Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

← Vorlage mal wechseln

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Erfahrungen mit der Umsetzung der DSGVO und Ausblick auf e-privacy-Verordnung“

Datenschutztag in Köln
RA Karsten Kinast

Mauritiussteinweg 59, 50676 Köln, den 30.10.2019

9.45 Uhr – 10.45 Uhr (incl. Fragen aus dem Publikum)

Es gilt das gesprochene Wort

Sehr geehrter Herr Kinast,

Sehr geehrte Damen und Herren,

liebe Kolleginnen und Kollegen,

Vielen Dank für die Gelegenheit, Ihre erste Datenschutztagung begleiten zu dürfen.

ich habe großen Respekt vor der Kraftanstrengung, neben der täglichen Arbeit in der Kanzlei noch eine Tagung auf die Beine zu stellen.

Ich wünsche Ihrem Vorhaben viel Erfolg. Das Thema Datenschutz braucht mehr Expertise und mehr Expertinnen und Experten, denn es ist ein entscheidendes Thema.

II: Bilanz der DSGVO nach eineinhalb Jahren

Seit dem 25. Mai letzten Jahres macht die Europäische Union endlich Schluss mit dem nationalstaatlichen und daher auch extrem löchrigen Flickenteppich beim Datenschutz. Die DSGVO setzt die Vorgaben der EU-Grundrechtecharta und der Europäischen Menschenrechtskonvention um.

Sie schafft einen verbindlichen Rahmen für Bürgerinnen und Bürger einerseits und Unternehmen sowie Behörden andererseits. Die Menschen haben nun bessere Möglichkeiten, als **Souverän** die Nutzung ihrer Daten zu kontrollieren.

Insofern hätte ich mir in der Zeit vor und kurz nach dem Wirksamwerden der DSGVO von Seiten der Medien und auch Teilen der Fachöffentlichkeit insgesamt doch etwas mehr **Willkommenskultur** gewünscht.

Das Datenschutzbewusstsein ist in dieser Zeit merklich gestiegen. Viele Unternehmen fremdeln aber trotz zwei Jahre Übergangsfrist und achtzehn Monate volle Wirksamkeit immer noch mit dem neuen Recht.

Ich kann dabei ja noch verstehen, dass im Herbst 2017 die Hälfte der Unternehmen in Deutschland mit den Neuregelungen der DSGVO nicht – oder noch nicht – vertraut waren.

Nach einer repräsentativen des Digitalverbands Bitkom haben aber auch heute noch immer Teile der deutschen Wirtschaft mit der Datenschutz-Grundverordnung zu kämpfen.

Zwar haben der Studie zufolge mittlerweile zwei Drittel der Unternehmen (67 Prozent) die neuen Datenschutzregeln mindestens zu großen Teilen umgesetzt. Gleichermaßen hat aber gerade einmal ein Viertel der Unternehmen die Umsetzung vollständig abgeschlossen; 6 Prozent stehen immer noch am Anfang.

Zudem treten Umsetzungsprobleme aktuell gerade da auf, wo es auch schon nach dem alten Bundesdatenschutzgesetz auf der Grundlage der früheren EU-Richtlinie von 1993 gehapert hat.

Nicht wenige Unternehmen haben in Wirklichkeit nichts anderes gemacht als einzugestehen, dass sie viele Jahre nicht rechtskonform gehandelt haben.

III. Fortschritte der DSGVO in Erinnerung rufen

Ich bin mir durchaus bewusst, dass die DSGVO auch Schwachstellen hat. Darauf werde ich noch zu sprechen kommen.

Ich will aber zunächst in Erinnerung rufen, was wir dem neuen Recht alles zu verdanken haben.

Für mich ist die DSGVO ein bedeutender Fortschritt, den es zu verteidigen gilt.

Der Erwägungsgrund 5 der Datenschutz-Grundverordnung bringt es sehr schön auf den Punkt. Die alten national geprägten Regelungen:

- waren ein „*Hemmnis für die unionsweise Wirtschaftstätigkeit*“
- *haben den Wettbewerb verzerrt*
- *und die Behörden an der Erfüllung*“ ihrer unionsrechtlichen Pflichten gehindert.

1. DSGVO stärkt den Schutz der individuellen Rechte in Deutschland, in Europa und weltweit

Die DSGVO schützt die Menschen vor einer Verletzung ihrer Privatsphäre.

Dieser Schutz gilt

- nicht nur vor dem Staat,
- sondern gerade auch vor Unternehmen wie Amazon, Google, Microsoft oder Facebook.

Nach der DSGVO ist der Schutz personenbezogener Daten vor Missbrauch keine Nebenfrage der Digitalisierung. Er ist vielmehr ein Grund- und Menschenrecht. Freiheits- und Persönlichkeitsrechte stehen immer im Mittelpunkt der Rechtsordnung.

Ich wende mich daher auch gegen ein verkürztes Verständnis von „Datensouveränität“, die ein Grundrecht auf die Resterampe ökonomischer Belange und Interessen abschiebt.

Es darf keine Tauschhandel zwischen der Wahrnehmung von Verfassungsrechten und der Gewährung wirtschaftlicher Vorteile geben.

Das käme einem Rabattsystem für Grundrechte gleich.

2. **Datenschutz als Wettbewerbsvorteil**

Zu den Vorzügen der DSGVO gehört des Weiteren die Verpflichtung, die Datenverarbeitung datenschutzfreundlich zu gestalten („***Privacy by Design“ und „Privacy by Default“***).

Hinter dem Begriff „Privacy by Design“ verbirgt sich nichts anderes als **„Datenschutz durch Technikgestaltung“**. Datenschutz kann doch bei Datenverarbeitungsvorgängen dann am besten eingehalten werden, wenn er bereits bei deren Erarbeitung technisch integriert ist.

Die Konzepte „Privacy by design“ und „Privacy by default“ gibt es übrigens bereits seit den 70er Jahren des vergangen Jahrhunderts und auch im „alten“ BDSG waren sie bereits im Zusammenhang mit den Vorschriften zu technisch organisatorischen Maßnahmen verankert. Die DSGVO rückt sie lediglich konkreter ins Rampenlicht und eröffnet damit nach meiner Überzeugung der europäischen Digitalwirtschaft eine große Chance.

IT-Verfahren- und Produkte „made in Europe“ können zu Erfolgsmodellen im internationalen Wettbewerb werden!

Denn dass es für entsprechende Angebote einen immer größer werdenden Markt gibt, ist unbestritten. Nehmen Sie nur Apple als Beispiel, die einen zweistelligen Millionenbetrag für eine Werbekampagne ausgegeben hat, mit der ausschließlich Datenschutzfeatures ihrer Produkte herausgestellt werden. Datenschutz wird also auch jenseits des Atlantiks immer wichtiger, unter anderem weil aufgrund des Marktortprinzips nun endlich auch die großen weltweit operierenden **Großkonzerne** an das europäische Regelwerk gebunden sind.

3. Internationale Fortschritte durch die DSGVO

Sogar über das Marktortprinzip hinaus hat sich die DSGVO mittlerweile allen Unkenrufen zum Trotz zu einem internationalen **Standard entwickelt. Daran orientieren sich auch andere Weltregionen.**

Die Entwicklungen in Japan, aber auch das hohe Interesse weiterer Staaten in Lateinamerika und Asien belegen die internationale Wertschätzung unseres neuen Datenschutzrechts eindrucksvoll.

In Kalifornien wurde als **Reaktion auf den Facebook-Skandal nach dem Vorbild der DSGVO der "California Consumer Privacy Act" verabschiedet.** Unternehmen müssen dort ab dem 1. Januar 2020 zum Beispiel offenlegen, welche Kunden- und Nutzerdaten sie speichern. Die Nutzer wiederum erhalten das Recht, die Verwendung ihrer persönlichen Daten zu kommerziellen Zwecken zu unterbinden. Internetfirmen werden verpflichtet, einen Link anzubieten, der es den Nutzern erlaubt, ohne Papierkrieg den Weiterverkauf ihrer Daten verhindern.

Kalifornien ist der Sitz zahlreicher Technologiekonzerne, so dass dem neuen Gesetz eine wichtige Pilotfunktion auch für andere US-Staaten und entsprechenden Überlegungen zu einem nationalem Datenschutzrecht zukommt. NY, Washington, Illinois und andere wollen folgen.

Dass die DSGVO auf internationaler Ebene Eindruck hinterlassen hat, beweist auch das Verhalten von Facebook-Chef Zuckerberg. Er bezeichnete vor dem US-Kongress und dem Europäischen Parlament die Grundverordnung als vorbildlich.

Auch wenn er dabei natürlich an die Zukunft seines unter Druck geratenen Geschäftsmodells denkt: auch er kann das europäische Recht nicht länger ignorieren.

III.China als abschreckendes Beispiel

Was wir an der DSGVO zu verdanken haben, zeigt sich sinnbildlich dort, wo die Digitalisierung für eine systematische Verletzung von Grund- und Menschenrechten ge- oder besser gesagt missbraucht wird.

Wie schnell technischer Fortschritt zum staatlichen Machtinstrument für die Unterdrückung seiner Bürgerinnen und Bürger verkommt, zeigt das Beispiel China.

- Setzt die DSGVO an einigen Orten der Welt positive Impulse, passiert an anderer Stelle das genaue Gegenteil.

- Will die DSGVO die Rechte der Bürgerinnen und Bürger auch institutionell stärken, nutzen andere Staaten die moderne Informationstechnik zur Totalüberwachung und Gängelung der Bürgerinnen und Bürger. Im Bündnis mit den Unternehmen dieser Region.

- Sagen bei uns noch immer Viele aus der Geborgenheit einer funktionierenden Demokratie heraus: **ich habe nichts zu verbergen** – müssen sich anderswo Menschen für einen Telefonanschluss eine noch vor wenigen Jahren selbst in dystopischen Romanen nicht vorstellbare Rundumüberwachung hinnehmen und dem Regime gegenüber devotes Wohlverhalten zeigen.

Mit einem als **gesellschaftliches Bonitätssystem** umschriebenen Verfahren entwickelt das Land eine völlig neue Variante von Big Data. Bürgerinnen und Bürger sollen ebenso wie NGOs und Unternehmen

- umfassender überwacht,
- ständig neu bewertet,
- und beständiger kontrolliert werden als die schon bei uns vielfach beklagten Systeme zur Bewertung der Kreditwürdigkeit.

Im Vergleich dazu ist sogar das auch von mir heftig kritisierte Scooring hierzulande ein datenschutzrechtlicher Kindergeburtstag.

Überwachungssysteme dieser neuen Art haben direkte - und gerade auch - indirekte Auswirkungen auf das Verhalten von Menschen, NGOs und Unternehmen.

Wer pariert wird belohnt, wer quer denkt und handelt, muss erhebliche Nachteil in Kauf nehmen. Schlechte Bewertungen können sowohl privat als auch geschäftlich negative Folgen haben:

- schlechtere Bedingungen für die Aufnahme eines neuen Kredits,
- Reisebeschränkungen,
- höheres Steuerniveau im Vergleich zu regelkonformen Konkurrenten,
- keine Erlaubnis, Anleihen zu emittieren oder in börsennotierten Unternehmen anzulegen,
- geringere Chancen, an öffentlich geförderten Projekten teilzunehmen,
- verpflichtende staatliche Genehmigungen für Investitionen bei denen der Marktzugang normalerweise nicht reguliert ist.

Wer nicht nach der Pfeife der Staatspartei tanzt, riskiert eine Sperrung von Online-Handelskonten des betreffenden Unternehmens und sogar eine Verschlechterung der individuellen Bonitätsbewertungen der Verantwortlichen des Unternehmens.

Ich sage das auch in Richtung von deutschen Unternehmen, die sich über ihr schweres Schicksal unter der DSGVO beklagen und die angebliche digitale Offenheit in China loben.

In der **deutschen Klage-Debatte** über das schwere Schicksal derer, die als Verantwortliche den Datenschutz zu beachten haben, fehlt mir oft die grundlegende Wertschätzung für Rechtsstaatlichkeit und Bürgerrechte.

IV. Die Evaluierung der DSGVO

1. Chance auch für Bürokratieabbau

Wenn ich die großen Fortschritte der Grundverordnung hervorhebe, bin ich mir natürlich immer bewusst, dass die DSGVO auch Schwächen aufweist.

Der europäische Gesetzgeber hat mit Weitblick in der DSGVO den **Evaluierungsprozess als Grundlage für ihre Weiterentwicklung** festgeschrieben. Der Prozess soll bis Mai des kommenden Jahres abgeschlossen sein.

Ich hoffe sehr, dass die Reformvorschläge nicht auf taube Ohren stoßen. Es gilt, den Datenschutz an den Stellen zu verbessern, die noch nicht zufriedenstellend gelöst sind.

Ziel muss es sein, mit so wenig Bürokratie wie nötig so viel Datenschutz wie möglich zu erreichen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder befassen sich zurzeit intensiv mit der **anstehenden Evaluierung**. Diese wird zwar in erster Linie von der Europäischen Kommission durchgeführt, aber die Kommission ist gehalten, die Datenschutzaufsichtsbehörden mit einzubeziehen. Vor diesem Hintergrund wollen wir Datenschützer vorbereitet sein und haben bereits eine Reihe von Themen herausgegriffen.

3. Weiterentwicklung durch Stärkung des Datenschutzes

Mit der DSGVO haben wir 2016 Regeln bekommen, die die Rechte von Nutzerinnen und Nutzern stärken. Sie gelten für alle Arten von Technologien.

Leider sind wir aber noch weit davon entfernt, das ganze Ausmaß der Datensammlung und -auswertung zu durchblicken. Auch aktuell führen intransparente Geschäftspraktiken nach wie vor dazu,

- dass das menschliches Verhalten heimlich und beständig beobachtet wird
- und in umfassenden Profilen gewaltige Mengen sensibler Daten zusammengeführt werden.

Weiterentwicklung der DSGVO heißt daher auch, an zentraler Stelle datenschutzrechtliche Vorgaben zu stärken, statt sie abzubauen:

Spätestens **seit dem Skandal um Cambridge Analytica** müsste jedem klar geworden sein, dass wir rote Linien für personalisierte Werbung brauchen. Es muss klar sein, wo sie grundsätzlich tabu sein muss. Die Grenze zwischen personalisierter Werbung und psychologischem Profiling hat sich längst verflüssigt. Es lohnt sich, beim Datenschutz mutiger zu sein und mehr einzufordern.

Die Aufsichtsbehörden müssen sich endlich die großen Internetkonzerne vorknöpfen.

Die EU-Datenschutz-Grundverordnung hat Verbraucherrechte entscheidend gestärkt. Es werden aber bereits jetzt Schwachstellen sichtbar. Die Regelungen zu Tracking und Profilbildung sind nicht im Sinne der Verbraucher. Hier muss im Rahmen der Evaluation 2020 nachgebessert werden.

Algorithmen dürfen nach der DSGVO nicht allein darüber entscheiden, ob wir einen Kredit, einen Job oder ein bestimmtes Produkt bekommen.

Außerdem können Verbraucherinnen und Verbraucher verlangen, Logik, Tragweite und die angestrebten Auswirkungen einer automatisierten Entscheidung zu erfahren.

Die Datenschutzaufsichtsbehörden müssen deshalb gegen Geschäftsmodelle vorgehen können, die weiterhin auf versteckten Tracking und voraussagendem Profiling basieren.

Ich muss jedoch einräumen, dass wir noch lange nicht in der Lage sind, diese Black Boxes zu öffnen. Es ist an der Zeit, dass diese Wissenslücke geschlossen wird.

Wichtig ist auch, dass NGOs künftig die Möglichkeit in die Hand bekommen**, Sammelklagen** einzureichen. Ohne dieses Instrument ist eine wirksame Umsetzung der DSGVO deutlich erschwert oder sogar blockiert.

V. Verschärftes Sanktionssystem

1. Übergangszeit für die DSGVO ist beendet

Ich habe eingangs bereits angesprochen: Unternehmen hatten inzwischen über 3 Jahre Zeit ihre Prozesse anzupassen.

Dass man in der täglichen Arbeit ggf. auf neue, i.S. von bisher nicht erkannte oder bearbeitete Fragestellungen trifft, weiß ich auch. Ich bitte in diesen Fällen darum, Problem zeitnah anzugehen und mit der zuständigen Aufsichtsbehörde zu klären.

Wir Aufsichtsbehörden können und werden bei Verstößen vermehrt Abhilfemaßnahmen einfordern, und bei Bedarf auch Geldbußen verhängen. Sonst lachen sich die ins Fäustchen, die sich um die Umsetzung nicht gekümmert haben, während sich andere Unternehmen sehr engagiert haben.

Im Einzelfall werden diese **Geldbußen auch drastisch** ausfallen, z.B. wenn wiederholte gleichartige Verstöße vorliegen oder grundlegende technische oder organisatorische Mängel bestehen. Dies gilt besonders, wenn selbstgeschaffene Strukturen (z.B. ein unkontrolliertes Vertriebssystem) oder veraltete und nicht dem Stand der Technik entsprechende technisch-organisatorische Maßnahmen Verstöße begünstigen.

Wer z.B. Passwörter für Onlinezugänge immer noch unverschlüsselt speichert (ja, das gibt es!), dem rufe ich das alte Sprichwort ins Gedächtnis: Dummheit schützt vor Strafe nicht.

Der BfDI erwartet, dass Unternehmen gut mit den Aufsichtsbehörden zusammenarbeiten, auf Fragen zeitnah antworten und angeforderte Unterlagen herausgeben. Viele angefragte Unterlagen müssen im Rahmen der Rechenschaftspflicht ohnehin vorliegen.

Ich werde es **nicht länger hinnehmen**, zum Teil wochen- oder gar monatelang vertröstet und manchmal auch „hingehalten“ zu werden. Es kann beispielsweise nich angehen, dass uns eine beaufsichtigte Stelle im Juni schreibt, dass sie aufgrund der bevorstehenden Urlaubszeit eine Anfrage von uns aus dem April leider erst im Herbst beantworten kann.

Ich sage deutlich: Die fehlende Zusammenarbeit mit einer Aufsichtsbehörde ist bußgeldbewehrt. **Auch die Herausgabe von Dokumenten kann mit Zwangsgeld durchgesetzt werden.**

Unternehmen sind verpflichtet, die Abläufe im gesamten Konzern entsprechend auszurichten und ggf. auch ihre Vertriebspartner auf Einhaltung des Datenschutzes zu kontrollieren.

Die betrieblichen Datenschutzbeauftragten haben dabei eine besonders wichtige Funktion. Sie müssen die Geschäftsleitung beraten und rechtzeitig auf mögliche Verstöße hinweisen. Dieser Präventionsgedanke ist mir sehr wichtig.

VI. E-Privacy-Verordnung

„Die DSGVO allein kann es nicht richten. Das Datenschutzniveau in Europa muss noch besser werden“

Ich teile diese Auffassung von Klaus Müller vom Verbraucherzentrale Bundesverband.

Dazu brauchen wir eine ePrivacy-Verordnung, die ihrem Namen gerecht wird. Dieses essentielle Puzzelstück zur Vervollständigung der Reform des europäischen Datenschutzrechts wird aber derzeit vom EU-Rat verschleppt.

Die neue ePrivacy-Verordnung soll die in die Jahre gekommene Richtlinie ablösen und in Zukunft einen besseren Schutz der Privatsphäre in der Kommunikation und im Internet rechtlich sicherstellen.

Dabei ist die Reform des E-Privacy-Regimes ein kompliziertes und manche Gratwanderung herausforderndes Vorhaben: Einerseits soll die E-Privacy-VO den Schutz des Privatlebens im Bereich der elektronischen Kommunikation effektuieren, gleichzeitig darf sie es Unternehmen nicht unmöglich machen, neue Geschäftsmöglichkeiten zu entwickeln. Dieser Spagat kann m.E. aber auch mit klaren und strikten Regelungen einhergehen, da ich fest davon überzeugt bin, dass Datenschutz und Innovation kein Widerspruch sind, sondern sich sogar gegenseitig fördern können.

Die E-Privacy-VO soll die in der DSGVO festgelegten allgemeinen Vorschriften über den Schutz personenbezogener Daten in ihrem spezifischen Bereich präzisieren und ergänzen. Im Hinblick auf den sensiblen Charakter der elektronischen Kommunikationsdaten darf die E-Privacy-VO zu keiner Absenkung des Schutzniveaus führen, das die DSGVO natürlichen Personen angedeihen lässt.

So darf beispielsweise das Koppelungsverbot der DSGVO nicht dadurch unterlaufen werden, dass die Nutzung bestimmter elektronischer Kommunikationsdienste davon abhängig gemacht werden, dass der Nutzer in die Verarbeitung seiner personenbezogenen Daten z.B. zum Zweck der personalisierten Werbung einwilligt (sog. Cookie-Walls).

Ebenso müssen die Ausnahmen, zu denen die Verwendung der sensiblen Kommunikationsdaten zugelassen werden, eben solche bleiben und nur sehr restriktiv vorgesehen werden. Das gilt nicht nur für die Verarbeitung dieser Daten durch die TK-Unternehmen selbst, sondern auch für die Zugriffsbefugnisse für Sicherheitsbehörden.

Die Reform des E-Privacy-Regime gibt uns Gelegenheit, wichtige Weichen für die Zukunft der elektronischen Kommunikation zu stellen. In diesem Kontext ist es mir ein wichtiges Anliegen, dass die Grundsätze von Privacy-by-Design und Privacy-by-Default eine gebührende Berücksichtigung in der E-Privacy-VO finden.

Der in den Entwürfen der europäischen Kommission und des europäischen Parlaments enthaltene Ansatz, Softwarehersteller zu verpflichten, nutzerfreundliche Datenschutzeinstellungen vorzusehen, halte ich für einen wichtigen ersten Schritt in diese Richtung.

VII. Schlussbemerkung

Nach der Reform ist vor der Reform.

Die DSGVO hat sich bewährt, sollte aber an bestimmten Stellen nachjustiert und vor allem entbürokratisiert werden.

Die E-Privacy-Verordnung wird hoffentlich bald kommen und die noch vorhandenen rechtlichen Lücken schließen.

Die Umsetzung der DSGVO war ein großer Kraftakt, der noch lange nicht abgeschlossen ist. Im Interesse der Grundrechte der Bürgerinnen und Bürger lohnt sich aber all diese Mühe.

Ich hoffe sehr, dass der kritische Dialog, so wie er in diesem Rahmen geführt wird, den Grundrechtsschutz durch Datenschutz und dessen technische Umsetzung auch weiterhin begleiten wird.

Ich danke Ihnen für Ihre Aufmerksamkeit.