Weitergehende Erkenntnisse aus den Verhandlungen zur EU-Datenschutzgrundverordnung

Zusammenfassung des Vortrags von Jan Philipp Albrecht

Welche Grundannahmen der Unternehmen und staatlichen Akteure haben sich in den DSGVO-Verhandlungen gezeigt? Welche Punkte waren ihnen sehr wichtig, welche eher weniger, und was kann man daraus ableiten, wie ihre zukünftigen Geschäftsmodelle aussehen?

Einleitend dankte Jan Philipp Albrecht dem FIfF für die Einladung. Es sei seine erste größere FIfF-Veranstaltung, er verfolge aber die Aktivitäten des FIfF regelmäßig und lese die *FIfF-Kommunikation*; während den Verhandlungen habe er die ganze Zeit die Cyberpeace-Taube auf dem Notebook gehabt. Es sei wichtig, deutlicher als bisher auf die Bedeutung von Technikregulierung, Technikfolgenabschätzung und Ethik für die Politik und die großen politischen Entscheidungen hinzuweisen; viele hätten das noch nicht erkannt. In der Politik Tätige müssten erkennen, dass der entsprechende Sachverstand und die Wahrnehmung dieser Themen ins Zentrum der politischen Auseinandersetzung rücken müssen – er ist aber auch der Ansicht, dass das in vielen Bereichen heute bereits passiert.

Die Arbeit an der Datenschutz-Grundverordnung habe ihren Teil dazu beigetragen, die Aufmerksamkeit für die Frage zu verstärken, wie Technik unser Leben verändert. Der Datenschutz als der Ausgangspunkt vieler weiterer Grundrechte und Regulierungsansätze in der Digitalisierung spiele dabei eine wichtige Rolle.

Bedeutung und Entwicklung der Datenschutz-Grundverordnung

Datenschutz und die damit verbundene informationelle Selbstbestimmung sind ein vorgelagertes Grundrecht; sie entspringen der Würde des Menschen. In Folge des Volkszählungsurteils findet sich damit der Datenschutz in den Verfassungen Deutschlands und aller europäischen Länder wieder. Seit 2009 ist er auch verbindlich im Vertrag der EU verankert. Artikel 16, einer der grundlegenden Vertragsgrundsätze, legt fest, dass jeder ein Recht auf den Schutz seiner persönlichen Daten hat. „Jeder" heißt auch wirklich *jeder*; der Datenschutz ist ein Menschenrecht, nicht nur ein Bürgerrecht. Auch in Artikel 8 der Charta der Grundrechte der Europäischen Union ist er als Schutzauftrag und Freiheitsrecht verankert.

Datenverarbeitung ist nur auf zwei Grundlagen zulässig: der Einwilligung des Betroffenen oder einer gesetzlichen Bestimmung. Artikel 16 enthält den Auftrag an den EU-Gesetzgeber, Gesetze zu verabschieden, um dieses Grundrecht zu schützen. Die EU-Kommission hat dies nach Inkrafttreten des Lissabon-Vertrags in Angriff genommen und 2009/10 ein entsprechendes Gesetzgebungsverfahren auf den Weg gebracht. Dieses Verfahren hat ca. 5–6 Jahre gedauert, begonnen mit dem in diesen Fällen üblichen Konsultationsverfahren. 2012 wurde ein Vorschlag für eine Verordnung unterbreitet, die nationale Gesetze in ihrem Regelungsbereich ersetzt. Im April 2016 wurde die Verordnung dann endgültig vom Ministerrat angenommen; sie gilt nach einer zweijährigen Übergangsphase ab dem 25. Mai 2018. Sowohl diejenigen, die mit Datenschutz befasst sind, als auch alle anderen sollten sich das Gesetz genau anschauen: Welche Rechte und Pflichten gibt es beim Datenschutz?

Jan Philipp Albrecht

Man darf sich dabei nicht abschrecken lassen von ungewohnten Begriffen. Es ist ein Gesetz für 28 Staaten in der Europäischen Union, und damit ein Kompromiss zwischen diesen 28 Staaten. Darin besteht gleichzeitig der große Mehrwert: Im europäischen Raum wird es künftig eine einheitliche Regelung für den Datenschutz im gesamten gemeinsamen Binnenmarkt geben; dies ist gegenüber der heutigen Situation ein großer Fortschritt. Viele Unternehmen verarbeiten eine große Menge an Daten – dabei war der Umfang der Verarbeitung in den letzten Jahren sehr expansiv. Es ist zu erwarten, dass sich dieser Trend fortsetzt und weiter verstärkt. Dabei versuchen Unternehmen, die heutigen Regelungen zu umgehen, indem sie sich in einem Land mit niedrigen Standards niederlassen und dessen Gesetze für sich nutzen. Außerdem überblicken viele Betroffene nicht, welche Datenschutzregelungen im konkreten Fall eigentlich gelten. Verbraucher.innen müssen durch alle Instanzen der Gerichte gehen, um ihre Rechte einzufordern – dies ist nicht zumutbar.

Der Datenschutzaktivist Max Schrems aus Österreich hat diesen Klageweg beschritten, um das Safe-Harbour-Abkommen anzugreifen; sein Fazit danach war: Wer seine Rechte einklagen will, sollte sich das zweimal überlegen; eigentlich funktioniert es so, wie es heute geregelt ist, nicht. Es muss immer klar sein, welche Regeln gelten, und es muss möglich sein, seine Rechte im eigenen Land einzuklagen. Das ist einer der großen Fortschritte der Verordnung: In ganz Europa gilt das gleiche Gesetz und kann an

allen Gerichten eingeklagt werden. Das Gesetz wird europaweit einheitlich ausgelegt. Die Datenschutzbehörden müssen sich europaweit vernetzen und eine gemeinsame Linie bei der Auslegung einnehmen.

Inhaltliche Regulierung

Welchen Datenschutz erhalten wir durch die neue Verordnung? Das Gesetz war sehr umstritten, wird aber hochrelevant sein für alle, die in der Datenverarbeitung tätig sind. Es wird ihre Tätigkeit künftig massiv bestimmen.

Die Interessenvertretungen einflussreicher Unternehmen haben von Beginn an versucht, massiv Einfluss auf die Verordnung zu nehmen. Es gab gegenüber dem ursprünglichen Parlamentsentwurf ca. 4.000 Änderungsanträge. Diese zu verarbeiten war eine umfangreiche Arbeit und es hat lange gedauert, die Gedanken hinter allen diesen Änderungsanträgen zu verstehen.

Es gibt eine anhaltende Debatte in Europa, welche Kontrolle der Einzelne über seine Daten haben soll, wenn es z. B. um Geschäftsmodelle geht, die darauf aufbauen, dass möglichst viele Leute ihre Daten preisgeben und man als Anwender nicht die Möglichkeit hat, sich der Datenverarbeitung zu entziehen. Zusätzlich gibt es ein öffentliches Interesse von Behörden, Daten zu erheben. All dies schränkt die Möglichkeit Einzelner ein, die Verwendung ihrer Daten zu kontrollieren.

Diese Auseinandersetzung findet ständig statt und wird intensiver, wenn sich die Gesellschaft einmal daran gewöhnt hat, dass bestimmte Informationen über alle zur Verfügung stehen, oder dass es Geschäftsmodelle gibt, die auf diesen Daten basieren. Im Nachhinein ist es schwierig, festzustellen und durchzusetzen, dass der Umfang der Datenverwendung über die Selbstbestimmung des Einzelnen hinausgeht. In vielen Bereichen sind wir heute schon zu weit gegangen, dies muss wieder revidiert werden. Einzelne Geschäftsmodelle sind bereits heute nicht mehr mit dem geltenden Datenschutzrecht vereinbar, zum Beispiel die Praxis der Datensammlung durch Browser-Apps. Doch die Durchsetzung des Rechts stößt auf Widerstand, wenn solche Geschäftsmodelle bereits umgesetzt sind.

Die europäischen Unternehmen stehen im Wettbewerb mit Unternehmen im Silicon Valley, die datenintensive Dienste marktbeherrschend anbieten. Konkurrenzfähig sind diese europäischen Unternehmen nur, wenn sie nicht unter unfairen Wettbewerbsbedingungen gegen die Konkurrenz unter unterschiedlichen Rechtsordnungen antreten müssen. Möglich ist dies unter zwei Bedingungen:

1. Man senkt die hiesigen Standards auf das im Silicon Valley geltende, niedrige Niveau ab – darauf haben viele gedrängt: Sonst würden die europäischen Unternehmen wettbewerbsunfähig.

2. Man gestaltet die Regelungen so, dass sich alle Wettbewerber an einen hohen Standard halten müssen. Dieser hohe Standard wird so fortgeführt, wie er über die letzten 30–40 Jahre entwickelt wurde. Wenn sich Wettbewerber nicht daran halten, werden angemessene Sanktionen verhängt.

Die EU-Datenschutzgrundverordnung setzt mit der Idee des Marktortprinzips die zweite Variante um: Jeder, der im Geltungsbereich der Verordnung Dienste oder Waren anbietet, muss sich an ihre Regeln halten, sonst drohen Strafen in Höhe von bis zu 4 % des weltweiten Umsatzes. Auf diese Weise kann der Standard gehalten und durchgesetzt werden.

Aus Sicht des Europäischen Parlaments darf die Verordnung nicht hinter den heutigen Standard zurückfallen; dies ist in der durch die Grundrechte gesetzten Situation gar nicht möglich. Deswegen haben sich auch große Unternehmensverbände hinter den Vorschlag gestellt. Dieser Vorschlag stellt das Vertrauen in das Recht wieder her. Weltweit werden Dienste aus Europa im Markt angenommen, auch technologisch anspruchsvolle Dienste.

Weitere Eckpunkte

Wichtige einklagbare und sanktionierbare Eckpunkte des Datenschutzes sind:

- Die Gestaltung der Einwilligung für den Anwender: Eine „stillschweigende“ Einwilligung, z. B. durch vorangekreuzte Kästchen, ist nicht als informierte Einwilligung gültig. Nur eine aktive Handlung zur Datenfreigabe zählt als Einwilligung.

- Die Verordnung macht einen großen Schritt hin zu mehr Transparenz: Verständlichkeit, einfache Sprache, wiedererkennbare standardisierte Symbole. Über alle wesentlichen Aspekte muss der Anwender informiert werden: Weitergabe in Drittstaaten, Automatisierung der Verarbeitung, nach welchen Kriterien Daten verarbeitet werden – all das muss in Zukunft offengelegt werden.

- Es werden neue Rechte geschaffen, z. B. auf Datenportabilität: Das Recht, dass Anwender.innen ihre Daten in maschinenlesbarem Format bekommen können oder dass der bisherige Anbieter die Daten an einen anderen Anbieter mit besseren Konditionen weitergibt.

- Es besteht nun eine verstärkte Löschungsverpflichtung auch im Internet. Das Recht auf Vergessenwerden wird etabliert.

- Datenverarbeiter erhalten deutlich weiter gehende Pflichten als bisher. Das Modell des Datenschutzbeauftragten wird europaweit verpflichtend gemacht. Bildung und Wahrnehmung von Datenverarbeitungsvorgängen soll verstärkt werden und sich durchsetzen; es soll deutlich mehr Aufmerksamkeit durch Technikfolgenabschätzung geben. Bei Data Breaches gibt es eine verbindliche Meldepflicht, dadurch wird mehr Aufmerksamkeit auf Datenschutz und Konsequenzen der Datenverarbeitung gelenkt.

Albrecht zieht ein positives Fazit: Es kann gelingen, über die Gesetzgebung deutliche Fortschritte zu erreichen, auch wenn das zunächst nicht erkennbar ist. Es gibt eine große Chance, über die EU und ihren globalen Machtfaktor Standards zu setzen. Das gilt auch für weitere Themen: IT-Sicherheitsstandards, die Nutzung von Open Source etc. – dafür müssen wir uns auf die entsprechenden Prozesse einlassen. Es geht um neue politische Debatten, die über die deutschen Debatten hinausgehen.

Diskussion

Wie kann das Bewusstsein für den Datenschutz und seine Bedeutung geweckt werden? Aufsichtsbehörden und Verbände müssen gerade bei alltäglichen Fällen darauf hinweisen, dass man immer überprüfen muss: Was wird mit den Daten gemacht? Es muss eine verpflichtende Technikfolgenabschätzung geben.

Die Verordnung wurde im Vortrag sehr positiv geschildert, dies ist auf europäischer Ebene nachvollziehbar. Aber: Im Vergleich zum heutigen Bundesdatenschutzgesetz gibt es teilweise große Rückschritte. Auch Albrecht hatte diese Befürchtung zu Beginn – aus seiner Sicht ist es dazu aber nicht gekommen. Die Unterstellung, dass es in anderen Ländern der EU keine vergleichbaren Datenschutzbestimmungen wie in Deutschland gibt, stimme so nicht. Die Datenschutz-Grundverordnung ist nicht vollkommen neu. Lediglich Begriffe wurden bisher unterschiedlich interpretiert. Hohe Standards waren schon bisher EU-weit vorhanden. Aus seiner Sicht gibt es fast keine Rückschritte, Ausnahmen dazu gibt es evtl. bei der Videoüberwachung (aber aus seiner Sicht keine niedrigeren Standards) und bei einem anderen Berechnungsschlüssel für betriebliche Datenschutzbeauftragte, aber auch hier gebe es keine Verschlechterung. Die EU-Datenschutzgrundverordnung geht in einigen Punkten über den bisherigen deutschen Datenschutz hinaus, z. B. durch konkrete Anforderungen an informierte Einwilligung – und das mit Gültigkeit in ganz Europa. Heute ist man zwar vom BDSG geschützt, das hilft aber nicht, wenn ausländische Dienste genutzt werden, wie z. B. Dienste von Facebook, Google, Apple, … Gleichzeitig kann man bei einem Kompromiss zwischen 28 Ländern nicht erwarten, dass die eigenen Formulierungen immer überall akzeptiert werden. Das ist der Preis der Globalisierung; die Alternative wäre der Rückzug ins Nationale. Das bedeutet nicht, dass alles perfekt ist. Weitergehende Regelungen zu Direktmarketing, Vertragsschluss mit Opt-out wären beispielsweise wünschenswert gewesen. Aber die Durchsetzbarkeit des Rechts macht die Verordnung zu einem großen Erfolg.

Großes Lob für die Transparenz, welche Lobbygruppe welche Vorschläge gemacht hat. Wie kann man diese Transparenz allgemein erreichen? Welche Visualisierungstechniken sind dafür geeignet, welche Erfahrungen gibt es dazu? Die Open-Data-Darstellung wurde von Aktivisten aus Hamburg erstellt. Damit wurde ein Einblick für Journalisten in ein sehr komplexes Themengebiet geschaffen. Wenn sich mehr Menschen engagieren, solche Projekte stärker gefördert werden und es Vereinfachungen und Möglichkeiten gibt, diese Informationen abzurufen, dann ist auch mehr Partizipation an solchen Prozessen möglich. Die Wahrnehmung für die Wichtigkeit dieser Transparenz ist noch nicht groß genug; wir müssen die Frage der Zugänglichmachung und Visualisierung zum Thema machen. Engagement im Bereich der Informationsfreiheit ist wichtig, aber ein dickes Brett. Es gibt bisher keine IFG-Regeln für Mitgliedsländer der EU.

Für die IT-Sicherheit brauchen wir eine europäische IT-Infrastruktur, die die europäischen Regeln einhält. Kann diese Infrastruktur erreicht werden? Ab Anfang des Jahres 2017 soll eine neue Richtlinie für IT-Sicherheit für kritische Infrastrukturen erarbeitet werden. Im Gesetzgebungsverfahren für Standards und Verbraucherschutz müssen Regeln für IT-Sicherheit durchgesetzt werden, die über Produkthaftung hinausgehen. EU-weite Standards sind dabei wichtig. Allerdings steht das heute industriepolitisch nicht im Vordergrund; z. B. bei Hardwareproduktion gibt es keine entsprechenden Angebote durch europäische Anbieter; es muss wieder ein wettbewerbsfähiges europäisches Angebot geben. Dazu brauchen wir Standards, die überprüfbar sind, z. B. sollte Open Source zum Standard gemacht werden. Produkte – beispielsweise von Microsoft – sind nicht überprüfbar; gleichzeitig kann durch die Transparenzforderung auch die europäische Industrie gefördert werden. Die Industrieverbände beschränken sich stattdessen leider auf den Kampf gegen ein Haftungsregime für Sicherheitsstandards.

Fast alle Regelungen der Verordnung sind auf dem Niveau des BDSG – gibt es eine Seite, wo es Konfliktfelder und Bruchstellen gibt? Dies sind Detailfragen; grundsätzlich gibt es keine großen Unterschiede. Die Linie des Datenschutzes wird weitestgehend gehalten; dies hängt aber auch von der nationalen Gesetzgebung ab. Die deutsche Initiative zielt auf Absenkung der Standards ab, z. B. bei der Zweckbindung. Deutschland entwickelt sich derzeit zum „Schmuddelkind" beim Datenschutz. Einen Vergleich der Verordnung mit dem bisherigen Recht gibt es bisher in Handbüchern; es existieren synoptische Darstellungen, auch in der eigenen Publikation.

Das Recht auf den Export eigener Daten aus sozialen Netzwerken und Recht auf Löschen wurden genannt. Ist das nun in der Verordnung enthalten? Ja, beides ist enthalten.

Was, wenn sich der Betreiber einer Webseite nicht an die Regelungen hält? Es gibt eine Beschwerdemöglichkeit bei Aufsichtsbehörden, auch bei eigenen Behörden. Diese ist einklagbar bei Gerichten im eigenen Land.

Welche Regelungen gelten für Tracking-Cookies? Tracking-Cookies sind durch die Regelungen abgedeckt; dies ist abhängig vom Zweck der Cookies: IT-Sicherheit und Gefahrenabwehr vs. Werbung. Hier ist auch die E-Privacy-Richtlinie zu beachten, diese soll ebenfalls demnächst reformiert werden. Hier muss die informierte Einwilligung auch eine zentrale Rolle spielen.

Jan Philipp Albrecht

Jan Philipp Albrecht sitzt für die Grünen im EU-Parlament und verhandelte dort wesentlich die EU-Datenschutzgrundverordnung. Zudem ist er dort stellvertretender Vorsitzender des Innenausschusses. Davor spezialisierte er sich in IT-Recht an den Universitäten Hannover und Oslo. Seither lehrt er neben seiner Abgeordnetentätigkeit Europäische Rechtsinformatik an der Universität Wien und schreibt juristische Fachbeiträge.