
Deutscher Industrie- und Handelskammertag

Zum Thema: **Stellungnahme zur Strategie zur Überarbeitung der Datenschutz-Richtlinie 95/46/EG**

Registrierungsnummer des DIHK: 22400601191-42

Der Deutsche Industrie- und Handelskammertag e. V. (DIHK) nimmt als Dachorganisation die Interessen von 3,6 Mio. gewerblichen Unternehmen in Deutschland wahr. Alle Unternehmen unterliegen den Datenschutzgesetzen.

I. Vorbemerkung

Der Schutz der Privatsphäre ist insbesondere im Zeitalter der Informationsgesellschaft und der Globalisierung unerlässlich. Instrumente wie E-Government und E-Business werden nur erfolgreich sein und sich durchsetzen können, wenn Integrität, Vertraulichkeit und Verbindlichkeit der Daten des Einzelnen gewährleistet werden können.

Die Schaffung einheitlicher Regelungen zum Schutz personenbezogener Daten innerhalb der EU ist eine wichtige Basis, die gleiche Rechte und Chancen für alle gewährleistet. Der Weg der EU, als treibende Kraft weltweit internationale Standards im Bereich des Schutzes personenbezogener Daten und beim Abschluss geeigneter internationaler Instrumente auf bi- und multinationaler Ebene zu entwickeln und zu fördern, ist richtig, weil Europa sich nicht abschotten kann und Datenschutz ein hohes Maß an internationaler Zusammenarbeit erfordert. Datenschutz darf nicht zu einer unüberwindlichen Hürde für europäische Unternehmen werden, die sie daran hindert, neue Geschäftsmodelle im Bereich z. B. des Internets zu kreieren.

Datenschutz darf ebenfalls nicht dazu führen, dass Datenschutzgesetze über Vorgaben auf EU-Ebene noch schwerer verständlich werden und der Datenschutz sich als Wirtschaftsbremse erweist, gerade weil KMU allein nicht mehr in der Lage sind, die Datenschutzgesetze wegen ihrer Komplexität richtig umzusetzen und/oder zu verstehen bzw. sie sich die Kosten für den geforderten technischen Aufwand und die datenschutzrechtliche Beratung nicht mehr leisten können.

Datenschutz ist ein Qualitäts- und Wettbewerbsfaktor. Datenschutz hat in Zeiten zunehmender Technisierung und Vernetzung einen hohen Stellenwert. Die Entwicklung neuer datenschutzsparsamer Technologien ist angesichts der fortschreitenden technologischen Entwicklung unverzichtbar.

Oberstes Ziel eines modernen Datenschutzes muss ein sachgerechter Interessenausgleich zwischen allen Betroffenen - den wirtschaftlichen Interessen der Unternehmen und dem Recht der mündigen Verbraucher auf informationelle Selbstbestimmung - sein.

II. zu den einzelnen Punkten

Zu 1. Anpassung an neue Technologien

Ein funktionierender Datenschutz schafft Vertrauen gegenüber der Wirtschaft und öffentlichen Institutionen und ist im Zeitalter moderner Technologie vor stets neue Herausforderungen gestellt. Datenschutz ist damit keine Aufgabe, die einmalig zu lösen ist, sondern er muss der Realität des technischen Fortschritts und der digitalen Welt Rechnung tragen. Daraus folgert aber auch, dass die Regelungen zum Datenschutz grundsätzlich abstrahiert sein müssen von der zum Zeitpunkt der Regelung verwendeten Technik, weil ansonsten ein ständiger Änderungsbedarf besteht.

Zu 2.1.2. Erhöhung der Transparenz der Datenverarbeitung

Die Globalisierung der Datenverarbeitung macht Datenschutz zu einer internationalen Aufgabe. Nationalstaatliche Regelungen ebenso wie Regelungen auf EU-Ebene sind nur begrenzt erfolgversprechend. Daher muss das Prinzip des Selbst Datenschutzes eines der Leitbilder für gesetzgeberische Maßnahmen sein. Der Schutz der eigenen Daten liegt ganz wesentlich in der Hand jedes Einzelnen. Diese Pflicht kann der Betroffene aber nur ausüben, wenn er ausreichend darüber informiert wird, wer wann wie welche Daten verarbeitet. Hier besteht eine Bringschuld der Daten verarbeitenden Unternehmen im Rahmen ihrer Informationspflichten. Viele Unternehmen kommen dieser Pflicht nach, würden jedoch ihre Kunden gern mit verständlicheren Formulierungen informieren, woran sie jedoch durch vielfältige Vorschriften zum Informationsinhalt gehindert sind.

Die Transparenz der Datenverarbeitung sollte als allgemeiner Datenschutzgrundsatz formuliert werden. Der besondere Schutz von Kindern, insbesondere im Internet, ist zu befürworten.

Zu 2.1.2. Informationspflichten bei Verstößen

Deutschland hat im Bundesdatenschutzgesetz (§ 42 a) eine entsprechende Regelung eingeführt. Unter den dort genannten Voraussetzungen – besonders sensible bzw. schutzwürdige Daten, Drohen eines schwerwiegenden Schadens, Vielzahl der betroffenen Fälle – können solche Informationspflichten ein geeignetes Mittel sein.

Zu 2.1.3. Stärkung des Rechts auf Datenzugang, Berichtigung, Sperrung und Löschung sowie „Recht auf Vergessen“

Personenbezogene Daten, die der Betroffene freiwillig zur Verfügung gestellt hat bzw. bei denen der Speicherungszweck entfallen ist, muss der Betroffene auch jederzeit wieder löschen können, sofern dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen oder aus anderen wichtigen Gründen eine Sperrung der Daten vorzuziehen ist. Allerdings erfordert die Umsetzung erhebliche technische Aufwendungen, die gerade für kleinere und mittlere Unternehmen schwierig zu bewerkstelligen sind. Zudem muss berücksichtigt werden, dass die weitaus überwiegende Menge der Daten, die z. B. über E-Commerce-Anwendungen über Verbraucher gespeichert sind, für die Abwicklung der Verträge erforderlich ist und aus steuerlichen Gründen einer längeren Aufbewahrungsfrist unterliegen. Daher entziehen sie sich dem Wunsch des Betroffenen auf Löschung.

Insbesondere bei der Normierung sozialer Netzwerke darf nicht verkannt werden, dass die Nutzer ihre persönlichen Daten freiwillig weltweit veröffentlichen. Hier sollte in erster Linie die Datenschutzkompetenz der Nutzer gestärkt werden und nicht die Unternehmen mit zusätzlichen Informations- und Auskunftspflichten oder Pflichten zu technisch aufwändigen Löschungen belastet werden.

Zu 2.1.3. Stärkung des Grundsatzes der Datensparsamkeit/-vermeidung

Ansätze zur Durchsetzung dieses Grundsatzes sind sehr sinnvoll. Allerdings kollidieren sie damit, dass in einer Informations- und Kommunikationsgesellschaft Daten immer stärker zu einer „normalen“ Ware werden.

Eine Verpflichtung zum Einsatz technischen Datenschutzes würde voraussetzen, dass das jeweilige IT-Produkt auch entsprechend programmiert/ programmierbar ist. Dies ist bei internationalen Produkten allerdings häufig nicht der Fall.

Zu 2.1.4. Stärkung der Datenschutzkompetenz, insbesondere bei jüngeren Menschen

Dieser Ansatz ist wichtig. Die Betroffenen müssen sich der Bedeutung ihrer Handlungen stärker bewusst sein. Wer seine eigenen Daten freiwillig weltweit über das Internet veröffentlicht, muss über die Folgen aufgeklärt werden, damit er die Tragweite erkennen kann. Die Stärkung der Eigenverantwortung der Betroffenen ist daher besonders wichtig.

Zu 2.1.5. Stärkung der Einwilligung

Die Einwilligung muss als Rechtsgrundlage für Datenverarbeitung erhalten bleiben. Sie ist Ausfluss des Rechts auf Datenschutz, dem eine individuelle Entscheidung darüber zugrunde liegt, personenbezogene Daten - und in welchem Umfang - zu offenbaren. Sie ist ebenso Ausfluss der Vertragsfreiheit. Für Arbeitsverhältnisse und andere rechtsgeschäftliche Schuldverhältnisse muss es bei dem bisherigen Regel-Ausnahme-Verhältnis bleiben: Die Einwilligung muss durchgängig als weiterer Erlaubnistatbestand für Datenverarbeitung gelten. Insbesondere in kleineren und mittleren Unternehmen ist die Einwilligung ein unverzichtbares Instrument zur vertrauensvollen Zusammenarbeit im Betrieb.

Aufgrund des technischen Fortschritts sollte jedoch die Schriftlichkeit durch elektronisch unterstützte Alternativen ersetzbar sein.

Zu 2.1.6. Definition der sensiblen Daten

Grundsätzlich ist die Erweiterung auf genetische Daten nachvollziehbar. Die Verarbeitung sensibler Daten wird in den nächsten Jahren allerdings erheblich zunehmen, z. B. durch e-health. Daher müssen die Regelungen die Verarbeitung dieser Daten - auch die Möglichkeiten zur Auftragsdatenverarbeitung - berücksichtigen.

Zu 2.1.7. Klagerechte und Sanktionen

Vor einer Änderung sollte der Vollzug der vorhandenen Buß- und Ordnungsgeldvorschriften verbessert werden. Bei einer Änderung sollten die Befugnisse zur Untersagung der Erhebung, Verarbeitung und Nutzung von Daten sowie der Einsatz einzelner Verfahren auf Fälle beschränkt bleiben, bei denen schwerwiegende Mängel festgestellt wurden.

Ein Klagerecht von Verbänden ist nicht erforderlich, da es Aufsichtsbehörden gibt. Beim Datenschutz handelt es sich um den Ausfluss eines Grundrechts, nicht um Verbraucherschutz, auch wenn Betroffene und Verbraucher häufig identisch sind. Keinesfalls darf es im Bereich des Datenschutzes über eine EU-weite Regelung dazu kommen, dass wie im Falle des Wettbewerbsrechts auch das Abmahn- und Klageunwesen droht und man sich zudem mit der Frage der Seriosität klagender Verbänden beschäftigen muss. Für Privatinitiativen wie Verbände besteht weder Notwendigkeit noch Bedarf.

Zu 2.2.4. Stärkung der Verantwortlichkeit der verantwortlichen Stelle

Die Überlegung zur verpflichtenden Bestellung eines betrieblichen Datenschutzbeauftragten ist sinnvoll, wie die Erfahrungen in Deutschland zeigen. Dies gilt auch für eine Grenze für kleinere und mittlere Unternehmen.

Die erforderliche Qualifikation des Datenschutzbeauftragten sollte klar definiert werden, um ein einheitliches Datenschutzniveau zu erreichen und Wettbewerbsverzerrungen zu vermeiden.

Ebenfalls begrüßen wir die Überlegung zu einem Datenschutzkonzept („privacy by design“), das für KMU zu Erleichterungen bei den Meldepflichten führen würde. Denn daraus würde ein Gewinn für den tatsächlichen Datenschutz in den Unternehmen entstehen.

Zu 2.2.5. Einführung eines Gütesiegels

Die Meinung darüber ist in der Wirtschaft geteilt: Während einige IT-Unternehmen durchaus einen gewissen Marketingeffekt sehen, befürchten andere zusätzliche Kosten und mehr Bürokratie, ohne dass dadurch der Datenschutz gesteigert würde. Die Erfahrungen mit der ISO-Zertifizierung haben gezeigt, dass aus Freiwilligkeit schnell ein faktischer Zwang entstehen kann, weil Unternehmen von ihren Zulieferern eine entsprechende Zertifizierung verlangen. Dies betrifft vor allem KMU. Zudem sind die Fragen des Verhältnisses zur Aufsichtsbehörde und zum betrieblichen Datenschutzbeauftragten nach wie vor ungeklärt. Daher ist bisher in Deutschland keine Regelung zustande gekommen.

Keinesfalls darf die Einführung von Datenschutzgütesiegeln zum Aufbau übermäßiger Bürokratie und zu Kostenbelastungen führen. Gerade für KMUs könnte sich sonst die Einführung von Datenschutzgütesiegeln schnell als nachteilig erweisen. Da Unternehmen sich stets datenschutzkonform verhalten müssen, stellt sich immer auch die Frage nach dem Mehrwert für

Unternehmen, aber auch für Kunden/Verbraucher. Die Einführung eines Gütesiegels erscheint nur dann sinnvoll, wenn das Unternehmen dafür „belohnt“ würde.

Zu 2.4.1. Verbesserung des Datentransfers in Drittländer

Der Datentransfer ins Ausland, auch in Drittländer, wird in Zukunft auf Grund der Globalisierung noch zunehmen. Dies gilt insbesondere für den konzerninternen Datentransfer. Die von der EU ins Auge gefassten Erleichterungen zum Datentransfer in Drittländer ebenso wie zum Datenfluss innerhalb von Konzernen werden von der Wirtschaft dringend benötigt. Es sollte daher eine Regelung eingeführt werden, die den konzerninternen Datentransfer privilegiert und den Datentransfer in Drittstaaten für die Unternehmen allgemein erleichtert. Dadurch soll keine Absenkung des Datenschutzniveaus erreicht werden, sondern es sollen vielmehr die bestehenden Verfahren zur Datenübermittlung in Drittländer vereinfacht und vereinheitlicht werden. Die derzeitigen Regelungsinstrumente z. B. beim Datentransfer in Drittländer sind sehr aufwändig, geben den Unternehmen aber keine Sicherheit bezogen auf Gesetzeskonformität.

Das Feststellungsverfahren der EU-Kommission zum angemessenen Datenschutzniveau bietet den weltweit tätigen Unternehmen keine ausreichende Unterstützung, weil es bisher Staaten betrifft, zu denen eher geringe Handelsbeziehungen bestehen. Das Genehmigungsverfahren für verbindliche Unternehmensregelungen (Binding Corporate Rules) ist ebenfalls zu bürokratisch ausgestaltet. Zudem mangelt es an einer einheitlichen Beurteilung durch Aufsichtsbehörden in den EU-Mitgliedstaaten. Es müssen daher sowohl Erleichterungen für Konzernregelungen als auch für eine verbindliche Kontrolle solcher Vorschriften geschaffen werden, die Unternehmen die Datenverarbeitung innerhalb ihrer Strukturen erleichtern. Die Regelungen sollten sowohl die Daten der Beschäftigten als auch die der Vertrags- und Geschäftspartner umfassen.

Zu 2.5. Vereinheitlichung des Rechtsrahmens

Wir teilen die Analyse der EU-Kommission, dass die EG-Datenschutzrichtlinie in den einzelnen EU-Mitgliedstaaten sehr unterschiedlich umgesetzt wurde. Hieraus ergeben sich für Unternehmen, die grenzüberschreitend tätig sind, erhebliche Probleme. Eine stärkere Harmonisierung der Datenschutzregeln ist notwendig. Allerdings ergibt sich aus einer unterschiedlichen Umsetzung der EG-Richtlinie nicht die notwendige Konsequenz einer Änderung der Rechtsgrundlage, sondern eher einer stärkeren Kontrolle durch die EU-Kommission.

Zweifelhaft erscheint, ob die Art. 29-Gruppe für eine Vereinheitlichung der Umsetzung der Richtlinie in den einzelnen EU-Mitgliedstaaten die richtige Institution ist, da sie bisher häufig die bestehende



Berlin, 11. Januar 2011

Richtlinie extensiv ausgelegt hat. Sollte jedoch die Art. 29-Gruppe die Funktion einer verbindlichen Aufsicht erhalten, sollten dort alle Aufsichtszuständigkeiten gebündelt werden.

Das Datenschutzrecht ist eine sehr komplexe Materie, bei deren Umsetzung und Einhaltung die Unternehmen nicht selten Schwierigkeiten haben. Eine Stärkung der Datenschutzaufsicht sollte daher auch eine Stärkung der Beratungs- und Aufklärungsfunktion der Aufsichtsbehörden mit sich bringen.

Ansprechpartnerin: Annette Karstedt-Meierriecks

E-Mail: karstedt-meierriecks.annette@dihk.de