aus Sicht der Durchsetzung von Datenschutzrecht, weil ich Datenschutzrecht nur durchsetzen kann, wenn ich es auch prüfe, und ich kann es nur prüfen, wenn in den Unternehmen die Datenverarbeitung auf eine Art und Weise gestaltet ist, die prüffähig ist. Wenn ich erst in ein Unternehmen komme und da ist alles kuddelmuddel, dann fange ich erst mal an zu sortieren und dann komme ich vielleicht am fünften oder sechsten Prüftag erst zur eigentlichen Prüfung. Die Grundverordnung verpflichtet jetzt die Unternehmen, ihre Datenverarbeitung so aufzubereiten, so transparent zu machen, so zu dokumentieren, dass sie prüffähig ist, und davon ausgehend folgen eine ganze Menge Pflichten. Unter anderem auch die Transparenzpflicht,

Durchsichtige Transparenz

Und da sind wir schon wieder bei meinem Lieblingsthema am heutigen Tag. Die Transparenz ist ein ganz erheblicher Teil, der die Grundverordnung prägt, und das sieht man auch an vielen Tweets und das spiegelt so ein bisschen den Geist wider, in dem wir in der ganzen Debatte leben. Transparenz ist im Grunde die Supermaßnahme, Transparenz ist quasi die Lösung für alles, und das ist genauso ein Problem, wenn man auf die Selbstbestimmung, Privatleben schaut, die Einwilligung fokussiert, dass Transparenz im Grunde zum Selbstzweck hochstilisiert wird. Und das ist tatsächlich etwas, was ich auch extrem kritisch sehe, aus dem einfachen Grund, dass Transparenz alleine keinen Wert hat. Wenn wir zum Supermarkt gehen und sagen, ich hätte gern einen Liter Milch und gehen dann zum Regal gucken und gucken uns an, was auf einem Liter Milch steht. Dann ist auf der Milch gedruckt, Achtung, enthält Arsen, ist supergiftig, nicht kaufen – ja, super transparent. Ich will aber nicht im Supermarkt eine halbe Stunde verbringen, das Kleingedruckte zu lesen, um zu gucken, welche Milch giftig ist. Transparenz alleine hat überhaupt keinen Wert. Wenn wir Artikel 8 DSGVO, Recht auf Schutz personenbezogener Daten ernst nehmen, dann müssen wir aus Transparenz immer auch irgendeinen Schutz ableiten, und das bedeutet schlicht, das es, genauso wie im Lebensmittelrecht üblich, höchste Vorgaben dafür gibt, dass man keine Milch mit Arsen verkaufen darf. Und das ist genau die Folgerung, die man, wenn man Transparenz isoliert betrachtet, vergisst: Es klingt manchmal so, als müsste man nur ins Kleingedruckte genug reinschreiben und den Nutzern klar machen, was alles an Unfug getrieben wird, Dann ist doch alles gut, dann ist es transparent. Klar, wenn man nur auf Selbstbestimmung abstellt, dann ist Transparenz der Inbegriff von Datenschutz, aber ich will eben nicht nur die Möglichkeit haben, zu wissen, was ich mir schlechtes antue – ich will schlicht davor geschützt werden. Das heißt, Transparenz ist in weiten Teilen tatsächlich auch ein Buzzword der DSGVO, und Buzzword ist genau das nächste Thema, davon gibt es noch eine ganze Reihe mehr in der Datenschutz-Grundverordnung. Vorher noch ein Tweet von Tim Wu, großartiger Professor an der Columbia University of Law, auf den Punkt gebracht: Transparenz ist im Grunde immer nur ein Ersatz dafür, überhaupt etwas zu tun. Aber das ist schwierig, wir müssen irgendwie den Onlinemarkt regulieren, mit so vielen Stakeholdern, und die Werbemenschen machen uns das Leben schwer: einfach Transparenz drauf klatschen, das hilft dann schon, und das ist genau das was der Grundverordnung auch nicht gerecht wird. Transparenz als Master ist im Grunde erst mal nur die Ausrede dafür, sich überhaupt Gedanken zu machen.

Buzzwords by Design

Wir bleiben beim Buzzword. Transparenz ist auch ein Buzzword aber natürlich: Transparenz ist notwendige Bedingung, es ist nur nicht hinreichend, und das Problem haben wir eben bei vielen Dingen in der Grundverordnung. Der Artikel, der das am schönsten zusammenfasst, ist der Artikel 25, der wird bei ganz vielen ganz hoch gelobt, da geht es nämlich um *Privacy by Design*. Das ist im Moment das Number-One-Buzzword neben den jetzt aufkommenden Ethics. Was steht eigentlich hinter dem Artikel 25? Der ist aufgeteilt in zwei Absätze. Der erste Absatz regelt Privacy by Design, der zweite Absatz regelt Privacy by Default. Ich möchte jetzt erstmal ausdrücklich nur über den Absatz

1 reden, der Absatz 2 hat nämlich durchaus einen eigenen Regelungsgehalt. Den würde ich dem Absatz 1 absprechen. Privacy by Design ist eigentlich nichts anderes als eine sehr wirkungsvolle, sehr mundgerechte, sehr marketingtechnisch gut gemachte Zusammenfassung dessen, was die DSGVO eigentlich will. Sie möchte, dass ich, bevor ich in eine Datenverarbeitung eintrete, also bevor ich anfange, automatisierte Datenverarbeitung zu betreiben – die fällt ja nicht vom Himmel, die muss ja designed werden, ich muss mir mal Gedanken machen, was für Daten will ich denn überhaupt verarbeiten, ich brauche auf jeden Fall immer Hardware und ich brauche immer Prozesse die das regulieren. Ich muss mir am Anfang eigentlich immer Gedanken machen, und das möchte Artikel 25 zum Ausdruck bringen: Mach Dir vorher Gedanken, bevor du in eine Datenverarbeitung einsteigst, und darüber hinaus mach Dir nicht nur Gedanken, sondern denk auch daran, dass es Rechtsvorschriften gibt, die Dir sagen, was du darfst und was du nicht darfst, und beachte die. Das ist nämlich ein Punkt den man erwähnen muss, der scheinbar nicht bekannt ist, dass es durchaus Rechtsbereiche gibt, die reguliert sind, und dass man sich dann tunlichst auch an die Vorgaben hält. Die Vorgaben mögen nicht immer präzise sein, manchmal sind sie genereller Natur, aber nichtsdestotrotz muss man sie beachten. Um das zu institutionalisieren, diesen Vorgang des Vorher-Gedanken-Machens, gibt es in der Grundverordnung eine Regelung, die sehr sinnvoll ist, und das ist das Datenschutz-Impact-Assessment. Das ist wirklich auch eine Neuerung der DSGVO, das gab es vorher so nicht in der Richtlinie, und das ist ein echter Mehrwert. Kleiner Haken an der Sache: Das Datenschutz-Impact-Assessment ist nur für Datenverarbeitung mit einem besonders hohen Risiko gesetzlich vorgegeben, das ist ein bisschen misslich, ist aber auch nicht so schlimm, weil man ja vorher zu dem Ergebnis kommen muss, dass für die Datenverarbeitung, die ich plane, kein hohes Risiko besteht. Wie komme ich dazu? Das sagt die Grundverordnung nicht explizit. Was ich aber immer empfehlen würde, und da kommen wir dann vielleicht auch zu den positiven Seiten der DSGVO, da kann nämlich ein echter Mehrwert daraus entstehen: Bei jeder Datenverarbeitung, bei jedem Projekt erst mal so ein Mini-Assessment zu machen; sich also die Daten anzugucken, die verarbeitet werden, die Software, die Hardware, die Prozesse, die Personen, die ich einbinde, und dann eine Risikoabschätzung zu machen: In welchem Bereich unterliege ich rechtlichen Vorgaben, in welchem nicht, wie tief ist die Eingriffsintensität? Das hat mehrere Vorteile: Einmal: Ich weiß ungefähr, dass ich mich rechtlich auf sicherem Terrain bewege, ist also ein Aspekt des Risikomanagement. Der andere Aspekt ist, dass ich im Idealfall tatsächlich weiß, was ich tue. Das ist vielleicht für so kleine EntwicklerInnen oder kleine Start-ups nicht so das Problem. Je größer das Unternehmen aber wird, desto schwieriger wird es, genau diese Frage in den Griff zu bekommen. Ich habe unterschiedliche Entwicklungsabteilungen, die alle vor sich hin arbeiten, und irgendwann wird das zusammengeführt. Aber wenn es dann zusammengeführt wird, weiß eigentlich niemand mehr so richtig, was da eigentlich passiert. Ich brauche immer jemanden, der den Überblick behält, und wenn man so ein Datenschutz-Impact-Assessment macht, Privacy by Design ernst nimmt, dann kommt da hinterher etwas heraus, das vernünftig dokumentiert ist, das sich dann jemand anschauen und diesen etwas weiteren Blick über die Datenverarbeitung behalten kann. Das wäre dann eine Win-Win-Situation.

Verarbeitungsverzeichnis – Bürokratie oder Empowerment?

Wir haben in der Grundverordnung noch eine weitere Regelung, die, wenn man sie ein bisschen intelligent anwendet, durchaus zu so einer Win-Win-Situation führen kann, und zwar ist das die Vorschrift, dass Verarbeitungsverzeichnisse zu führen sind. Da könnte man jetzt sagen, was ist das denn für eine blöde Bürokratie? Hat das auch noch andere Folgen, ist das Bürokratie oder Empowerment? Ich würde sagen, wenn man das intelligent macht, dann kann das dazu führen, dass ich tatsächlich Kontrolle über meine Verarbeitungstätigkeiten erlangen kann. Das Management muss sich nämlich fragen, was tue ich eigentlich? Welche Daten verarbeite ich eigentlich? Das führt immer wieder zu überraschenden Ergebnissen, wir haben das bei uns in der Dienststelle zum Beispiel auch gemacht, und dann kam heraus, dass wir mehr Verfahren haben, als wir eigentlich selbst dachten. Es ist immer wieder ein spannender Prozess, der am Ende dazu führt, dass ich weiß, was ich was ich tue. Der insofern – und so kann man das dem Management auch immer sehr gut verkaufen – ein Aspekt des Risikomanagement ist. Ich kann mich ja nur schützen vor Risiken, wenn ich sie überhaupt kenne, und insofern kann ich eigentlich nur empfehlen, dieses Verzeichnis der Verarbeitungstätigkeiten ernst zu nehmen und durchaus kleinteilig zu betreiben und nicht zu grobgranular. Wenn ich das grobgranular mache, dann hat es wirklich keinen Mehrwert für das Unternehmen, dann ist es wirklich nur Bürokratie. Wenn ich das aber ein bisschen feingranularer mache, dann tauchen da manchmal Dinge auf über die ich selbst überrascht bin.

IT-Sicherheit: falsche Schwerpunktsetzung ...

Für mich persönlich die wichtigste Regelung in der Grundverordnung, eine die sich ein wenig versteckt. Was wir jetzt häufig erleben, ist, dass gerade bei den externen Datenschutzbeauftragten oder auch bei den betrieblichen Datenschutzbeauftragten der Fokus sehr stark auf die IT-Sicherheit gelegt wird. Wie hängen IT-Sicherheit und Datenschutz eigentlich zusammen? In der Grundverordnung geregelt wird die Sicherheit der Verarbeitung in Artikel 32, eine der Normen, die ich mit zu den vier bis fünf wichtigsten Normen der Grundverordnung zählen würde. Neben Artikeln 4, 5, 6 ist das der Artikel 32. Warum? Artikel 32 muss in dem Kontext der Grundverordnung gelesen werden, das heißt, er betrachtet eben nicht nur die klassischen IT-Sicherheitsziele, also Vertraulichkeit, Verfügbarkeit und Integrität, sondern geht darüber hinaus. Der Artikel 5 spielt eine große Rolle, und was was der eigentliche Kern ist: Über Artikel 32 kommt das Recht oder fließt das Recht in die Technik ein. Das ist nämlich genau die Schnittstelle, die wir brauchen, um rechtliche Anforderungen in die Technik zu überführen, und das machen wir in der Regel mit Schutzzielen und mit den daraus generierten Maßnahmen. Die sollen sicherstellen, dass das, was wir rechtlich vorgeben, auch tatsächlich in der Technik ankommt. Jetzt haben wir – und das sehen wir ganz deutlich gerade in Artikel 5 und Artikel 32 –, dass da Schutzziele, Maßnahmen, Grundsätze wild durcheinander gewürfelt sind. Das liegt vermutlich daran, dass die Grundordnung in erster Linie von Lobbyisten, zumindest aber von Juristen gemacht worden ist. Einige Väter und Mütter der Grundverordnung waren halt Juristen und insofern ist dieser Bereich dann einfach ein bisschen zu kurz gekommen – auch vor dem Hintergrund,

dass die Grundverordnung natürlich den Anspruch hat, technikneutral zu sein. Aber Technikneutralität heißt ja nicht, dass man keine Vorgaben macht, die man auch technisch umsetzen kann. Insofern würde ich sagen, Artikel 32 ist ausbaufähig. Maßnahmen sind eigentlich die der Umsetzung der Grundverordnung.

Transparenz ist für die anderen …

Ich habe ja schon ein bisschen frech über die Transparenz geschimpft, und wollte nur einen Punkt noch betonen, denn witzigerweise verlangt die Grundverordnung von den Aufsichtsbehörden etwas Neues, nämlich dass sie Transparenz wahren bei der Besetzung ihrer Spitzenposten. Das ist eine positive Entwicklung der Grundverordnung, dass erstmals wir zumindest eine Vorgabe haben, bei der Besetzung der Spitzenposten: klare Vorgaben, Bestenauslese, orientiert an dem Vorbild für den europäischen Datenschutzbeauftragten, kompliziertes Auswahlverfahren, Ausschreibung. Das Problem ist bisher, obwohl die Grundverordnung gilt, dass alle Posten, die bisher besetzt worden sind oder die dabei sind, besetzt zu werden, das scheinbar ignorieren, d. h. wir könnten jedenfalls nicht feststellen, ob die Personen, die dann wirklich benannt werden, auch die bestgeeigneten sind.

Who watches the Watchmen?

Wir wissen es schlicht nicht, weil wir keinen konkreten Vergleich haben, und wozu das führt, kann am besten daran messen, wie sich die Aufsichtsbehörden gerade zumindest so schlagen. Wenn man sich das mal anguckt, dann findet man unter anderem das Problem, dass die Aufsichtsbehörden – die 18, die wir haben, also jedes Bundesland eine, Bayern zwei und der Bund – sich alle gerne mal widersprechen, sich in die Quere kommen, und das ist etwas, wo man fragen muss: Funktioniert es eigentlich gerade mit der Grundverordnung?

Endlich mit Biss?

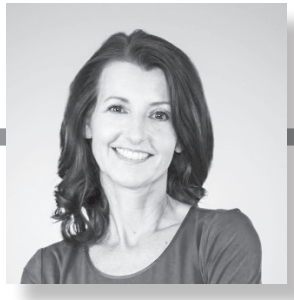
Und wenn man dann eine Aussage wie diese liest, dass der hessische Datenschutzbeauftragte sagt, bisher waren wir zahnlos und jetzt haben wir Zähne bekommen; wir sind zwar nicht bissig, aber wir haben Biss – das ist etwas, da kann ich mich einfach nur wundern, denn entweder hat Herr Ronellenfitsch die vorherige Rechtslage nicht richtig verstanden und seine eigenen Befugnisse nicht gekannt, denn schon vorher gab es die Möglichkeit, Bußgelder bis 300.000 € zu verhängen. Das wurde nie ausgenutzt, also die Bußgelder sind nie an diese Grenze gekommen, und es war nie so, dass die Datenschutzbeauftragten sagten, wir hätten gerne, aber wir konnten nicht mehr. Oder er hat tatsächlich die Grundwerte und die neuen Kompetenzen falsch eingeschätzt, und was aus dieser komischen Gemengelage jetzt entsteht, ist eine ganz merkwürdige Situation von Unsicherheit und von einer Drohkulisse, die den letzten Punkt, den ich vielleicht noch anspreche, nämlich das berühmte Blogsterben betreffen.

Bußgelder und Blogsterben

Es scheint bei den Nutzern auf einmal die Sorge zu sein: Jetzt kommt auf einmal die Grundverordnung und macht mir den Blog dicht, weil ich ein Komma in der Datenschutzerklärung falsch gesetzt habe. Das ist genau dieser verschobene Blick, der aus dieser Betonung kommt, jetzt haben wir richtig Macht bekommen, jetzt haben wir wirklich Eingriffsbefugnisse bekommen, die tatsächlich aber im wesentlichen vorher schon bestanden. Warum sie jetzt auf einmal mehr vollzogen werden dürfen, wissen wir nicht, werden wir sehen. Das Problem ist, dass diese Drohkulisse, die aufgebaut wird, mit Forderungen, wie auch zum Beispiel jetzt endlich 4 % des Jahreseinkommens auch zu vollstrecken, diese Drohkulisse kann sich auch zum Bumerang entwickeln. Wenn wir in fünf, sechs Monaten merken, da kommt nichts, dann wird das möglicherweise eine kleine Blase, dann wird man vielleicht das Problem haben, dass uns auch keiner mehr ernstnimmt. Da muss man sehen, wie diese neue Drohkulisse nachher umgesetzt wird, ob tatsächlich die Grundverordnung hier zu einem besseren Vollzug führt oder nur zu viel Sorge – und dann ist auch nichts draus geworden.

Goldstandard?

Bleiben wir bei der Frage: Ist denn die Grundverordnung jetzt der neue Goldstandard? Damit ist 2012 mal Viviane Reding angetreten: Die Grundverordnung sollte Goldstandard sein. Lassen wir mal die Frage offen.



Kirsten Bock und Malte Engeler

Kirsten Bock ist Juristin und arbeitet seit 2004 im *Unabhängigen Landeszentrum für Datenschutz*. Dort hat sie das Europäische Datenschutz-Gütesiegel, kurz *EuroPriSe*, gegründet. Derzeit arbeitet sie zusammen mit Martin Rost und anderen an der Entwicklung des Standard-Datenschutzmodells, einem systematischen und Grundrechte-fokussierten Verfahren zum Datenschutzmanagement. Sie ist Mitglied der Grünen.

Malte Engeler ist promovierter Rechtswissenschaftler, aktuell Richter am Schleswig-Holsteinischen Verwaltungsgericht. Zuvor hat er vier Jahre im Bereich der nationalen und europäischen Datenschutzaufsicht gewirkt und kennt die DSGVO gut. In seinem Blog *deathmetalmods* kommentiert er kritisch vor allem Hardware und Dienstleistungen.