Stefan Loebisch
Rechtsanwalt

Datenschutz und Datensicherheit in kleinen und mittelständischen Unternehmen

Die neue EU-Datenschutzgrundverordnung

Landshut 19.03.2013

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. Inhalt
5. Zeitplan

Inhalt

- Hintergrund: Von der Datenschutz-Richtline zur Datenschutz-Verordnung
- EU-Rechtsgrundlagen:
  Richtline - Verordnung – Unterschied
- Adressaten der Datenschutz-Grundverordnung
- Inhalt der Datenschutz-Verordnung: Entwurf vom 25.01.2012
- Zeitplan: Vom Entwurf zum In-Kraft-Treten

1. **Hintergrund**
2. EU-Rechtsgrundlagen
3. Adressaten
4. Inhalt
5. Zeitplan

1. Hintergrund: Von der Datenschutz-Richtline zur Datenschutz-Verordnung

- Derzeitige Rechtsgrundlage: EU-Datenschutz-Richtlinie 1995

- Ziel der Datenschutz-Grundverordnung

1. **Hintergrund**
2. EU-Rechtsgrundlagen
3. Adressaten
4. Inhalt
5. Zeitplan

1.1 EU-Datenschutz-Richtlinie 1995

- In der Bundesrepublik durch verschiedenen Reformen des BDSG umgesetzt

- Innerhalb der EU-Staaten uneinheitliches Datenschutzniveau
  z.B. Cookie-Richtlinie: In der Bundesrepublik Deutschland nicht in nationales Recht umgesetzt, im Vereinigten Königreich, den Niederlanden und Frankreich umgesetzt

1. **Hintergrund**
2. EU-Rechtsgrundlagen
3. Adressaten
4. Inhalt
5. Zeitplan

1.2 Ziel der Datenschutz-GrundVO

- Reibungsloser Transfer personenbezogener Daten innerhalb der EU

- EU-weit soll allen Betroffenen einen wirksamer Datenschutz garantiert werden

1. Hintergrund
2. **EU-Rechtsgrundlagen**
3. Adressaten
4. Inhalt
5. Zeitplan

2. EU-Rechtsgrundlagen: Richtline - Verordnung - Unterschied

- Rechtswirkung der EU-Richtline

- Rechtswirkung der EU-Verordnung

1. Hintergrund
2. **EU-Rechtsgrundlagen**
3. Adressaten
4. Inhalt
5. Zeitplan

2.1 EU-Richtline

Keine unmittelbare Wirkung in den Mitgliedstaaten:

- Richtlinien setzen regelmäßig eine Frist, innerhalb derer sie in innerstaatliches Recht umgesetzt werden müssen
- Die Umsetzung erfolgt, indem
  - ein innerstaatliches Gesetz neu erlassen
  - oder ein bestehendes innerstaatliches Gesetz an die Vorgaben der Richtlinie angepasst wird

  → z.B. BDSG-Reformen 2009

1. Hintergrund
2. **EU-Rechtsgrundlagen**
3. Adressaten
4. Inhalt
5. Zeitplan

2.1 EU-Verordnung

Gelten unmittelbar in jedem Mitgliedstaat:

- Müssen von den EU-Mitgliedstaaten nicht in nationales Recht umgesetzt werden („Durchgriffswirkung“)
- Modifikationen der vorgegebenen Regelungen durch die einzelnen Mitgliedstaaten sind grundsätzlich nicht möglich („Umsetzungsverbot“)

1. Hintergrund
2. EU-Rechtsgrundlagen
3. **Adressaten**
4. Inhalt
5. Zeitplan

3. Adressaten der Datenschutz-Grundverordnung

- Alle öffentlichen und nicht-öffentlichen Stellen, die Daten innerhalb der EU verarbeiten
- Unternehmen, die personenbezogene Daten von EU-Bürgern im Zusammenhang mit dem Anbieten von Waren und Dienstleistungen in der EU verarbeiten, unabhängig davon, wo sich deren Sitz befindet.

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4. Inhalt der Datenschutz-Verordnung: Entwurf vom 25.01.2012

- Definition personenbezogener Daten
- Privacy by Design / Privacy by Default
- Explizite Einwilligung
- Recht auf Vergessenwerden
- Auskunft und Korrektur
- Datenportabilität
- Auftragsdatenverarbeitung
- Meldepflicht bei Datenpannen
- Betrieblicher Datenschutzbeauftragter
- Datenübermittlung in Nicht-EU-Länder
- One-Stop-Shop
- Sanktionen: Erhöhung von Bußgeldern

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.1 Definition personenbezogener Daten Art. 4 VO-Entwurf

- „alle Informationen, die sich auf eine Personen beziehen“

- Neu: „Standortdaten“ und „Onlinekennungen“ als mögliche Mittel der Identifikation
- Erwägungsgrund 24: IP-Adressen oder Cookies fallen nicht zwangsläufig darunter

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.2 Privacy by Design / Privacy by Default (1)

- Datensparsamkeit - Art. 5 VO-Entwurf
  „auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt“

- Zweckbindung - Art. 5 VO-Entwurf:
  „... müssen für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.2 Privacy by Design / Privacy by Default (2)

- Anonymität / Pseudonymität - Art. 5 und 10 VO-Entwurf:

  - Art. 5 VO-Entwurf: „(Personenbezogene Daten) dürfen nur verarbeitet werden, wenn und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können“

  - Art. 10 VO-Entwurf: „Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, ist er nicht verpflichtet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen.“

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.2 Privacy by Design / Privacy by Default (3)

- Verbot nicht genehmigter Nutzerprofile - Art. 20 VO-Entwurf:

  "Eine natürliche Person hat das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden..."

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.3 Explizite Einwilligung - Art. 6 bis 8 VO-Entwurf

- Art. 6 VO-Entwurf: ein oder mehrere genau festgelegte Zwecke
- Art. 7 VO-Entwurf: Beweislast der verantwortlichens Stelle für Einwilligung
- Art. 8 VO-Entwurf: Personenbezogene Daten eines Kindes bis zum vollendeten 13. Lebensjahr

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.4 Auskunft und Korrektur - Art. 14 bis 16 VO-Entwurf

- **Jetzt bereits:** §§ 34, 35 BDSG - Recht auf Auskunft, Berichtigung und Löschung

- **Neu** Art. 17 Ziff. 1 - Lex facebook:

  Anspruch, solche personenbezogene Daten zu löschen und ihre weitere Verbreitung zu unterlassen, die die betroffene Person im **Kindesalter** öffentlich gemacht hat

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.5 Recht auf Vergessenwerden - Art. 17 VO-Entwurf

- **Derzeit:** § 35 BDSG - Recht auf Datenlöschung

- **Neu:** Ausweitung auf eine differenzierte Anspruchsgrundlage:

  Hat eine datenverarbeitende Stelle die Daten veröffentlicht oder die Veröffentlichung beauftragt, wird ihr die Pflicht auferlegt, alle zumutbaren Schritte zu unternehmen, auch Dritte, an die die Daten weiter gegeben wurden, über den Löschwunsch zu informieren.

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.6 Datenportabilität - Art. 18 VO-Entwurf

Verbraucher sollen ihre einmal auf einer Plattform abgelegten oder eingestellten Daten

- barrierefrei zu einer anderen Plattform „transportieren“ dürfen

- oder eine elektronische Kopie ihrer Daten erhalten.

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.7 Auftragsdatenverarbeitung Art. 26 VO-Entwurf

- Nicht nur: Cloud Computing
- **Jetzt:** § 11 BDSG - schriftlicher Datenverarbeitungsauftrag

- **Neu:**
- Pflicht des Auftragnehmers (d.h. Rechenzentrumsbetreiber, Cloud-Anbieter, Anbieter von Fernwartung), dem Auftraggeber nach Abschluss der Verarbeitung sämtliche **Ergebnisse** auszuhändigen
- Ausdrückliches Verbot, die personenbezogenen Daten nach Abschluss des Auftrags auf **andere Weise** weiterzuverarbeiten
- Pflicht des Auftragnehmers, Auftraggeber und Aufsichtsbehörde alle erforderlichen **Informationen für die Kontrolle** der Einhaltung der Pflichten zur Verfügung zu stellen

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.8 Meldepflicht bei Datenpannen Art. 31 VO-Entwurf

- **Jetzt:** § 42a BDSG - Aufsichtsbehörde und Betroffene muss nur bei Datenpanne in Verbindung mit
  - besonderen Arten personenbezogener Daten
  - oder Informationen zu Berufsgeheimnissen
  - oder Straftaten und Ordnungswidrigkeiten
  - oder Bank- und Kreditdaten

  benachrichtigt werden
- **Neu:** Meldepflicht bei "Datenpannen" schon bei jeglichem Verlust von Daten
- Meldefrist soweit möglich innerhalb von 24 Stunden

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.9 Betriebl. Datenschutzbeauftragter Art. 35 VO-Entwurf

- Jetzt: § 4f BDSG - mehr als 9 Personen

- Neu: Erst ab 250 Mitarbeitern

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.10 Datenübermittlung in Nicht-EU-Länder - Art. 40 ff. VO-Entwurf

- regelkonforme Datentransfers außerhalb der EU vorzunehmen sind u.a. mittels

  - EU-Standardvertragsklauseln

  - oder ah hoc genehmigten Vertragsklauseln

- Binding Corporate Rules (verbindliche unternehmensinterne Vorschriften) als favorisierte Lösung

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.11 One-Stop-Shop - Art. 51 VO-Entwurf

- Aufsichtsbehörde des EU-Mitgliedsstaates zuständig, in dem sich der Hauptsitz befindet
- Maßgeblich: Ort, an dem wichtigsten Unternehmensentscheidungen getroffen werden
- Unternehmen ohne EU-Niederlassung: ausschlaggebend, wo der überwiegende Teil der Datenverarbeitung innerhalb der EU stattfindet

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. **Inhalt**
5. Zeitplan

4.12 Sanktionen: Erhöhung von Bußgeldern - Art. 79 VO-Entwurf

- Jetzt: § 43 BDSG - Bußgeld im Regelfall bis 300.00 €

- Neu: maximal 2% des globalen Jahresumsatzes; Höchstbetrag 1 Mio. €

1. Hintergrund
2. EU-Rechtsgrundlagen
3. Adressaten
4. Inhalt
5. **Zeitplan**

5. Zeitplan: Vom Entwurf zum In-Kraft-Treten

- 27.02.2013: Frist für Änderungsanträge
- 18./19.03.2013: Abstimmung im Rechtsausschuss
- 20.03.2013: Erste Diskussion der Änderungsanträge im Innenausschuss
- Ende April 2013: Orientierungsabstimmung im Innenausschuss
- ab Mai oder Juni 2013 (je nach Verhandlungsstand im Rat): Verhandlungsbeginn zwischen Europäischem Parlament, Rat und Europäischer Kommission („Trilog“)
- In Kraft 2 Jahre nach ihrer Verabschiedung und Veröffentlichung im Verordnungsblatt, d.h. vsl. nicht vor Sommer 2015

Vielen Dank für Ihre Aufmerksamkeit!

RA Stefan Loebisch :: Steiningergasse 5 :: 94032 Passau

:: Telefon (08 51) 756 80 74 :: Telefax (08 51) 756 80 76 ::

www.loebisch.de

www.xing.com/profile/Stefan_Loebisch

info@loebisch.de