Erläuterungen

zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven „Europa muss den Datenschutz stärken“

- **Jedes personenbeziehbare Datum muss geschützt werden**

  Nach Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie z. B. IP-Adressen, Kenn-Nummern, Standortdaten ein.

- **Es darf keine grundrechtsfreien Räume geben**

  Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

- **Einwilligungen müssen ausdrücklich erteilt werden**
  Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäische Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es – auch mit Blick auf Artikel 8 Abs. 2 der Grundrechtecharta – nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

- **Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern**

  Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch – in Anlehnung an Artikel 8 Abs. 2 der Grundrechtecharta - das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

- **Profilbildung muss beschränkt werden**

  Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

- **Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte**

  Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

- **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**

  Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die

Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

- **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**
  Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Art. 8 Abs. 3 der Grundrechtecharta und Art. 16 Abs. 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

- **Grundrechtsschutz braucht effektive Kontrollen**
  Die Sanktionen müssen – wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat – abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

- **Hoher Datenschutzstandard für ganz Europa**

  Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-

Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.