Hanns Seidel Stiftung

www.hss.de

Tagungsbericht

Die Europäische Datenschutzreform und ihre Auswirkungen auf Recht und Wirtschaft

Ass. jur. Kea-Sophie Stieber

Expertentagung
der Hanns-Seidel-Stiftung
am 31. März 2016
im Konferenzzentrum München

Empfohlene Zitierweise

Beim Zitieren empfehlen wir hinter den Titel des Beitrags das Datum der Einstellung und nach der URL-Angabe das Datum Ihres letzten Besuchs dieser Online-Adresse anzugeben.
[Vorname Name: Titel. Untertitel (Datum der Einstellung).
In: http://www.hss.de/...pdf (Datum Ihres letzten Besuches).]

Die Europäische Datenschutzreform

Im Zuge einer sich in Sachen Datenverbrauch, -erhebung und -austausch immer weiter und schneller entwickelnden Welt, hat die Europäische Kommission bereits am 25. Januar 2012 die beabsichtigte EU-Datenschutzreform vorgestellt. Ziel der Reform ist, den Schutz von personenbezogenen Daten innerhalb der Europäischen Union (EU) zu erhöhen sowie den freien Datenverkehr innerhalb des Europäischen Binnenmarktes zu gewährleisten. Nach fast vierjährigen Verhandlungen und Debatten sowie mehr als 3.000 Änderungsanträgen im Parlament, haben sich Europäischer Rat, Europäisches Parlament und Europäische Kommission nun über den Inhalt der neuen Europäischen Datenschutzgrundverordnung (EU-DSGVO) geeinigt.

Auch die Vorsitzende der Hanns-Seidel-Stiftung, Professor Ursula Männle, hatte in ihrer Eigenschaft als Berichterstatterin im Ausschuss der Regionen für die Datenschutzgrundverordnung einigen dieser Debatten beigewohnt und hierzu gemeinsam mit dem Ausschuss für Recht und Verfassung eine Anhörung im Bayerischen Landtag durchgeführt. Sie wies in Ihrem Grußwort auf die mit der wachsenden Internationalisierung von Arbeits- und Geschäftsprozessen und dem damit einhergehenden steigenden internationalen Datenverkehr auf Teil sehr komplexen Fragenstellungen hin, welche zu einem immensen datenschutzrechtlichen Informationsbedarf führen. Um diesem auch seitens der Hanns-Seidel-Stiftung nachzukommen, eröffnete sie am 31. März 2016 die Fachtagung zu der Thematik **„Die Europäische Datenschutzreform und ihre Auswirkungen auf Recht und Wirtschaft“**, welche in Kooperation mit der Stiftung Datenschutz durchgeführt wurde.

Frederick Richter, Vorsitzender der Stiftung Datenschutz, betonte zu Beginn der Tagung, Datenschutz müsse wirksam und pragmatisch sein. Das heißt, er solle die Lebenswirklichkeit widerspiegeln und sich den tatsächlichen wirtschaftlichen und technischen Verhältnissen anpassen. Gleichzeitig ist Effektivität, Effizienz und Durchsetzbarkeit unabdingbar. Die Diskussion, welchen Mehrwert die EU-DSGVO in diesem Zusammenhang bringt überließ er den geladenen Experten.

Die Europäische Datenschutz-Grundverordnung (EU-DSGVO)
Die Entwürfe wurden im so genannten ordentlichen Gesetzgebungsverfahren auf Grundlage der Lissabonner Verträge in den EU-Gremien behandelt. Das bedeutet, dass das Europäische Parlament und die im Rat der Europäischen Union vertretenen Regierungen der 28 Mitgliedstaaten zunächst getrennt darüber beraten und sich auf Änderungsvorschläge verständigen. Diese werden im Anschluss in einem so genannten informellen Trilog-Verfahren zwischen Kommission, Rat und Parlament so aufeinander abgestimmt, dass Rat und Parlament sich am Ende auf einen Gesetzestext einigen und diesen verabschieden.
Der Europäische Rat hat die verschiedenen Sprachfassungen der Datenschutz-Grundverordnung nun veröffentlicht. Nach derzeitiger Planung soll die Zustimmung zum Reformpaket im Plenum des Europäischen Parlaments am 27. April 2016 erfolgen. Nach der Zeichnung am 11. Mai 2016 würden die Texte im Amtsblatt veröffentlicht und demnach bereits Anfang Juni 2016 in Kraft treten. Anwendbar wird die DSGVO nach der 2-jährigen Übergangsfrist somit voraussichtlich Anfang Juni 2018.

Inhalt

Als erster Redner gab **Stephan Mayer, MdB, Innenpolitischer Sprecher der CDU/CSU-Fraktion im Deutschen Bundestag**, sein Statement ab. Gleich zu Beginn betonte er bezugnehmend auf die Anschläge von Brüssel, dass die Zeiten, in denen „Datenschutz als Täterschutz“ bezeichnet werden konnte, längst der Vergangenheit angehören. Dennoch müsse überprüft werden, ob gewisse Vorschriften des Datenschutzes beim Austausch personenbezogener Daten von Gefährdern ein Hindernis in der europaweiten Zusammenarbeit der Nachrichtendienste und Sicherheitsbehörden darstellen. Auch in diesem Zusammenhang sei eine Harmonisierung von Vorschriften datenschutzrechtlicher Regelungen innerhalb Europas klar von Vorteil.

Die **EU-DSGVO** sei ein großer Fortschritt gegenüber alten Regelungen. Die deutsche Wirtschaft werde von einem einheitlichen Datenschutz in Europa profitieren, da sich Drittstaaten für den Zugang zum Europäischen Markt nicht mehr das Land aussuchen können, welches die niedrigsten Datenschutzvoraussetzungen aufweist. Auch habe der deutsche Datenschutz, als eine der qualitativ hochwertigsten und fortschrittlichsten Datenschutzregelungen in der EU nur vernachlässigenswert durch die Reform eingebüßt.

Folgende Errungenschaften hob Mayer besonders hervor:

- Das **Marktortprinzip**. Es soll Datenschutzoasen verhindern, weil es die Unterschiedlichkeit in den Regeln für verschiedene Marktteilnehmer beseitigt. Der Marktort ist dabei der Ort, an dem eine Leistung zielgerichtet angeboten wird. Dabei finden die Regeln des Ziellandes Anwendung. Somit muss jedes Unternehmen, das in Europa tätig ist, die europäischen Datenschutzregelungen einhalten. Dies gilt auch, wenn es keinen Sitz innerhalb der EU hat.

- Die **Pseudonymisierung** der Daten als milderes Mittel, um Chancen und Möglichkeiten der Digitalisierung zu nutzen und zugleich einen angemessenen Schutz der Persönlichkeitsrechte zu gewährleisten. Diese Technik erlaubt die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren. Dabei werden Name oder ein anderes Identifikationsmerkmal der betroffenen Person durch ein Pseudonym, etwa eine mehrstellige Buchstaben- oder Zahlenkombination, ersetzt.

- Die Bestellung eines **Datenschutzbeauftragten** ist zwar nur noch in wenigen Fällen Pflicht, durch die Öffnungsklausel bleibt das Institut des betrieblichen Datenschutzbeauftragten jedoch gewährleistet und kann durch deutsches Recht ausgefüllt werden.

- Die Stärkung des Rechts des Nutzers auf **Vergessenwerden und Löschung** nach Art. 17 EU-DSGVO als ein maßgeblich deutscher Verdienst. Künftig wird es für den Einzelnen leichter werden, einmal über ihn veröffentlichte Informationen löschen zu lassen.

Bezüglich des weiteren Vorgehens stellte Mayer klar, dass der Bundesgesetzgeber an bis zu 300 Bundesgesetzen zumindest kleinteilige Änderungen vornehmen muss. Dieses Gesetzgebungsverfahren solle, insbesondere in Hinblick auf das bevorstehende Ende der Legislaturperiode innerhalb der nächsten 12 Monate abgeschlossen werden.

Der **Passauer Rechtswissenschaftler, Professor Kai von Lewinski** fragte sich in seinem Statement, ob der Praxis durch die Rechtsumwälzungen lange Unklarheiten drohen. Aus wissenschaftlicher Perspektive betrachtete er zunächst die größten Veränderungen, welche die DSGVO im Gegensatz zu unserem bestehenden Datenschutzrecht aufweist.

Charta der Grundrechte der Europäischen Union
Artikel 8
Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

- Essentiell dabei ist die Ersetzung des Rechts auf Informationelle Selbstbestimmung durch das **Recht auf Datenschutz, Art. 8 der Grundrechte-Charta der Europäischen Union**.

- Auch der **Rechtsweg** wird sich verändern. Während heute noch die Möglichkeit des Wegs zu deutschen Gerichten besteht, werden künftige Klagen mit wenigen Ausnahmen vor dem Europäischen Gerichtshof erhoben werden müssen.

- Voraussichtlich wird das Datenschutzrecht zukünftig aus einer **Regelungskaskade auf EU-Ebene** bestehen, die teilweise durch verschiedene Öffnungsklauseln durch den deutsch oder bayerischen Gesetzgeber **konkretisiert** werden kann.

Zudem sprach von Lewinski **Unsicherheiten** an, die durch die neuen Herausforderungen vorerst entstehen. So ist die Ausgestaltung der Umstrukturierung der Datenschutzaufsicht derzeit noch gänzlich unklar. Details hierzu werden sicherlich sehr kontrovers diskutiert werden. Bisher sei keine klare Verantwortlichkeits- oder Rechtschutzstruktur ersichtlich. Die Aufsicht erscheine zudem sehr politisiert. Inwieweit derzeit bestehende nationale Datenschutzregelungen bestehen bleiben, sei derzeit noch offen. Nicht abwegig jedoch erscheine die Umarbeitung zu Ausführungsgesetzen. Zudem sieht die Verordnung an einer ganzen Reihe zentraler Regelungspunkte die Möglichkeit vor, durch nationales Recht Sonderregelungen zu schaffen.

Insgesamt hält von Lewinski die Datenschutzreform für unser heutiges Zeitalter nicht angemessen und ausreichend. Er sieht das Datenschutzrecht zukünftig in das Kartell- und Wettbewerbsrecht als Teil eines allgemeinen Informationsrechts hinein wandern.

Werner Herrmann, Konzerndatenschutzbeauftragter der UniCredit Bank, beleuchtete die Vor- und Nachteile der europäischen Regelungen für mittelständische Unternehmen.

Dabei sah er an einigen Stellen **Erleichterungen**, wie die Entbindung der Führung eines Verzeichnisses von Verarbeitungstätigkeiten für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen. Auch die Möglichkeit der Zertifizierung von IT-Sicherheit und Datenschutzorganisation erleichtern die täglich Arbeit, wenn sie auch um die Zertifizierung zu bekommen, erst einmal mit Kosten verbunden sind.

Einen klaren Vorteil stelle auch das in Art. 43 DSGVO statuierte **Konzernprivileg** dar, welches die Datenweitergabe innerhalb einer sog. Unternehmensgruppe unter erleichterten Voraussetzungen ermöglicht. Und gegebenfalls könnten sich auch Vorteile aus dem **Joint-Controller Prinzip** ergeben. Sofern zwei verantwortliche Stellen dieselben Daten verarbeiten, müssen die Unternehmen eine „kleine Vereinbarung zur Auftragsverarbeitung“ schließen. Diese muss nach Art. 24 DSGVO definierte „transparente“ Regelungen enthalten.

Insgesamt betrachtete Herrmann jedoch die **hohen Kosten**, die Unternehmen für die Anpassung an die EU-DSGVO aufwenden müssen, sowie den drastisch erhöhten Bußgeldrahmen als insgesamt eher nachteilig für kleine und mittlere Unternehmensstrukturen. Er betonte mehrfach, nichts zu tun und die Neuanforderungen zu ignorieren wäre falsch und gerade hinsichtlich der zu erwartenden Strafen sehr gefährlich. Zusätzlich gab er zu bedenken, dass die erweiterten Rechte von Kunden, Interessenten und Mitarbeitern zumindest aus Sicht der Unternehmen wenig vorteilhaft sind. Dazu kommen umfassende Informations-, Rechenschafts- und Dokumentationspflichten sowie die Etablierung eines Datenschutzmanagementsystems. Aus Verbrauchersicht weisen diese Aspekte hingegen deutliche Verbesserungen auf.

©HSS

In der anschließend intensiven Diskussion im Plenum, an der auch **Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht,** teilnahm, wurde zunächst das Folgeabkommen „**Privacy Shield**“ zu dem im Herbst des letzten Jahres durch Urteil des EuGH gekippten „Safe Harbor“ -Abkommens, diskutiert.

Im Februar hat die EU Kommission das neue Abkommen zum transatlantischen Datenaustausch zwischen der EU und den USA vorgestellt. In Kraft treten wird die Nachfolgeangemessenheitsvereinbarung aber voraussichtlich erst in mehreren Monaten. Ein rechtsloser Zustand besteht nach einhelliger Meinung der Experten dennoch nicht. Es gibt andere Instrumente wie **Standardverträge und Einwilligungen**, die eine Datenübertragung in die USA ermöglichen. Derzeit gehen die Aufsichtsbehörden in diesem Zusammenhang auch nicht proaktiv auf die Unternehmen zu, erklärte Kranig. Beschwerden werde aber selbstverständlich nachgegangen.

Von Safe Harbor zu Privacy Shield

Mit Urteil vom 6. Oktober 2015 hat der Gerichtshof der Europäischen Union (EuGH) das Safe-Harbor-Abkommen für ungültig erklärt. Safe Harbor wurde gemeinsam von der Europäischen Kommission und dem US-Handelsministerium als Regelwerk entwickelt. Das Abkommen sollte es Unternehmen mit Sitz in der EU rechtssicher ermöglichen, personenbezogene Daten an US-Unternehmen zu übermitteln. Aufgrund einer rechtlichen Auseinandersetzung zwischen dem Österreicher Max Schrems und dem irischen Data Protection Commissioner musste der EuGH im Rahmen eines Vorlageverfahrens entscheiden, ob eine nationale Datenschutzaufsichtsbehörde an die Entscheidung der Europäischen Kommission gebunden ist, dass Safe Harbor für ein angemessenes Schutzniveau für Daten aus der EU sorgt. In seiner Entscheidung geht der EuGH über diese konkrete Frage noch hinaus und vertritt die Auffassung, dass die Safe-Harbor-Entscheidung tatsächlich kein angemessenes Datenschutzniveau sicherstellt.

Da die Übermittlung personenbezogener Daten aus der EU in die USA unzulässig werden, soweit sie nicht von den Datenschutzaufsichtsbehörden genehmigt werden oder unter die gesetzlichen Ausnahmetatbestände fallen (vgl. etwa § 4c Abs. 2 BDSG), haben die Parteien nach intensiven Verhandlungen am 2. Februar 2016 das Nachfolgeabkommen „Privacy Shield“ vorgestellt. Damit ist das neue Abkommen jedoch noch nicht in Kraft. Zunächst wird ein Ausschuss aus Vertretern der Mitgliedstaaten und EU-Datenschutzbehörden über den Entwurf der Kommissionsentscheidung beraten. Dieser Ausschuss wird dann zu dem geplanten Datenschutzschild Stellung nehmen. Erst dann wird das Kollegium der Kommissarinnen und Kommissare abschließend über den Privacy Shield entscheiden. In der Zwischenzeit treffen die USA die notwendigen Vorkehrungen zur Einrichtung des neuen Rahmens, der neuen Überwachungsmechanismen sowie der neuen geplanten Ombudsstelle.

Nach Ansicht Mayers hinken die USA europäischen Datenschutzstandards hinterher, es gebe zu viele Eingriffe in die informationelle Selbstbestimmung. Deshalb müsse ein Folgeabkommen gut geprüft werden. Er bezeichnete das „Safe Harbor“-Urteil als bahnbrechend. Dennoch sei nicht zu verkennen, das europäische Unternehmen grundsätzlich starkes Interesse an einem Abkommen über den Datenaustausch haben, weshalb das Folgeabkommen „Privacy Shield“ nötig ist. Er verwies darauf, dass die Art. 29-Gruppe sich insbesondere bezüglich der Angemessenheitsprüfung positionieren wird.

Von Lewinski erklärte, dass das Privatheitsverständnis in unterschiedlichen Kulturen oft stark divergiere. Dies stelle zwar nicht zwingend eine Unterschiedlichkeit im Niveau dar, die verschiedenen Ansätze müssen aber vereinbart werden. Das **Problem ist ubiquitär, die Betroffenheit lokal**. Als am besten geeigneten Ansatz nannte er deshalb die Harmonisierung auf Ebene der einzelnen Rechtsfragen, um eine Zwischeneben zwischen den beiden Rechtsordnungen zu schaffen. Auch auf die Frage aus dem Fachpublikum, warum man das „Privacy Shield“-Abkommen überhaupt brauche, betonte er, dass es im Datengeschäft und im Internet kein „hier und da“ gebe. Dies sei ein Problem des sogenannten **Informationskollisionsrechts**, also Regeln, die bei zwei kollidierenden Informationsrechtsordnungen die anwendbare bestimmen. Ein ubiquitärer Sachverhalt muss auf eine territoriale Rechtslandschaft umgesetzt werden. Um mit Unternehmen in Ländern, die über ein der EU nicht angemessenes Datenschutzrechtsniveau verfügen, geschäftlich in Kontakt zu treten, werden separate Abkommen benötigt, um Rechtssicherheit für die Unternehmen zu schaffen. Dies ist in beiderseitigem Interesse.

Die Artikel-29-Datenschutzgruppe

wurde im Rahmen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eingerichtet. Sie ist eine beratende, gleichwohl unabhängige Instanz und setzt sich aus einem Vertreter der Kontrollstelle, die von jedem EU-Mitgliedstaat eingerichtet wird, einem Vertreter der Behörde, die für die EU-Institutionen und-Organe geschaffen wird und einem Vertreter der Europäischen Kommission zusammen. Die Aufgaben der Datenschutzgruppe sind in Artikel 30 der Europäischen Datenschutzrichtlinie und Artikel 15 der Richtlinie 2002/58/EG festgelegt. Danach hat die Gruppe vornehmlich beratende Funktion. Sie kann aber auch von sich aus Empfehlungen und Stellungnahmen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Gemeinschaft betreffen.

Nach Beratung zu den Anforderungen an das „Privacy Shield"-Abkommen, wurden folgende Forderungen an die künftige Einigung zwischen EU und USA gestellt:

- **Klarheit – Transparenz – vollständige Information**. Klare, verständliche Regelungen für das künftige Abkommen. Die Betroffenen sollen von Anfang an absehen können, was mit ihren personenbezogenen Daten geschieht, die Gegenstand des Datentransfers und der Verarbeitung in den USA sind.
- **Erforderlichkeit – Angemessenheit**. Die Verarbeitung der Daten muss den in Europa etablierten Prinzipien der Angemessenheit und Erforderlichkeit genügen.
- **Interessenabwägung**. Die Regelungen sollen einen gerechten Ausgleich zwischen den berechtigten Interesses des Datenexporteurs (am Transfer und der Verarbeitung der personenbezogenen Daten in den USA) und den schützenswerten Interessen der Betroffenen (dass der Datenverarbeitung klare Grenzen gesetzt werden) schaffen
- **Unabhängige Datenschutzaufsicht**. Zur Durchsetzung der Datenschutzrechte und Garantien sollen Regelungen für eine effektive und objektive Datenschutzaufsicht geschaffen werden.
- **Wirksame Rechtsmittel**. Schließlich müssten den Betroffenen wirksame Rechtsmittel zur Durchsetzung ihrer Rechte und Ansprüche vor derartigen unabhängigen Gremien offen stehen.

Auf die Anschläge in San Bernardino eingehend kam die im Datenschutz immer wieder kontrovers diskutierte Frage auf: **„Sicherheit gegen Freiheit?".** Mayer betonte, die beiden Komponenten würden sich eindeutig bedingen und seien kein Widerspruch. Im Einzelfall müsse ohnehin immer abgewogen werden.

Kranig prononcierte, dass es wichtig sei zu prüfen, ob die bestehenden Normen die wir haben, nicht ausreichen um genügend Schutz zu leisten. Dann stelle sich die Frage „Daten gegen Sicherheit" erst gar nicht.

Auf Nachfrage aus dem Plenum, wie es mit Vorhaben bezüglich **Schlüsselhinterlegungen** in Deutschland aussehe, betonte Mayer, dass er strikt gegen die Zusammenarbeit zwischen deutschen Nachrichtendienst und IT unternehmen votiert. Es darf auch keine Backdoors, wie die Schlüsselhinterlegung oder ähnliches geben.

Zum Schluss führte der Moderator, **Prof. Dr. Peter Bräutigam, Rechtsanwalt und Partner, Noerr LLP**, das Plenum noch einmal zurück auf die EU-DSGVO. Darauf gerichtet lobte Kranig die Vereinheitlichung der Vorschriften und die Bemühungen der einzelnen Datenschutzaufsichtsbehörden, sich untereinander abzustimmen. Dieser Prozess habe bereits begonnen. Mit Sorge schaute er jedoch auf den durch die DSGVO vorgegebenen Aufgabenkatalog und die Rechtsprechung des EuGH zu den Aufgaben der Aufsichtsbehörden in Relation zu den tatsächlichen Kapazitäten. Auch werde derzeit bereits an einer europäischen Vereinheitlichung gearbeitet, in welchen Fällen welche Bußgelder und in welcher Höhe verhängt werden. Um Rechtssicherheit zu gewährleisten, müssten außerdem zukünftig einheitliche Zertifizierungskriterien entwickelt werden. Insgesamt sieht er den Grundrechtsschutz in Europa eindeutig gestärkt, da jeder berechtigt ist mithilfe der für ihn zuständigen Aufsichtsbehörde sein Recht auf Datenschutz durchzusetzen. Dies bedeute eine deutliche Verbesserung gegenüber der derzeitigen Rechtszersplitterung.

In Ihrem Fazit waren sich die Experten über die enorm hohe Wichtigkeit des Datenschutzes und des begonnen Reformprozesses einig, jedoch nicht ohne einige Kritikpunkte anzubringen. Mayer betonte zum Abschluss: in Unternehmen solle Datenschutz Chefsache sein!