Compliance Management

DSRI – Oldenburg, 16.03.2007

Dietmar Kalkbrenner
Leiter Prozess- und Projektmanagement
arxes NCC AG

Die Blickrichtung

Der Ängstliche

- sieht die Gefahren
- hat Angst – z.B. vor dem Finanzamt – und dem gläsernen Unternehmen
- wartet ab und hofft …
- kennt kein Unternehmen, dass die Compliance-Anforderungen erfüllt

Der Optimist

- sieht nicht die Risiken, sondern die Möglichkeiten.
- sieht Compliance als Möglichkeit interne Prozesse zu optimieren
- nutzt Informationen, um Risiken zu minimieren
- will agieren, nicht reagieren.

Compliance – Überblick

Was ist Compliance?

- Befolgung und Einhaltung von **„Spielregeln“,** d.h.:
- Rechtliche (Gesetze, Unternehmenssatzung), unternehmerische (Bilanzanforderungen, Rechnungslegung) und sonstige Branchen-Standards (ITIL, IFRS)
- Regelverstoß wird bestraft: Risiken für Unternehmen, Unternehmer und Geschäftsführung

Wo ist Compliance geregelt?

- Unternehmensorganisationsregeln (KonTraG, UMAG, HBG, Basel II etc.)
- Datenschutz (BDSG), Datensicherheit (IT-Security)
- Arbeitsrecht
- Buchhaltung, Rechungslegung, Prüfung (HGB, GoB, **GoBS**, **GDPdU**; IFRS, SOX

Was droht bei Complianceverstößen?

- Haft, Geldbußen, Hausdurchsuchungen, Presseberichterstattung
- Bußgeldverfahren wegen Aufsichtspflichtverletzung gegen geschäftsführende Organmitglieder (OWi)

Ausgangssituation am Beispiel GDPdU

- Durch das Steuersenkungsgesetz (01/02) wurde die Abgabenordnung (AO) geändert
- Die AO stellt bzgl. der Archivierung u.a. die Anforderung der **Revisionssicherheit**
- Die **Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen** (GDPdU) liegen in der AO begründet

Artikel 7 – Änderung der Abgabenordnung

„(6) Sind die Daten nach Absatz 1 mit Hilfe eines Datenverarbeitungssystems erstellt worden, hat die Finanzbehörde im Rahmen einer Außenprüfung das Recht, **Einsicht in die gespeicherten Daten** zu nehmen und das **Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen**. Sie kann im Rahmen einer Außenprüfung auch verlangen, dass Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die maschinell **verwertbaren Datenträger zur Verfügung gestellt werden**.

Die Kosten trägt der Steuerpflichtige

„Bei der Führung der Bücher und der sonst erforderlichen Aufzeichnungen muss insbesondere sichergestellt sein, dass während der Dauer der Aufbewahrungsfrist die Daten **jederzeit verfügbar** sind und **unverzüglich lesbar gemacht** werden können."

Stand der Vorbereitung in den Unternehmen

Nach einer Umfrage der SER Solutions Deutschland GmbH sind erst

- **6%** der Befragten* auf die elektronische Steuerprüfung vorbereitet (**)
- **9%** können die Daten im Beschreibungsstandard zur Verfügung stellen
- **11%** haben GDPdU-Projekte im Portfolio
- **17%** haben gerade GDPdU-Projekte neu aufgesetzt
- **76%** bewahren ihre steuerlich relevanten Daten in den Produktiv-Systemen auf

* 01/2005 - Umfrage bei 513 KMU und Großunternehmen

** 5% lt. Umfrage von Ernst &Young

E-Mail und das Steuerrecht

Frage: Was ist für die Besteuerung von Bedeutung

- Steuerlich relevant sind Daten immer dann, wenn sie für die Besteuerung des Steuerpflichtigen von Bedeutung sein können.
- Nach den GDPdU ist es Aufgabe des Steuerpflichtigen, die steuerrelevanten Daten von anderen abzugrenzen.
- ……und das ist das Problem in der Praxis…

E-Mail und das Steuerrecht

Frage: Müssen E-Mails aufgrund der GDPdU archiviert werden?

- Die offizielle Antwort:
- „E-Mails, die für die Besteuerung von Bedeutung sind, sind nach den allgemeinen Vorschriften des §147 AO aufzubewahren.“

….und dann immer dieser IT-Kram…..

Die Herausforderungen der Fachabteilungen und der IT

Vorgeschriebene Datenzugriffsarten

- **Z1 (Unmittelbar):** Direkter Zugriff auf steuerrelevante Daten in den steuerrelevanten Systemen des Steuerpflichtigen

- **Z2 (Mittelbar):** Bereitstellung von Auswertungen im steuerrelevanten System durch den Steuerpflichtigen nach Vorgaben des Prüfers

- **Z3 (Datenträgerüberlassung):** Überlassung von Datenträgern mit den angeforderten steuerrelevanten Daten durch den Steuerpflichtigen

Der Prüfer kann die Zugriffsart frei auswählen, beliebig kombinieren und auch nach erfolgter Auswahl zwischen den Zugriffsarten wechseln.

Die Herausforderungen der Fachabteilungen und der IT

Fachbereich

- Es gibt **keine konkreten Richtlinien** des Gesetzgebers / BMF
- Identifikation der steuerrelevanten Daten und Systeme
- Fachliche **Verfahrensdokumentation** für die betroffenen Systeme

IT-Abteilung

- **Umsetzung** der gesetzlichen Anforderungen
- **Anpassung** der steuerlich relevanten Systeme für Z1, Z2 und Z3
- Berücksichtigung **Datenschutz** und **IT-Sicherheit** (z.B. Zugriff durch Prüfer)
- **Protokollierung** der Datenzugriffe durch den Prüfer
- Technische **Verfahrensdokumentation** für die betroffenen Systeme
- Gewährleistung von **Aufbewahrungsfristen** & **Revisionssicherheit** (u.a.)
- **Optimierungen:** z.B. Trennung des produktiven vom archivierten Datenbestand, damit das System von kritischen Zugriffen auf produktive Daten zu Auswertungszwecken entlastet wird

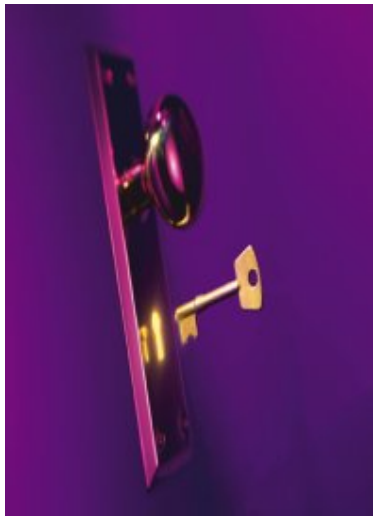
Elektronische Steuerprüfung – mögliches Phasenmodell

Operationelle Risiken im Kontext von Basel II

Menschliches Fehlverhalten

Höhere Gewalt

Vorsätzliche Handlungen



Organisatorische Mängel

Technisches Versagen

SOX – Sarbanes-Oxley Act / Auswirkungen auf die IT

- **Controlling**
  - Entwicklung/Ableitung einer IT-Strategie
  - Investitionsplanung und Überwachuung von Kosten/Nutzen
  - Nachvollziehbarkeit und Zuordnung der IT-Leistungen (Transparenz)
- **Risikomanagement und Frühwarnsystem**
  - Identifikation und Beurteilung von geschäftsgefährdenden Risiken
  - **Kontinuitätsplanung**
  - **Archivierung**
  - **Präventive Sicherheitsmaßnahmen**
  - Zeitgemäße IT-Infrastruktur (nach dem Stand der Technik)
- **internes Kontrollsystem**
  - Definierte Aufbau- und Ablauforganisation
  - **Festgelegte Rollen und Verantwortlichkeiten**
  - **Funktionstrennung und Berechtigungsmanagement**
  - **Dokumentierte Prozesslandschaft und**
  - Security Policies
  - Leistungs- und Qualitätsmanagement
  - Überwachungsmaßnahmen und interne Revision

Elektronische Steuerprüfung – mögliches Phasenmodell

Elektronische Steuerprüfung

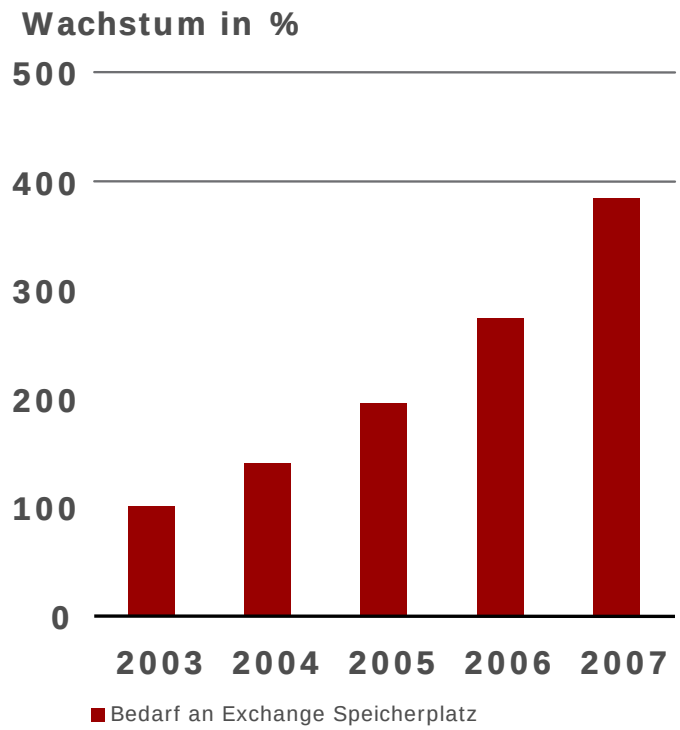
Der Kunde wird GDPdU-konform

Analyse und Strategie | **Konzeption E-Mail-Archivierung** | Realisierung

E-Mail-Archivierung

- der Bedarf wächst rasant
- die Zahl der Adressaten steigt
- die Größe der Mails steigt
- die Menge der Mails steigt

  150-250 MB p.a. pro Mitarbeiter
- die Relevanz nimmt zu
- im Ergebnis: **40 % p.a**.



Projekt-Management / Projekt-Coaching

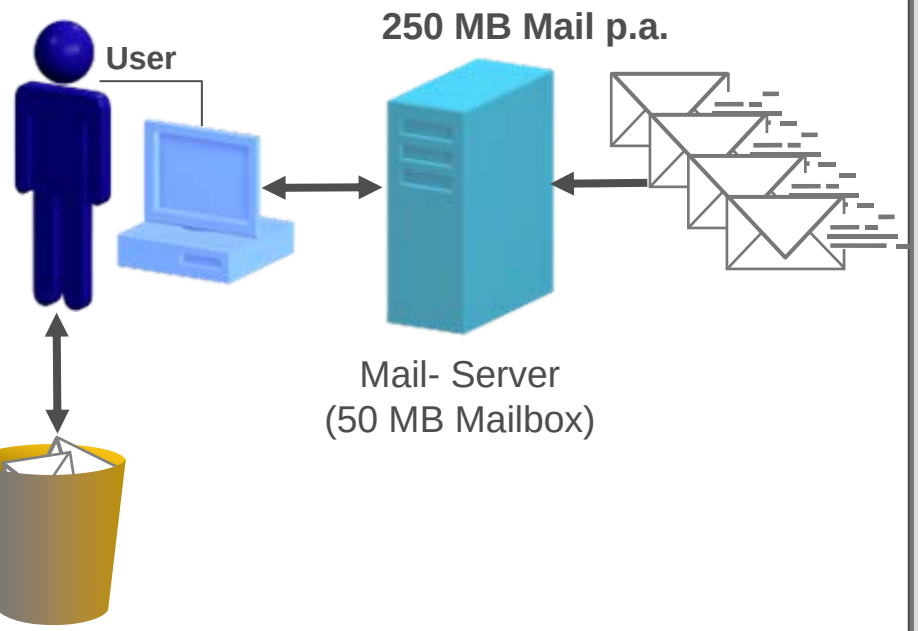
Elektronische Steuerprüfung

Der Kunde wird GDPdU-konform

Analyse und Strategie | **Konzeption E-Mail-Archivierung** | Realisierung

Löschen von E-Mails

- Freiwillig
- Zwang durch Beschränkung der Mailboxgröße
- Zwang durch Kosten-Verrechnung
- Kostet MA-Produktivität
- Verlust steuerlich relevanter Daten



Projekt-Management / Projekt-Coaching

Elektronische Steuerprüfung

Der Kunde wird GDPdU-konform

Analyse und Strategie | **Konzeption Elektr. Archivierung** | Realisierung

Vorteile der elektronischen Archivierung

- **Wegfall der Wegezeiten**: „Akte suchen & holen“ fällt weg
- **Klassisches Ablegen:** Richtigen Ordner haben, lochen, in richtige Mappe einfügen **= 30 sek**.
- **Finden:** Zum zentralen Archiv gehen, Bereich … Ordner … und Mappe finden, entweder Kopie machen und zurückstellen oder Original mitnehmen und später wieder ins Archiv gehen, einsortieren und zurückstellen **= 7 min**.
- **Mehrfachnutzung**: „Akte verliehen“ entfällt

Projekt-Management / Projekt-Coaching

Elektronische Steuerprüfung

Der Kunde wird GDPdU-konform

Analyse und Strategie | **Konzeption Elektr. Archivierung** | Realisierung

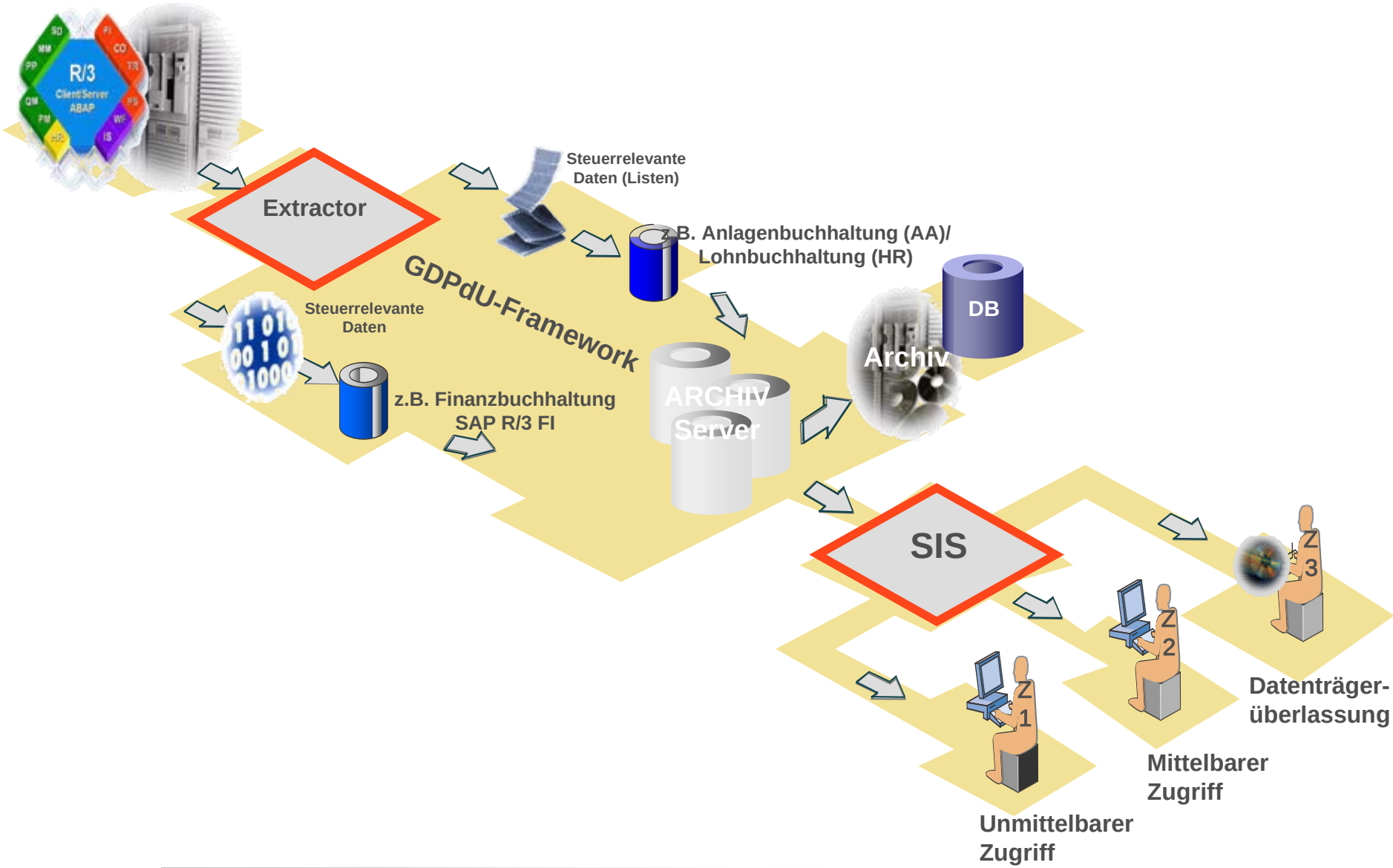
Massenspeicher:
Beispiel - Pioneer DRM-7000

- Inhalt: 720 CDs oder DVDs
- 1 CD = 36 Aktenordner Dokumente
- Ergibt 25.920 Ordner Ablage
- DVD (4,7 GB) = 260 Aktenordner
- Ergibt 187.200 Ordner Ablage
  oder 234 Meter Regal
- Maße: 43 x 65 x 152 cm (91 KG)

50er Magazin

Projekt-Management / Projekt-Coaching

Projektbeispiel – Umsetzung bei einem Finanzdienstleister



…..zum Schluss….

Compliance ist Führungsaufgabe
und Aufgabe der Unternehmensleitung

Compliance ist auch die Chance Prozesse zu optimieren

Herzlichen Dank.

Dietmar Kalkbrenner
Leiter Prozess- und Projekt-Management

arxes NCC AG
+49.221.96486-309
+49.178.61 60 -402
dietmar.kalkbrenner@arxes.de

www.arxes.de

Köln (Zentrale)
arxes NCC AG
Schanzenstraße 36
Gebäude 197
51063 Köln
0221.96486-0
0221.96486-200

Essen
arxes NCC AG
Bonsiepen 7
45136 Essen
0201.61638-0
0201.61638-10

Frankfurt
arxes NCC AG
Martin-Behaim-Straße 4
63263 Neu-Isenburg
06102.86800-0
06102.86800-60

Mannheim
arxes NCC AG
Joseph-Meyer-Str. 13-15
68167 Mannheim
0621.30980-0
0621.30980-50

München
arxes NCC AG
Bayerwaldstraße 3
81737 München
089.614540-0
089.614540-23

Berlin
arxes Berlin GmbH
Maxstraße 3a
13347 Berlin
030.46063-0
030.46063-299

Bonn
ACT AG
Rudolf-Diesel-Straße 18
53859 Niederkassel
0228.97125-0
0228.97125-40