Auditprozess beim Auftragsdatenverarbeiter: Darf’s ein bißchen mehr sein?

Itella Information GmbH
Klaus Martens
QMB
Datenschutzbeauftragter

Itella Information – Teil der Itella Gruppe

- Mehr als 300 outgesourcte Finanz- und Buchhaltungsprozesse

<u>Jährlich</u>:

- Mehr als 30 Millionen Eingangsrechnungen
- Mehr als 50 Millionen elektronische Transaktionen
- 1 900 Millionen Papierdokumente
- 1 300 Millionen Dokumente elektronisch archiviert

Itella Information Deutschland

Produktionsstandorte in:

- Düsseldorf:
  - Hochvolumiger Endlos- und Einzelblattdruck
- München:
  - Einzelblattdruck mit viel manueller Nachbearbeitung
  - COM
  - COLD
  - Scanning

Dateneingang in Frankfurt:

- Historisch, da früherer Produktionsstandort

Sicherheitsanforderungen an den Auftragsdatenverarbeiter

Gesetzliche Anforderungen

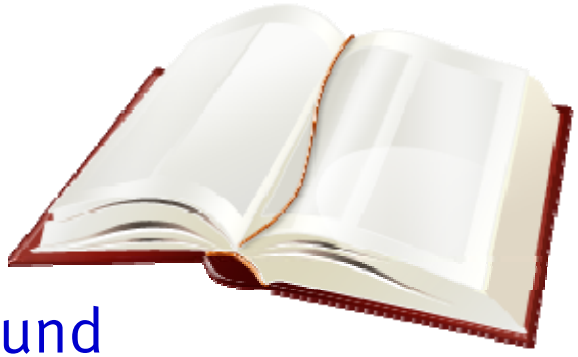
- Bundesdatenschutzgesetz (BDSG) § 9 und Anlagen regelt die Verarbeitung **personenbezogener** Daten

Kundenanforderungen

- BSI Grundschutz
- ISO 20000
- ISO 27001
- Sarbanes Oxley Act
- Kreditwesengesetz (KWG)
- + Sonstige Anforderungen (ISO 14000, FSC etc.)

§ 11 BDSG: Auftragsdatenverarbeitung

(2) ….. Der Auftrag ist schriftlich zu erteilen, wobei im Einzelnen festzulegen sind:

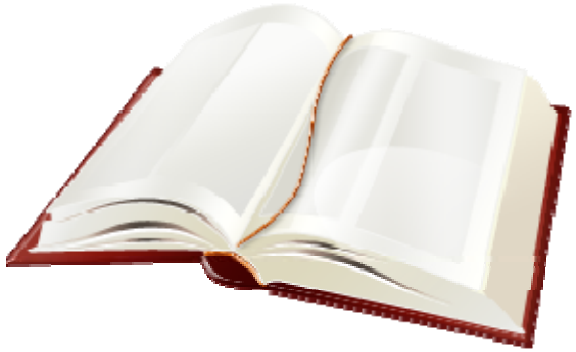


1. ……
2. ……
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen

…….. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

BDSG schweigt sich aus

- Was ist regelmäßig?
- Wie überzeugen:
  - Abfrage per Fragebogen?
  - Selbsterklärung?
  - Testat?
  - Zertifizierung (welche)?
  - Vor Ort?
- Wer trägt die Kosten?
- Wer ist zur Überprüfung geeignet?



§ 9 BDSG + Anhang: Technische und organisatorische Maßnahmen

8 Gebote:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Überprüfungen in der Praxis

- Keine
- Fragebögen
- Audits vor Ort:
  - Zwischen 2 Stunden und 2 Tagen
  - Von Einkäufern und Juristen bis zu IT-Leitern, Datenschutzbeauftragten und Sicherheitsexperten
  - Mitarbeiter des Auftraggebers und beauftragte Dienstleister

Überprüfungen in der Praxis (2)

- Verschiedene Vorgehensweisen bei Audits:
  - Planlos („Zeigen Sie mal, was Sie haben!“)
  - Vorbereiteter Fragenkatalog wird „aus dem Hut gezaubert“.
  - Fragenkatalog wird vorab zugeschickt.
  - Orientierung an BSI Grundschutz (Sollvorschriften)
  - Übertragung eigener Sicherheitseinrichtungen als Anforderung für den Dienstleister
  - Abstrakte Vorstellungen und praxisfern („Wunschkonzert“)
  - Anforderungen variieren jährlich

Überprüfungen (2)

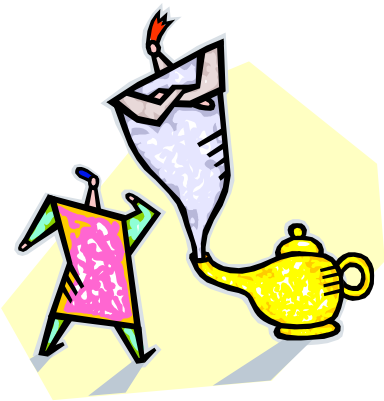
- Ergebnis:
  - Alles in Butter!

  - Das haben wir bei uns aber so und so geregelt.

  - Das müssen Sie aber unbedingt noch umsetzen.

Unser Wunsch

- Einheitlicher Standard
- Klare vertragliche Vereinbarungen:
  - Zu treffende technische und organisatorische Maßnahmen
  - Überprüfungen:
    - Art der Durchführung (Fragenkatalog, Überprüfung vor Ort)
    - Umfang
    - Kostenübernahme
- Überprüfung der **vereinbarten** Maßnahmen - und mehr nicht!



Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen bitte fragen.