EU-Grundverordnung zum Datenschutz

Was könnte sich für die Unternehmenspraxis ändern?

DB Mobility Logistics AG

Konzerndatenschutz

Karen Sokoll, LLM

20.04.2013

Agenda

1. Überblick: Ziel & Stand des Gesetzgebungsverfahrens

2. Mögliche Änderungen

- Datenschutzorganisation
- Kundendatenschutz
- Beschäftigtendatenschutz
- Konzernweite/internationale Datentransfers
- Joint Controllership
- Zertifikate und Prüfsiegel

Entwurf Europäische Grundverordnung Datenschutz („EU DS GVO-E“) - Zielsetzung

- **Weiterentwicklung der EU-Richtlinie 95/46/EG**
  - Harmonisierung der Vorschriften zur Datenverarbeitung im EU-Raum
  - Stärkung und Schutz der Grundrechte und Grundfreiheiten natürlicher Personen
  - Schaffung eines **einheitlichen Rechtsrahmens** für den freien Datenverkehr zwischen den Mitgliedstaaten
  - Weiterentwicklung des EU-Binnenmarkts
  - Wahrung der Betroffenenrechte auch bei Datenübermittlungen aus der EU in Drittländer und z.T. der Verarbeitung von Daten der EU-Bürger durch Unternehmen in Drittländern

- **Anpassung an neuere Entwicklungen mit Datenschutzrelevanz** (Social Networks, etc.)

Unterschied Verordnung – Richtlinie

EU-Richtlinie	Umsetzung in nationales Recht der Mitgliedstaaten ist erforderlich. Abweichungen zur *Verbesserung* des Schutzniveaus sind zulässig.
EU-Verordnung	Unmittelbare Gültigkeit in allen EU-Mitgliedstaaten Abweichung durch nationales Recht „*nach oben oder unten*“ ist grundsätzlich nicht zulässig. Ziel: Schaffung eines einheitlichen Standards & von mehr Rechtssicherheit. Vorliegend allerdings … ▪ zahlreiche Optionen zum Erlass delegierter Rechtsakte durch die EU-Kommission ▪ einzelne Bereiche, wie der Beschäftigten- und Sozialdatenschutz, können weiterhin auf Basis nationaler Rechtsvorschriften geregelt werden, sofern im Rechtsrahmen der EU DS GVO.

Zeitschiene

bis Ende Mai 2013

- Kommissions-entwurf
- Änderungsan-träge der Frak-tionen des EP
- Stellungnahme der Ausschüsse
- Orientierungs-abstimmung im Innenausschuss EP (LIBE)

ab Juni 2013

Entwurfs-abstimmung zwischen Kommission, EP und Rat

Beispiele: Änderungen gegenüber dem Status Quo

Datenschutzorganisation

Rolle des DSB (Art. 35 – 37 EU DS GVO-E):

- Pflicht zur Bestellung eines DSB ab 250 Mitarbeitern (Entwurf EU-Parlament: ab 500 Betroffenen)
- Befristung der Bestellung des DSB auf minimal zwei Jahre möglich (Entwurf EU-Parlament: vier Jahre, aber ohne Wiederbestellungsoption)
- Hauptaufgaben des DSB: Monitoring und Beratung in Datenschutzangelegenheiten

Dokumentationspflichten (Art. 28 EU DS GVO-E):

- Pflicht zur umfassenden Dokumentation der Verarbeitungsvorgänge für Verantwortliche und Auftragsverarbeiter (inkl. Datenkategorien, Datenempfängern, Löschfristen, ggf. Übermittlungen in Drittstaaten). Die Dokumentation ist der Aufsichtsbehörde auf Verlangen vorzulegen.

Datenschutz-Folgenabschätzung (Art. 33 EU DS VO-E):

- Abschätzung der Risiken für die Persönlichkeitsrechte der Betroffenen und vorgesehenen Gegensteuerungsmaßnahmen durch die Verantwortlichen und Auftragsverarbeiter

Beispiele: Änderungen gegenüber dem Status Quo

Datenschutzorganisation

Meldepflichten bei Datenschutzvorfällen (Art. 31 EU DS GVO-E):

- Meldung von Datenschutzvorfällen bei der zuständigen Aufsichtsbehörde möglichst binnen 24 Stunden (Entwurf EU-Parlament: binnen 72 Stunden)

Sanktionen (Art. 79 EU DS GVO-E):

- Bußgelder bis zu 1.000.000 € oder 2 % des weltweiten Jahresumsatzes möglich

Beispiele: Änderungen gegenüber dem Status Quo

Kundendatenschutz

Information der Betroffenen (Art. 14 insbes. Abs. 1 b) und g) EU DS GVO-E):

Erweiterte Informations- und Auskunftspflichten gegenüber den Betroffenen, u.a. zu Verwendungszwecken und Übermittlungsabsichten in Drittstaaten

Recht auf „Vergessenwerden“ (Art. 17 EU DS-GVO-E):

Undifferenziertes Verbot der Weiterverbreitung personenbezogener Daten ist in der Praxis kaum umsetzbar:

- Verlinkungen von Social Networks untereinander durch den Betroffenen können eine Löschung der personenbezogenen Daten durch die verantwortliche Stelle mit vertretbarem Aufwand unmöglich machen.

Recht auf Datenübertragung (Art. 18 EU DS GVO-E):

Option des Betroffenen, sämtliche personenbezogenen Daten auf einen neuen Verantwortlichen zu übertragen, ist in der Praxis u.U. nicht umsetzbar oder zumutbar:

- Kollision mit anderen Rechtsnormen
- Weitergabe von Betriebs- und Geschäftsgeheimnissen

Beispiele: Änderungen gegenüber dem Status Quo

Beschäftigtendatenschutz

Datenverarbeitung im Beschäftigungskontext (Art. 82 EU DS GVO-E):

- EU DS GVO ist Rechtsrahmen für spezifische nationale Regelungen
- Beibehaltung von Betriebsvereinbarungen/Tarifverträgen möglich (sie sollten auch ausdrücklich als Rechtsgrundlage genannt werden!)
- Noch nicht absehbar: Reichweite möglicher „delegierter Rechtsakte“

Einwilligung im Beschäftigtenverhältnis (Art. 7 Abs. 4 und Erwägungsgrund 34 EU DS GVO-E):

- Bedeutet dies den kategorischen Ausschluss der Einwilligung im Beschäftigtenverhältnis, auch in Fällen, in denen sie ausschließlich zum Vorteil des Beschäftigten als Rechtsgrundlage dienen kann?

Beispiele: Änderungen gegenüber dem Status Quo

Internationale Datentransfers

Datenübermittlung auf Basis eines Angemessenheitsbeschlusses (Art. 41 Abs. 5 und 6 EU DS GVO-E):

- Feststellung eines nicht angemessenen Datenschutzniveaus in einem Drittland durch die EU-Kommission mit Untersagung der weiteren Datenübermittlung in das betroffene Drittland (unterschiedliche Interpretationen in Verbindung mit anderen Artikeln der GVO möglich, Klarstellung wegen der möglichen wirtschaftlichen Folgen dringend erforderlich)

Kohärenzverfahren (Art. 55 – 63 EU DS GVO-E):

- Durchführung auf Antrag einer Aufsichtsbehörde, des EU-Datenausschusses oder der EU-Kommission

- Ziel: Einheitliche Rechtsanwendung durch die Aufsichtsbehörden

Beispiele: Änderungen gegenüber dem Status Quo

Joint Controllership

Gemeinsame Verantwortliche für eine Datenverarbeitung (Art. 24 und Art. 26 (4) EU DS GVO-E):

- Durch die EU GVO für alle EU-Mitgliedstaaten verbindliche Umsetzung der bereits in der Richtlinie 95/46/ EG definierten Joint Controllership (bislang nicht in BDSG transformiert)

- **Vorteil:** Bei grenzüberschreitenden Datenverarbeitungen ist die Dokumentation und Datenschutzfolgenabschätzung nur einmalig durchzuführen, sofern keine weiteren nationalen Regelungen zu berücksichtigen sind.

- **Risiko:** Keine eindeutige Zuweisung, bis hin zur gewollten Verschleierung, der konkreten Verantwortlichkeiten. Der Entwurf des EU-Parlaments fordert deshalb klar definierte und dokumentierte Verantwortlichkeiten der Beteiligten oder eine gesamtschuldnerische Haftung bzw. Haftung eines nach Ermessen des Betroffenen ausgewählten Verantwortlichen.

Beispiele: Änderungen gegenüber dem Status Quo

Zertifikate und Prüfsiegel

Zertifikate und Prüfsiegel (Art. 39 EU DS GVO-E):

- Förderung von datenschutzspezifischen Zertifizierungsverfahren und Prüfsiegeln angestrebt
- Vorteile:
  - Orientierungshilfe für Betroffene und bei der Auswahl von Auftragsverarbeitern
  - Chance für Erleichterungen bei der Prüfung interner und externer Auftragsverarbeiter durch den Auftraggeber

Vielen Dank für Ihre Aufmerksamkeit!