SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Betrieblicher Datenschutz (Kunden- und Beschäftigten-Daten)

Agenda

1. Allgemeine Regelungen, die auf alle betroffenen Personen anwendbar sind
2. Ergänzende Ausführungen zum betrieblichen Datenschutzbeauftragten
3. Beschäftigtendatenschutz
4. Kundendatenschutz und Werbung

1. Betroffenenrechte (1)

Neu:

- **Recht auf Datenübertragbarkeit**, Art. 20

  „Portabilität“ von Daten über die Betroffene Person oder direkt von einem auf den anderen Verantwortlichen, wenn Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und automatisiert erfolgt.

- **Recht auf Vergessenwerden**, Art. 17

  Haben Verantwortliche Daten öffentlich gemacht und müssen sie diese auf Antrag löschen, so treffen sie angemessene Maßnahmen, um weitere Verantwortliche darüber zu informieren, dass Löschung von Links, Kopien oder Replikationen verlangt wurde

1. Betroffenenrechte (2)

Erweitert:

- **Informationspflichten**, Art. 12, 13, 14
  - Betroffene Person muss zusätzlich informiert werden über: Kontaktdaten des Datenschutzbeauftragten, Rechtsgrundlage der Datenverarbeitung, Interessenabwägung, Dauer der Speicherung oder Kriterien der Festlegung der Dauer, Betroffenenrechte, Widerspruchsrecht, Recht auf Widerruf der Einwilligung, Drittstaatentransfer, Zweckänderung, Beschwerderecht bei Aufsichtsbehörde, automatisierte Entscheidungsfindung einschließlich Profiling
  - Information muss auch erfolgen, wenn Daten aus öffentlichen Quellen stammen

Form: schriftlich, elektronisch, mündlich (wenn Identität nachgewiesen)

1. Betroffenenrechte (3)

- **Rechtsfolgen bei Verstößen**
  Aufsichtsrechtliche Maßnahmen und Bußgelder bis zu 20 Mio. €

- **Tipps**
  - legen Sie Verfahren und Zuständigkeiten bzgl. der Betroffenenrechte fest, die es ermöglichen, die Rechte wahrzunehmen
  - passen Sie Ihre IT-Strukturen an, so dass Betroffenenrechte effizient erfüllt werden können
  - entwickeln Sie Vorlagen für die Belehrungen

1. Dokumentationspflichten (1)

- **Rechenschaftspflicht**, Art. 5 Abs. 2
  Nachweis der Einhaltung der Grundsätze der Datenverarbeitung (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit)
- **Nachweispflicht bzgl. Einhaltung der DSGVO**, Art. 24 Abs. 1
  Ergreifung techn. und org. Maßnahmen zum Nachweis, dass DSGVO eingehalten wird (müssen aktuell gehalten werden)
- **Verzeichnis der Verarbeitungstätigkeiten**, Art. 30
  Nicht mehr Aufgabe des Datenschutzbeauftragten, sondern der Verantwortlichen oder Auftragsverarbeiter; muss nicht (mehr) jedermann zur Verfügung gestellt werden; Vordrucke demnächst auf Homepages der Aufsichtsbehörden; Inhalte ähnlich derzeitigem Verfahrensverzeichnis; bei Verstoß Bußgeld bis 10 Mio. € (Art. 83 Abs. 4)

1. Dokumentationspflichten (2)

- **Rechtsfolgen bei Verstößen**
  Aufsichtsrechtliche Maßnahmen und Bußgelder bis zu 10 Mio. € (Verstoß gegen Art. 30) bzw. 20 Mio. € (Verstoß gegen Art. 5)

- **Tipps**
  - Entwickeln Sie betriebsinterne Verfahren, Muster, Aufstellungen, die beweissicher dokumentieren, auf welcher Rechtsgrundlage und zu welchem Zweck die jeweilige Datenverarbeitung erforderlich ist
  - Dokumentieren Sie die techn. und org. Schutzmaßnahmen
  - Legen Sie die Verantwortlichkeiten, insbesondere für das Verzeichnis von Verarbeitungstätigkeiten, fest

1. Meldepflicht bei Datenschutzverletzungen (1)

(gilt für alle Datenarten, Art. 33)

- **Auftragsverarbeiter** meldet dem Verantwortlichen
- **Erfolgt** Meldung nicht binnen 72 Stunden, ist deren Verzögerung zu begründen
- **Inhalt**: Art der Verletzung, Kategorie und Anzahl der betroffenen Personen und Datensätze, Anlaufstelle, wahrscheinliche Folgen, Abwehrmaßnahmen
- Meldepflicht **entfällt**, wenn Verletzung „**nicht zu einem Risiko** für die Rechte und Freiheiten einer natürlichen Person führt.“
- Besteht ein **hohes Risiko**, so ist unverzüglich die **betroffene Person** zu benachrichtigen
  (Ausnahme: Daten mittlerweile für Unbefugte unzugänglich, Risiko besteht nicht mehr, Benachrichtigung unzumutbar (dann aber öff. Bekanntmachung))

1. Meldepflicht bei Datenschutzverletzungen (2)

Tipp:

Informieren Sie alle Beschäftigen, die mit der Verarbeitung personenbezogener Daten befasst sind von der Meldepflicht und **legen Sie fest**, wer die Meldung ggü. der Behörde und die Benachrichtigung ggü. den betroffenen Personen fertigt.

2. Betrieblicher Datenschutzbeauftragter, Art. 37 ff

Ist gemäß Art. 37 zu benennen, wenn **Kerntätigkeit**

- aus Verarbeitungsvorgängen besteht, die eine **regelmäßige und systematische Überwachung** erforderlich machen
- in der umfangreichen Verarbeitung **besonderer Kategorien** von Daten (Art. 9) oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht
- Achtung, hier **Regelungsoption**:
  - Mitgliedstaaten können zusätzliche Benennungspflichten vorsehen
  - Wahrscheinlich Benennung nach wie vor immer, wenn mehr als neun Personen ständig mit automatisierter Verarbeitung von personenbezogenen Daten beschäftigt sind (derzeit § 4f BDSG)

2. Stellung des betrieblichen Datenschutzbeauftragten, Art. 38

Der betriebliche Datenschutzbeauftragte…

- ist frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **eingebunden**
- ist durch Ressourcen und Zugang zu Verarbeitungsvorgängen **zu unterstützen**
- ist **weisungsfrei**, darf wegen der Erfüllung seiner Aufgabe nicht abberufen oder benachteiligt werden, berichtet unmittelbar der höchsten Managementebene
- kann von betroffenen Personen **zu Rate gezogen** werden
- ist an **Geheimhaltung und Vertraulichkeit** gebunden
- kann **andere Aufgaben** wahrnehmen, sofern **kein Interessenkonflikt** vorliegt

2. Aufgaben des betrieblichen Datenschutzbeauftragten

- **Unterrichtung und Beratung** der Verantwortlichen, Auftragsverarbeiter und Beschäftigten
- **Überwachung** der Einhaltung der Datenschutzvorschriften
- Beratung im Zusammenhang mit der **Datenschutz-Folgeabschätzung**
- **Zusammenarbeit** mit der **Aufsichtsbehörde**
- **Anlaufstelle** für Aufsichtsbehörde

3. Beschäftigtendatenschutz (1)

- Einwilligung, Art. 7
  - ist „keine gültige Rechtsgrundlage“ für die Verarbeitung, wenn „ein klares Ungleichgewicht besteht“ (EG 43) – wird im Beschäftigungsverhältnis häufig anzunehmen sein
  - gilt i. d. R. nicht als erteilt, wenn die Erfüllung eines Vertrages, einschließlich die Erbringung einer Dienstleistung, von der Einwilligung abhängig ist
- Regelungsoption, Art. 88

  Mitgliedstaaten können durch Rechtsvorschrift oder Kollektivvereinbarung (Tarifverträge, Betriebsvereinbarungen) spezifischere Vorschriften zur Gewährung des Schutzes der Rechte und Freiheiten vorsehen
  - weitgehende Fortgeltung des § 32 BDSG?
  - Verarbeitungen aufgrund gesetzlicher Verpflichtungen weiter möglich
  - konzernintern kann ein berechtigtes Interesse darin bestehen, Beschäftigtendaten zu Verwaltungszwecken zu übermitteln (gilt auch für Kundendaten, EG 48)

3. Beschäftigtendatenschutz (2)

➢ Tipp

- behalten Sie die Entwicklung des BDSG-Nachfolgegesetzes im Auge

- prüfen Sie Einwilligungen insbes. bzgl. des „Ungleichgewichts“

- prüfen Sie, inwieweit Tarifverträge und Betriebsvereinbarungen anzupassen sind; diese müssen angemessene Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbes. im Hinblick auf Transparenz, Übermittlung, Überwachung umfassen, Art. 88 Abs. 2

- legen Sie die Zwecke der Verarbeitung **bei Erhebung** fest, damit Zweckänderungen prüfbar sind

4. Kundendatenschutz

Die Verarbeitung von personenbezogenen Kundendaten kann zulässig sein aufgrund:

- **Einwilligung**, Art. 6 Abs. 1 Nr. 1
  Einwilligung muss **nachgewiesen** werden, **eindeutig und freiwillig** erteilt worden sein (Problem bei Abhängigkeitsverhältnissen) und einen Hinweis auf **Widerruf** enthalten, Art. 7
- **Rechtsvorschrift**
  - Art. 6 Abs. 1b: Verarbeitung ist zulässig, wenn sie **zur Erfüllung eines Vertrages erforderlich** ist (nicht: Werbung, Problem: Geburtsdaten?)
  - Art. 6 Abs. 1f: **Interessenabwägung** (EG 47: „Direktwerbung **kann** als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden“)
  - Weitere Alternativen des Art. 6 Abs. 1
- **Zweckänderung** (bei Weiterverarbeitung), Art. 6 Abs. 4
  Weiterverarbeitung muss hier mit Zweck der Erhebung **vereinbar** sein

4. Kundendatenschutz (2)

- DSGVO nicht anwendbar auf personenbezogene Daten **juristischer Personen** (EG 14)
- DSGVO ist anwendbar, wenn Daten von **Funktionsträgern** der juristischen Person verarbeitet werden

- **Tipp**
  - prüfen Sie, ob Einwilligungen den Anforderungen der DSGVO entsprechen und nachgewiesen werden können; enthält sie Hinweis auf Widerruf?
  - prüfen Sie, nach welcher Vorschrift die Verarbeitung zulässig ist
  - legen Sie die Zwecke der Verarbeitung bei Erhebung fest, damit Zweckänderungen (Werbung) prüfbar sind

4. Werbung

- **Wegfall** des sog. „**Listenprivilegs**“ (z. B. Anschriften), aber:
- Werbung ist nur dann zulässig, sofern nicht die **Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten** erfordern, die **berechtigten Interessen des Werbenden** überwiegen
  Problem: ist Werbung **absehbar** (EG 47)? Art und Weise, Intensität…
- Besonderer Schutz für **Kinder** erforderlich, EG 38
  „Kind“ nach DSGVO meint alle nach deutschem Recht **Minderjährigen**
- Beschränkungen des **UWG** sind weiterhin zu beachten, soweit ePrivacy Richtlinie nicht geändert wird
  http://www.datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Materialien/Was_darf_Werbung.pdf
- Nach **Werbewiderspruch** keine Verarbeitung mehr zulässig, Art. 21 Abs. 3

4. Werbung

- **Tipp**
  - beachten Sie bei Art und Weise jeglicher Werbung, dass keine berechtigten Interessen des Beworbenen überwiegen
  - achten Sie auf die evtl. Neufassung der ePrivacy-Richtlinie

Vielen Dank für Ihre Aufmerksamkeit!

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Geschäftsstelle und Besucheradresse: Leiterstraße 9, 39104 Magdeburg
Postadresse: Postfach 1947, 39009 Magdeburg

poststelle@lfd.sachsen-anhalt.de

Telefon: 0391 81803-0
Telefax: 0391 81803-33