GDD-Stellungnahme
zum neuen Datenschutzkonzept der EU-Kommission

I. Einführung

(...)

II. Nutzung von Entbürokratisierungspotenzialen

Die GDD begrüßt die Intention der EU-Kommission, unnötige administrative Hürden abzubauen. Dies gilt insbesondere im Hinblick auf das derzeitige Meldeverfahren. Gleichzeitig teilt die GDD die Auffassung der Kommission, wonach eine Verringerung des Verwaltungsaufwands nicht zu einem generellen Abbau der Datenschutzverantwortlichkeit der datenverarbeitenden Stellen führen darf. Insofern hat die GDD bereits im Rahmen ihrer vorangegangenen Stellungnahmen darauf hingewiesen, dass die Notwendigkeit zur Verbesserung interner Datenschutzkontrollmechanismen besteht. Aus Sicht der GDD kann eine sinnvolle Reduzierung administrativer Belastungen insbesondere durch eine Stärkung der Rolle des betrieblichen Datenschutzbeauftragten kompensiert werden. Angesichts der Tatsache, dass die verantwortlichen Stellen in allen Mitgliedsstaaten dazu verpflichtet sind, datenschutzrechtliche Vorschriften zu beachten und sich ohnehin eine kompetente Instanz innerhalb des Unternehmens bzw. der Behörde um diese Aufgabe kümmern muss, bedeutet die Bestellung qualifizierter Datenschutzbeauftragter nach Auffassung der GDD insofern auch keinen Mehraufwand („Somebody has to do the job!“).

III. Stärkung der Rolle des betrieblichen Datenschutzbeauftragten

1. Perspektive der Kommission

Gemäß der Mitteilung – COM(2010) 609 final – wird die Kommission u.a. folgende Maßnahmen prüfen, um die Verantwortung der für die Verarbeitung Verantwortlichen zu stärken:

- Verpflichtende Benennung eines unabhängigen Datenschutzbeauftragten, wobei zur Vermeidung eines übermäßigen Verwaltungsaufwands vor allem für kleine und kleinste Unternehmen angemessene Schwellen in Erwägung zu ziehen wären;

- Harmonisierung der Bestimmungen über die Aufgaben und Zuständigkeiten der Datenschutzbeauftragten.

2. Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter

a) Weltweit wachsende Akzeptanz betrieblicher Datenschutzbeauftragter

Wie die GDD bereits in vorangegangen Konsultationsbeiträgen dargestellt hat, hat Deutschland in den vergangenen 30 Jahren weitestgehend gute Erfahrungen mit der Institution des betrieblichen Datenschutzbeauftragten gemacht; inzwischen finden diese nicht nur bei einer zunehmenden Anzahl von Mitgliedstaaten, sondern auch bei Unternehmen in der ganzen Welt erhöhte Anerkennung.

Anlässlich der 31. Internationalen Datenschutzkonferenz im Jahr 2009 in Madrid haben Aufsichtsbehörden aus über 50 Ländern die sogenannte „Madrid-Resolution“ zu internationalen Datenschutzstandards angenommen. Ein wichtiger Abschnitt der Resolution betrifft proaktive Datenschutzmaßnahmen, wozu auch die Bestellung von qualifizierten und mit den notwendigen Mitteln und Befugnissen ausgestatteten betrieblichen Datenschutzbeauftragten gezählt wird.

b) Angemessene Schwellen

Die EU-weite Einführung einer Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter könnte nach Ansicht der GDD einen wichtigen Beitrag zur Verbesserung interner Kontrollmechanismen leisten. Gleichzeitig ist die GDD mit der EU-Kommission insofern einer Meinung, als vor allem kleine und kleinste Unternehmen nicht mit einem übermäßigen Verwaltungsaufwand überzogen werden dürfen und es insofern angemessener Schwellen bedarf. Die *Anzahl* der mit der Datenverarbeitung im Unternehmen regelmäßig beschäftigten Personen betrachtet die GDD insofern nur als einen von mehreren Ansatzpunkten. Immerhin hängt das Risiko für die Rechte und Freiheiten der Betroffenen von den Gegebenheiten des Einzelfalls ab. Im Hinblick auf eine mögliche Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter empfiehlt die GDD auch folgende Kriterien in Erwägung zu ziehen:

- **Menge personenbezogener Daten**

Unternehmen, die personenbezogene Daten in großer Anzahl verarbeiten, sehen sich naturgemäß größeren Datenschutzrisiken ausgesetzt, als Unternehmen, die mit einem Minimum an personenbezogenen Daten auskommen.

Bei Unternehmen, in denen die Verarbeitung personenbezogener Daten zum eigentlichen Kerngeschäft gehört (z.B. Internet- oder Telekommunikationsprovider), besteht im Regelfall ein erhöhtes Risikopotenzial.

Das Gleiche gilt für Unternehmen, die personenbezogene Daten im Auftrag verarbeiten. Insofern teilt die GDD die Auffassung der EU-Kommission, dass interne Kontrollmechanismen besonders wichtig sind, wenn verantwortliche Stellen – was immer häufiger der Fall ist – die Verarbeitung personenbezogener Daten an andere Stellen delegieren (z.B. an Auftragsdatenverarbeiter). Sofern in solchen Fällen der Auftraggeber datenschutzrechtlich verantwortlich bleibt, ist es für ihn wichtig, dass ihm auch beim Auftragnehmer ein qualifizierter Ansprechpartner zur Verfügung steht.

- **Zwecke der Datenverarbeitung**

Ein erhöhtes Risikopotenzial kann auch bei solchen Unternehmen bestehen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung an Dritte verarbeiten (z.B. Adresshändler oder Markt- und Meinungsforscher).

Grundsätzlich beinhaltet auch die Datenverwendung zur Profilbildung spezifische Datenschutzrisiken.

- **Sensitivität der Daten**

Nach dem Bundesdatenschutzgesetz (BDSG) obliegt die Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter allen Unternehmen, die eine Vorabkontrolle vornehmen müssen. Dies kann bspw. die Verarbeitung sensitiver Daten gem. Art. 8 (1) der EU-Datenschutzrichtlinie betreffen. Gesundheitsdaten werden z.B. nicht nur von Krankenhäusern sondern auch von Versicherungsgesellschaften verarbeitet. Auch im Finanzsektor besteht ein vitales Interesse an einer vertraulichen Behandlung der personenbezogenen Daten (z.B. im Hinblick auf Bankkonto- oder Kreditkarteninformationen).

c) Alternativlösung: Der Datenschutzbeauftragte als Option

Für den Fall das sich die EU-Kommission letztlich gegen eine Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter entscheidet, empfiehlt die GDD Folgendes:

Nicht zuletzt mit Blick auf die von der EU-Kommission angestrebte Harmonisierung sollte der betriebliche Datenschutzbeauftragte zumindest als Option in die einzelnen Datenschutzgesetze der Mitgliedstaaten aufgenommen werden. Diese Auffassung wird auch von der französischen Datenschutzorganisation „Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCDP)“ geteilt. Seit das französische Datenschutzrecht den betrieblichen Datenschutzbeauftragten optional vorsieht, ist die Anzahl bestellter Datenschutzbeauftragter sowie anderer berufsmäßig tätiger Datenschützer gewachsen, was sich positiv auf den betrieblichen/behördlichen Datenschutz und die Datenschutzkultur in Frankreich insgesamt ausgewirkt hat.

Den Unternehmen sollten echte Anreize zur Bestellung betrieblicher Datenschutzbeauftragter in Aussicht gestellt werden, da die Datenschutzbeauftragten auf einen effektiven Datenschutz hinwirken und somit die staatlichen Aufsichtsbehörden entlasten werden.

2. Harmonisierung und Spezifizierung der Rolle betrieblicher Datenschutzbeauftragter

Im Hinblick auf die Rolle des Datenschutzbeauftragten, seine Bestellung, seine Aufgaben, seine völlige Unabhängigkeit und seine Qualifikation ist die EU-Datenschutzrichtlinie nicht besonders aussagekräftig. Demgegenüber beinhaltet das deutsche Datenschutzrecht detailliertere Informationen über die Rolle von betrieblichen Datenschutzbeauftragten, was der EU-Kommission als Informationsquelle dienen mag (vgl. Christoph Klug, Improving self-regulation through – law-based – Corporate Data Protection Officials; abrufbar unter http://www.gdd.de/international/english).

Darüber hinaus gibt die GDD folgende Empfehlungen:

Bestellung: In einigen Mitgliedstaaten besteht die Pflicht, bestellte Datenschutzbeauftragte bei der zuständigen Datenschutzaufsichtsbehörde zu registrieren. Einige Datenschutzaufsichtsbehörden pflegen auf Basis dieser Meldungen ein öffentlich verfügbares Verzeichnis bestellter Datenschutzbeauftragter. Im Sinne der von der EU-Kommission angestrebten Harmonisierung und aus Gründen der Transparenz für Datenschutzaufsichtsbehörden und Betroffene wäre eine EU-weite Pflicht zu erwägen, wonach die Bestellung von Datenschutzbeauftragten bei der zuständigen Datenschutzaufsichtsbehörde angezeigt werden muss.

Aufgaben und Pflichten: Die GDD betont erneut (siehe vorherige Stellungnahmen) die Notwendigkeit einer Klarstellung dahingehend, dass die rechtzeitige Information der Datenschutzbeauftragten über sämtliche Verfahren automatisierter Verarbeitung personenbezogener Daten und – wo notwendig – die Durchführung einer Vorabkontrolle unabdingbare Rechtmäßigkeitsvoraussetzungen sind.

Die zuletzt erfolgte Revision der sogenannten E-Privacy-Directive (Richtlinie 2002/58/EG) hat eine Informationspflicht von Telekommunikations- und Internetprovidern im Fall von „Datenschutzpannen" mit sich gebracht. Diese EU-Regelung ist bereits im deutschen Datenschutzrecht umgesetzt worden. Dabei ist der deutsche Gesetzgeber sogar einen Schritt weitergegangen, indem er über § 42a BDSG eine allgemeine Informationspflicht eingeführt hat, die den gesamten nicht-öffentlichen Bereich betrifft. Angesichts der Tatsache, dass nunmehr auch die EU-Kommission die Einführung einer allgemeinen Anzeigepflicht im Fall von Datenschutzverstößen prüfen wird, empfiehlt die GDD eine dahingehende Klarstellung, dass der betriebliche Datenschutzbeauftragte sowohl zum Präventions- als auch zum Sicherheitsvorfallteam gehören muss; er sollte in das Gesamtkonzept als Mitwirkender einzubinden sein.

Völlige Unabhängigkeit: Um die Datenschutzbeauftragten in die Lage zu versetzen ihre Aufgaben effektiv erfüllen zu können, müssen ihnen die nötigen Kompetenzen, Mittel, Einrichtungen, Ausstattungen und Ressourcen insgesamt garantiert werden. Einmal bestellt, sollte der Datenschutzbeauftragte in der Lage sein, sich in unabhängiger Art und Weise sein eigenes professionelles Urteil zu bilden. Hinsichtlich der völligen Unabhängigkeit der Datenschutzbeauftragten ist es besonders wichtig, ihnen ein direktes Vortragsrecht gegenüber der Leitung der verantwortlichen Stelle einzuräumen. Nach deutschem Datenschutzrecht ist der Datenschutzbeauftragte der Leitung der verantwortlichen Stelle unmittelbar zu unterstellen.

Insgesamt ist es aus Sicht der GDD wünschenswert, dass sich die Rolle des Datenschutzbeauftragten nicht lediglich auf eine reine Compliance-Funktion reduziert. Angesichts der wachsenden Gefahren für die Persönlichkeitsrechte der Betroffenen sollte die Rolle von Datenschutzbeauftragten zukünftig auch zunehmend strategisch ausgerichtet sein.

Qualifikationen: Nur qualifizierte Datenschutzbeauftragte können ihre zunehmend wichtige Aufgabe effektiv erfüllen. Daher sollte das zukünftige EU-Datenschutzrecht zumindest einige essentiell wichtige Job-Voraussetzungen beinhalten. Die GDD hat vor einiger Zeit eine Studie über die notwendige Qualifikation von Datenschutzbeauftragten durchgeführt. Die Ergebnisse dieser Studie sind aktuell im Wesentlichen durch die obersten Datenschutzaufsichtsbehörden in Deutschland bestätigt worden (Beschluss des Düsseldorfer Kreises am 24./25. November 2010). Nach dem GDD-Ausbildungskonzept sollte der Datenschutzbeauftragte insbesondere über Kenntnisse in folgenden Bereichen verfügen:

- Datenschutzrecht und -organisation,
- Technisch-organisatorischer Datenschutz,
- Datenschutz-Management.

Basierend auf diesen Ausbildungsinhalten hat die GDD u. a. ein Konzept zur Zertifizierung betrieblicher Datenschutzbeauftragter entwickelt (GDDcert.).

Ergänzend sei erwähnt, dass das BDSG seit dem Jahr 2009 eine Pflicht der verantwortlichen Stellen beinhaltet, dem Datenschutzbeauftragten die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

IV. Datenverarbeitung in – internationalen – Unternehmensgruppen

Die EU-Kommission beabsichtigt die Regelungen für internationale Datentransfers klarer zu fassen und zu vereinfachen.

In Ergänzung zu der von der GDD zu diesem Themenkomplex bereits abgegebenen Stellungnahme weist die GDD darauf hin, dass jüngst die Deutsche Bundesregierung (BT-Drs. 17/4230) die Auffassung des Deutschen Bundesrates (BR-Drs. 535/10) geteilt hat, wonach im Rahmen der Reform der EU-Datenschutzrichtlinie die Fragen des Konzerndatenschutzes zu beraten sind. Nach Auffassung der Bundesregierung bedarf dabei insbesondere die Frage, welche Arten von Unternehmenszusammenschlüssen erfasst werden sollen, weiterer vertiefter Untersuchungen.

Hinweise:

Die GDD-Stellungnahme im Rahmen der ersten von der EU-Kommission durchgeführten Konsultation und eine dazugehörige Executive Summary sind auf der Website der Kommission abrufbar unter

http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/gdd_de.pdf

bzw.

http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/gdd_en.pdf.

Die aktuelle Stellungnahme der GDD ist in englischer Sprache abrufbar unter
https://www.gdd.de