Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Datenschutz als Innovationsmotor“

bei den BvD-Verbandstagen 2022
Berufsverband der Datenschutzbeauftragten Deutschlands e.V.

Berlin, 10. Mai 2022

Es gilt das gesprochene Wort

Lieber Herr Spaeing,

sehr geehrter Herr Füllhaase,

liebe Kolleginnen und Kollegen Datenschützer,

I. [Einleitung]

Ich bedanke mich für die Einladung und die Gelegenheit, Ihnen meine Sicht zu den Themen, die uns alle tagtäglich beschäftigen, darzustellen.

Ich will mich aber zunächst einmal bei Ihnen allen für Ihre Arbeit als betriebliche und behördliche Datenschutzbeauftragte bedanken. Ohne Ihre Arbeit vor Ort in den Unternehmen und Verwaltungen wären meine Länderkollegen und ich heillos überfordert und wenig durchsetzungsfähig. Sie sind unsere verlängerten Schreibtische und Sie sollen wissen, dass ich Ihre Arbeit sehr zu schätzen weiß.

Die beiden letzten Pandemiejahre haben uns alle vor neue Herausforderungen und Aufgaben gestellt, die so niemand erwarten konnte. Dass Homeoffice und mobiles Arbeiten heute für viel Beschäftigte „normal“ geworden ist, dass die Unternehmen und Verwaltungen sich darauf nicht nur sehr schnell, sondern auch flexibler als man ihnen zugetraut hätte, reagieren, hätte von uns allen vor zwei Jahren sicher niemand erwartet.

Wir Datenschutzbeauftragten mussten darauf genauso schnell und flexibel reagieren und haben dies auch getan, anders als in manchen Kommentaren und Talk-Shows dargestellt. Wir wissen nämlich, dass Datenschutz kein Selbstzweck und Bürokratiemonster, sondern notwendiger Schutz für Menschen, Unternehmen und Verwaltungen ist.

Vielmehr haben wir in den letzten zwei Jahren feststellen müssen, dass die Digitalisierung weltweit weiter rasch voranschreitet, wir in Deutschland aber leider ziemlich hinterherhinken. Der Datenschutz trägt daran nicht die Schuld, wir drängen vielmehr oft auf durchgängige digitale Lösungen.

II. Digitalisierung schreitet voran

Deutschland verliert beim Innovations-Tempo im internationalen Vergleich an Boden, und zwar deutlich. Das ist auch für uns Datenschützer ein Problem, denn vor allem die Menschen, deren Daten wir schützen wollen, sind die Verlierer mangelhafter Digitalisierung. Eine gut umgesetzte digitale Lösung ist auch aus datenschutzrechtlicher Sicht in den meisten Fällen besser als die analoge Zettelwirtschaft oder unnötige analoge Dateneinsicht, wie z.B. in Personalausweise, Impfbücher & Co.

Der Datenschutz kann seine Aufgabe zum Schutz der verfassungsmäßigen Rechte der Menschen nur dann erfüllen, wenn er selbst Teil der technologischen Entwicklung ist oder mindestens wird. Immer mehr Staaten sind digital innovativer als Deutschland.

Das geht aus dem jüngsten Global Innovation Index der UN-Organisation für geistiges Eigentum hervor. Danach ist Deutschland im Ländervergleich der UN-Organisation für geistiges Eigentum bei Innovationen zurückgefallen. Bei der digitalen Beteiligung der Bevölkerung rutschte Deutschland von Platz 23 im Vorjahr auf Platz 57 ab, bei Digitalangeboten der öffentlichen Verwaltung sogar von Platz 17 auf Platz 59.

Übrigens liegen viele Staaten mit dem gleichen Datenschutzrecht, der europäischen Datenschutzgrundverordnung, vor uns in der Rangliste.

Ich kann mich der Auffassung der Präsidentin des Deutschen Patentamts, Frau Rudloff-Schäffer, nur anschließen, dass die digitale Transformation und das Bewusstsein für die Dringlichkeit ihres Vorantreibens in unserer Gesellschaft noch nicht so ausgeprägt sind wie in anderen Teilen der Welt. Und: „Etwas mehr Dynamik würde unserer Innovationslandschaft guttun."

Dazu brauchen wir hier deutlich mehr weltmarktfähige Produkte. Datenschutz darf angesichts dieser Defizite nicht als Ausflucht dienen, die Digitalisierung nicht anzupacken und zu verschleppen, wir müssen im Gegenteil noch frühzeitiger beraten und prüfen – wenn man uns denn lässt.

Die Corona-Krise hat diese längst bekannten Schwächen bei der Digitalisierung schonungslos offengelegt. Was vor Corona nicht geklappt hat, ist mit Corona implodiert: der fehlende WLAN-Anschuss, antike Endgeräte, mangelnder Austausch oder Zuständigkeitswirrwarr. Das Beispiel der klappernden Faxgeräte in den Gesundheitsämtern, womöglich noch mit Thermopapier, ist hinlänglich bekannt. Die öffentliche Gesundheitsvorsorge ist über viel Jahre hinweg kaputtgespart worden. Diese Versäumnisse haben sich in der Pandemie bitter gerächt.

Ich bin einfach nur entsetzt darüber, dass bis Ende 2021 gerade einmal 16 von insgesamt 575 Verwaltungsleistungen für die Bürger bundesweit online verfügbar sind. Bund, Länder und Kommunen haben sich zwar vorgenommen, auf der Grundlage des Onlinezugangsgesetzes bis Ende 2022 alle 575 Behördenleistungen zu digitalisieren. Ehrgeizige Ziele – wer von uns glaubt, dass das noch zu schaffen ist?

Der unabhängige Nationale Normenkontrollrat, der die Bundesregierung seit 2006 beim Bürokratieabbau berät, hält dieses Ziel für nicht mehr erreichbar. Auch der Deutsche Städte- und Gemeindebund warnte vor einem Scheitern der Regierungspläne für die Digitalisierung der Verwaltungen.

Hier kommt auf die neue Bundesregierung einiges zu. Und sie hat sich viel vorgenommen.

- Ein Transparenzgesetz
- Ein Umweltdatenportal
- Einen Digitalisierungscheck für alle Gesetzesvorhaben

- Eine souveräne Bundescloud
- Den Umbau der Sicherheitsarchitektur
- Ein Datengesetz und ein Dateninstitut
- Ein Beschäftigtendatenschutzgesetz
- Ein Forschungsdatengesetz
- Einen Datenraum Mobilität
- Ein Register- und Gesundheitsdatengesetz

Um nur einige wenige Verabredungen aus dem Koalitionsvertrag zu nennen.

Ich kann nur hoffen, dass sie dabei nicht den Fehlern einiger Digitalisierungsversager aus den Vorjahren folgen und den Schwarzen Peter an den Datenschutz und andere schieben. Ich hoffe sehr, dass sie die tatsächlichen Probleme angehen und Lösungen finden. Mein Haus und ich stehen jedenfalls für die Beratung und Prüfung bereit. Auch für die nationale Umsetzung der vielfältigen europäischen Rechtsetzungsakte wie DA, DGA, DMA, DSA, KI-Regulierung, ePrivacy-Verordnung und Data Spaces.

III. Datenschutz als Differenzierungsmerkmal

Datenschutz ist gelebter Grundrechtsschutz und wichtiger Vertrauensanker für die Digitalisierung unserer freiheitlichen Gesellschaft. Damit hat Digitalisierung eine enorme wirtschaftspolitische Dimension. Hier geht es darum, Prozesse durch die Digitalisierung effizienter zu gestalten. Aber es geht auch darum, z.B. im produzierenden Gewerbe völlig neue Wege zu beschreiten.

Um perspektivisch viel kundenspezifischer, termingerechter und ressourcenschonender zu produzieren.
All diese Systeme müssen „Daten“-sicher sein. Denn es stellen sich neue Herausforderungen, etwa mit Blick auf das Thema Industriespionage und Sabotageschutz. Ohne starken Datenschutz und ein hohes Maß an Datensicherheit steigen die Risiken hierfür massiv an. Gerade in dem ,,Land der Entwickler“ und der vielen kleinen und mittelständischen Unternehmen, die mit ihren Ideen „hidden Champions“ sind, wäre ein Know-how- und Wissensabfluss existenzbedrohend. Wenn Produktionsabläufe und Arbeitsverfahren digitalisiert werden, ist man gut beraten, die genutzten IT-Systeme bestmöglich zu schützen.

Es gilt mein Dauercredo: Datenschutz und Datensicherheit müssen bei der Entwicklung und Entstehung neuer Produkte, Programme und Systeme von Anfang an mitgedacht und mitentwickelt werden. Das ist kostengünstiger, sicherer und ressourcenschonender. Und er schützt eben nicht nur Menschen, sondern auch Ideen und Patente und Wissen und Verfügbarkeit und Glaubwürdigkeit und Kooperationsfähigkeit – und …und …und.

Wie positioniert sich Deutschland und Europa also in dieser vernetzten Welt? Es tritt auf der Stelle, äußert Bedenken und nervt mit Belehrungen. Asien und die USA betrachten technologisch Europa zunehmend in immer mehr Bereichen im Rückspiegel. Europa wird zum reinen Absatzmarkt digitaler Services. Wir haben es bisher selbst kaum geschafft, weltweit agierende IT- und Internetunternehmen hervorzubringen. Wir sollten uns fragen, woran das liegt, auch um werthaltige Arbeitsplätze in Europa zu sichern.

Der erste Reflex bei manchen dürfte ein Wort sein: Datenschutz!

Genau so wenig, wie es Sie überraschen wird, diese vermeintliche Konvexität zu hören, wird es Sie auch nicht verwundern, dass ich da direkt reingrätsche. Mittlerweile fällt mir nicht viel mehr Zurückhaltendes dazu ein. Der Sündenbockstatus des Datenschutzes für Dinge, die nicht funktionieren, ist zwar nicht wirklich etwas Neues, die Quantität seiner Nutzung hat allerdings in den letzten Monaten und Jahren dermaßen zugenommen, dass es beinahe schon selbst eine kleine Pandemie geworden ist.

Mehr technischer Sachverstand und mehr Ehrlichkeit bei den wahren Gründen für Digitalisierungsversagen wäre der einzige Impfstoff dagegen. Wenn es nicht so gefährlich wäre, würde ich das Ganze nur noch genervt hinnehmen. Aber gerade, weil die Behauptung nicht mehr überwiegend aufgrund bloßen Unwissens, sondern gezielt als Falschinformation eingesetzt wird, muss ich klar und immer wieder Stellung zu beziehen.

Daher auch heute: Datenschutz hat bis heute keine einzige geeignete Maßnahme zur Pandemiebekämpfung verhindert. Datenschutz ist keine heilige Kuh, die über allem anderen steht. Und Datenschutz ist kein Wirtschaftshemmnis und damit auch nicht der Sargnagel der deutschen Unternehmen.

Datenschutz könnte vielmehr Innovationsträger und Wettbewerbsvorteil sein, wenn wir uns darauf einlassen!

Lassen Sie mich hierzu einen Vorschlag unterbreiten: 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. 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.

Die Grundsätze des Datenschutzes durch Technikgestaltung („Data Protection by Design“) und der datenschutzfreundlichen Voreinstellungen („Date Protection by Default“) sind ein wichtiger Bestandteil der Datenschutzgrundverordnung (Art. 25 DSGVO).

Ich will aber auch die Hersteller von IT-Verfahren und IT-Produkten stärker in die Pflicht nehmen. Es kann und darf nicht sein, dass es dem Softwarehersteller egal sein kann, ob sein Produkt datenschutzkonform und er nur dann verantwortlich ist, wenn er es selbst einsetzt und damit personenbezogene Daten verarbeitet. Der Grundgedanke der Herstellerhaftung muss auch ins Datenschutzrecht übertragen werden.

IV. Kein Datenschutz ohne IT-Sicherheit

Damit komme ich zu einem weiteren wichtigen Punkt in Sachen Innovation: der IT-Sicherheit. Lassen Sie mich dazu eine ganz zentrale Aussage formulieren, über die glaube ich nicht wirklich eine Diskussion notwendig ist: Es kann IT-Sicherheit ohne Datenschutz geben, aber es gibt keinen Datenschutz ohne IT-Sicherheit. Eine funktionierende IT-Sicherheit ist eine grundlegende Voraussetzung für einen funktionierenden Datenschutz. Ohne IT-Sicherheit funktioniert Datenschutz nicht.

Wie der Zusammenhang aber genau ist, das verdient durchaus einer genaueren Betrachtung, denn Datenschutz braucht nicht nur IT-Sicherheit, sondern er setzt ihr auch Grenzen.

V. Wo steht die IT-Sicherheit in der DSGVO?

Artikel 32 der DSGVO ist der zentrale Artikel für das Verhältnis von IT-Sicherheit und Datenschutz, denn er beschreibt in Verbindung mit Artikel 24 die Anforderungen des Datenschutzes an die Sicherheit der Verarbeitung und lässt keinen Zweifel daran, dass sich der Gesetzgeber hier ein funktionierendes IT-Sicherheitsmanagement vorstellt.

Zum Artikel 32 gleich mehr, zunächst aber noch ein Hinweis auf einen weiteren wichtigen Artikel der DSGVO, nämlich den Artikel 25.

Der Artikel 25 hat in der deutschen Fassung der DSGVO den etwas sperrigen Titel „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, im Englischen etwas einfacher und für IT-ler wahrscheinlich auch verständlicher: „Data Protection by Design and by Default“.

Die Beziehung des Artikels 25 zum Thema „Anforderungen des Datenschutzes an die IT-Sicherheit“, ist etwas indirekter, dafür aber nicht weniger wichtig, denn in Verbindung mit dem Grundsatz der Datenminimierung (formuliert im Artikel 5 Absatz 1 Buchstabe c der DSGVO) beschreibt er eine erste, aber bedeutende Einschränkung für die IT-Sicherheit, so wichtig sie auch sein mag: Da nämlich IT-Sicherheitsmaßnahmen in der Regel auch eine Verarbeitung personenbezogener Daten umfassen, müssen sie selbst so gestaltet sein, dass der Datenschutz in diesem Zusammenhang gewahrt bleibt.

VI. Sicherheit der Verarbeitung und IT-Sicherheitsmanagement

Wenn wir nun den Artikel 32 DSGVO mit dem Titel „Sicherheit der Verarbeitung“ näher betrachten, dann werden sich Fachleute auf dem Gebiet IT-Sicherheit darin sicher schnell „zuhause“ fühlen, denn dieser Artikel enthält eine Menge Begriffe und Konzepte, die direkt aus dem „Lehrbuch der IT-Sicherheit“ kommen:

Der Verantwortliche muss Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitung sicherstellen. Das sind die bekannten Grundwerte der Informationssicherheit und sie bekommen in der DSGVO noch einen weiteren Aspekt zur Seite gestellt, der aber aus der IT-Sicherheit ebenfalls bekannt ist, nämlich die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung.

Außerdem muss der Verantwortliche Maßnahmen ergreifen, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen. Auch wenn das Stichwort selbst nicht wörtlich dort steht, so ist es doch relativ klar, dass damit ein Notfallvorsorgekonzept gemeint ist, denn ohne entsprechende Maßnahmen im Vorfeld eines Zwischenfalls ist der Versuch einer raschen Wiederherstellung in der Regel zum Scheitern verurteilt.

Schließlich fordert der Artikel 32 vom Verantwortlichen noch explizit, ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen umzusetzen. Das heißt: ein IT-Sicherheitsmanagement.

Auf diese Weise stellt der Artikel 32 DSGVO die Verbindung zwischen dem Datenschutz und der IT-Sicherheit her. Denn die genannten Stichworte Vertraulichkeit, Integrität und Verfügbarkeit sind – wie dargestellt – die bekannten Grundwerte der Informationssicherheit.

VII. Der Unterschied: Wer trägt das Risiko?

Bei allen Gemeinsamkeiten und möglichen Synergieeffekten gibt es aber auch Unterschiede: Risiken aus der IT-Sicherheit bzw. aus dem IT-Sicherheitsmanagement sind Risiken für die Organisation, die die Daten verarbeitet. IT-Sicherheitsvorfälle können zu Schäden für die Organisation führen, deren Eintrittswahrscheinlichkeit und Höhe das Risiko bestimmen; Schäden aus diesem Bereich sind letztlich eigentlich immer finanzielle Schäden. Für solche Risiken gibt es Berechnungsmodelle, die letztlich einen Wert liefern, mit dem das Risiko eben „bewertet“ werden kann.

Die DSGVO spricht hingegen von den Risiken für die Rechte und Freiheiten natürlicher Personen. Der Unterschied ist in diesem Fall wirklich nicht fein, sondern grundlegend, denn die „Träger“ des Risikos sind andere: Bei der IT-Sicherheit trägt die Organisation das Risiko und kann abwägen, was sie zur Verminderung des Risikos tun möchte oder ob sie das Risiko vielleicht (abhängig von ihrem „Risikoappetit“) nicht doch einfach tragen möchte.

Die Träger der Risiken bei der Verarbeitung personenbezogener Daten im Sinne der DSGVO sind hingegen diejenigen Personen, deren Daten verarbeitet werden – in der Terminologie der DSGVO die „betroffenen

Personen“. Diese Personen haben keinen Einfluss darauf, wie ihre Daten verarbeitet werden und welche Maßnahmen der Verantwortliche gegebenenfalls zu ihrem Schutz umsetzt. Es geht hier also ganz konkret um Menschen.

Diesen vermeintlichen Zwist zwischen den IT-Abteilungen und den betrieblichen Datenschützern und Rechtsabteilungen kennen Sie wahrscheinlich noch besser als ich. Deshalb bin ich sehr froh, dass die DSGVO auch in diesem Bereich konkrete Handlungsempfehlungen vorgibt, um fruchtlose Diskussionen von vorneherein zu vermeiden.

IV. Schlussbemerkung

Ich bin gelernter Informatiker, deshalb können Sie ganz sicher sein, dass ich weiß, dass digitale Lösungen in der Regel viel datenfreundlicher sind als die analogen. Niemand muss mich überzeugen, dass die Digitalisierung viele Vorteile mit sich bringt und weiter bringen wird.

Aber es muss eben auch jedem klar sein, dass nicht jede Neuerung tatsächlich auch innovativ und gesetzeskonform ist. Die Potenziale der Digitalisierung müssen wir zum Wohle Aller und für eine gute gesellschaftliche und wirtschaftliche Zukunft nutzen. Eine „menschenfreundliche“ Gestaltung digitaler Geschäftsmodelle von Anfang an ist hierfür wichtig und machbar. Wir müssen die Chancen der Digitalisierung nutzen und dabei unsere europäischen Werte bewahren.

Datenschutz und Datensicherheit betrifft eben nicht nur die Menschen in unserem Land, sondern ist auch für Verwaltungen und Unternehmen von zentraler Bedeutung. Wir müssen sicherstellen, dass die Digitalisierung alle mitnimmt und sich alle darauf verlassen können, dass kein Missbrauch mit Daten stattfindet. Vertrauen ist hier von zentraler Bedeutung, für die Menschen wie für die Wirtschaft und Verwaltung.

Die Datenschutzbehörden stehen für diesen Prozess als Partner mit Beratung und Prüfung zur Seite.

Ich danke Ihnen für Ihre Aufmerksamkeit.