17. Alsberg-Tagung

Anforderungen an IT-Systeme aus technischer Sicht – welche Folgen haben Verstöße insbesondere bei Durchsuchungen?

Dr. Siegfried Streitz
öffentlich bestellter und vereidigter Sachverständiger
für Systeme der Informationsverarbeitung

Streitz@Streitz.de
Pingsdorfer Str. 54, 50321 Brühl
02232/43076

16.10.2009 Berlin

STREITZ
EDV-SACHVERSTÄNDIGE

Dr. Siegfried Streitz

- Studium der Informatik, Mathematik und Betriebswirtschaftslehre
- Promotion mit den Fächern Informatik und Betriebswirtschaftslehre
- seit 1988 von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme der Informationsverarbeitung mit Schwerpunkt im kaufmännisch-administrativen Bereich
- seit 1989 selbstständig als Sachverständiger
- seit 1993 Mitglied, seit 2008 Vorstand des Deutschen EDV-Gerichtstages e.V.
- seit 1996 Mitglied des Fachgremiums Informationsverarbeitung der IHK zu Köln
- Tätigkeit an der Schnittstelle zwischen Recht, Technik und Betriebswirtschaft
- Autor zahlreicher Veröffentlichungen
- Inhaber einer führenden IT-Sachverständigenpraxis in Deutschland (derzeit acht Sachverständige, davon vier öffentlich bestellt und vereidigt)

STREITZ
EDV-SACHVERSTÄNDIGE

Übersicht

1. IT-Aspekte bei Durchsuchungen, auch nach § 103 StPO
   - Verhältnismäßigkeit
   - Datenschutzrecht
   - Steuerliche Anforderungen
2. Handakte und E-Mails
3. Diskussion

Verhältnismäßigkeit und Datenschutz

- Ziel: Eingriff möglichst gering halten (Verhältnismäßigkeit, Berufsausübungsfreiheit); insbesondere bei Banken, Rechtsanwälten, Wirtschaftsprüfern
- Annahme: Suche nach personenbezogenen Daten
- Ansatz: Inhaltsverzeichnis der Daten und Verarbeitungsabläufe
- Lösung: Anforderungen des BDSG (immer Verfahrensverzeichnis, ggf. Datenschutzbeauftragter und/oder Meldepflicht)
  neu ab 01.09.2009: verschärfte Anforderungen, zum Beispiel bei Wartungen

Unzureichende Verfahrensverzeichnisse

49 Seiten, davon 43 Seiten bis auf einzelne Begriffe identisch

1. **Verfahren:** [redacted]

Nutzung, Zweckbindung und Weitergabe personenbezogener Daten

Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung	banktechnisches Abwicklungsverfahren ❑ Kontoführung und Verwaltung banküblicher Produkte ❑ Durchführung des Zahlungsverkehrs (einschl. Multicom Webcare) ❑ Unterstützung und Absicherung unterschiedlicher Vertriebswege ❑ Darstellung des Rechnungswesens ❑ Abwicklung des Meldewesens (unter Einbezug Riskman)
Daten/Datenkategorien	❑ persönliche Daten ❑ Marketingdaten ❑ Vermögensverhältnisse ❑ Schufaauskünfte ❑ Kontendaten ▸ Kontokorrent ▸ Spareinlagen ▸ Termineinlagen ▸ Derivate ▸ Darlehen

STREITZ EDV-SACHVERSTÄNDIGE

§ 4e BDSG Inhalt der Meldepflicht

Alternativen:

- Meldepflicht und/oder
- Datenschutzbeauftragter

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle, …
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

STREITZ EDV-SACHVERSTÄNDIGE

Beschreibung

betroffener Personengruppen und diesbezüglicher Daten oder Datenkategorien - Zweck:

- Kontrollen (z. B. durch Datenschutzbeauftragten)
- Vergabe und Einhaltung von Rechten und Rollen (Zugriff, Bearbeitung, Löschen,…)
- Auskunft
- Löschen

Beispiele: Personalverwaltung, Finanzbuchhaltung

STREITZ
EDV-SACHVERSTÄNDIGE

§ 9 Technische und organisatorische Maßnahmen

Wesentlich: Anlage zu § 9

…

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. … (Weitergabekontrolle),
5. … (Eingabekontrolle),
6. … (Auftragskontrolle),
7. … (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

STREITZ
EDV-SACHVERSTÄNDIGE

Ablauf bei der Durchsuchung

1. Zur Einhaltung der Verhältnismäßigkeit zielgerichtetes Vorgehen auf Basis des Verfahrensverzeichnisses
   - in der Regel Begriff unbekannt, falls doch
   - nicht in geeigneter Form vorhanden → OWI (Opportunitätsprinzip)
2. Mündliche Erläuterung (mit stichprobenartiger Validierung) durch Datenschutzbeauftragten (muss schriftlich bestellt sein, kein Leitungspersonal, kein Anwalt) auf Basis von Tätigkeitsberichten (Einhaltung Datenschutz Durchführung von Kontrollen), aber:
   Bestellungsnotwendigkeit erst ab 10 Beschäftigten
   in der Regel nicht bestellt/nicht anwesend/nicht auskunftsfähig
3. Einhaltung Datenschutz in Frage stellen → Aufsichtsbehörde?

Ergebnis: Überblick liegt trotz gesetzlicher Regelungen nicht vor, für Durchführung muss Gesamtsystem in Augenschein genommen werden.
→ kein geringst möglicher Eingriff

Steuerliche Anforderungen

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

- beziehen sich auf steuerlich relevante Daten, hier: Handelsbriefe
- Abgrenzung Handelsbrief schwierig, in der Regel wird die Entscheidung nicht den Mitarbeitern überlassen

Fokus: per E-Mail empfangene Handelsbriefe

Die originär digitalen Unterlagen dürfen nicht ausschließlich in ausgedruckter Form oder auf Mikrofilm aufbewahrt werden.

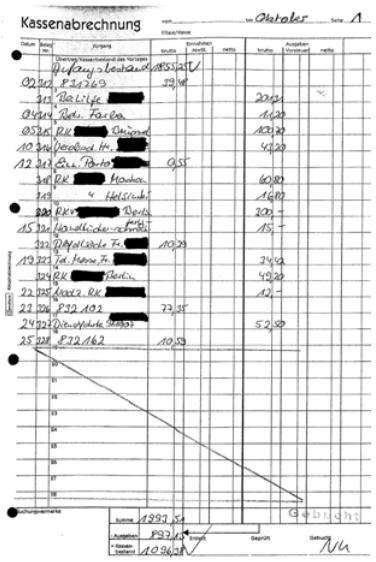
→ Was ist der Hintergrund dieser Anforderung?

Begriff der *Ordnungsmäßigkeit*

- Ordnungsmäßigkeit der Datenverarbeitung bedeutet: Sicherstellung der Verfügbarkeit, Integrität und Kontrollierbarkeit der Datenverarbeitungsprozesse einschließlich der Daten in diesen Prozessen
- wesentliche Komponente: organisatorische Regelung
- im kaufmännisch-administrativem Bereich:
  - Grundsätze ordnungsmäßiger Buchführung (GoB)
  - Grundsätze ordnungsmäßiger Buchführungssysteme (GoBS)
- Beispielhafte Erläuterung:
  - Papierdokumentation
  - Übergang zu IT-gestützten Verfahren
  - Resultierende Anforderungen

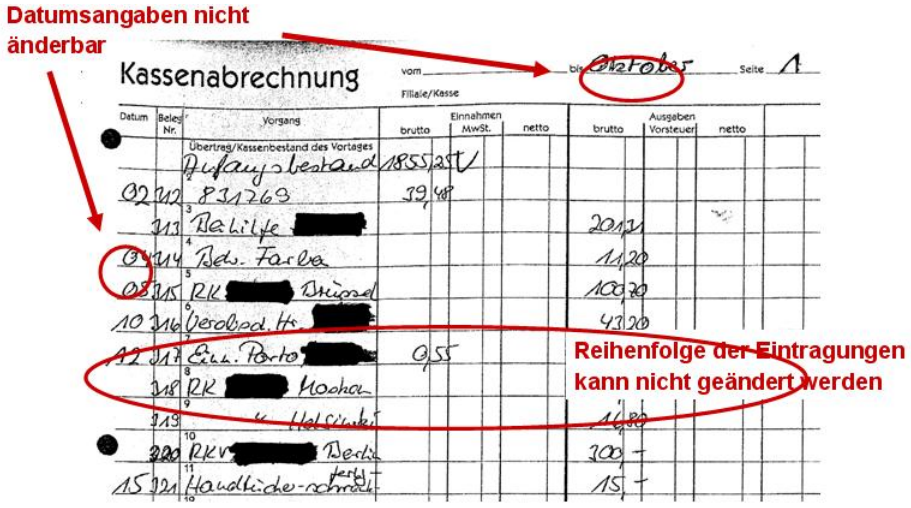
STREITZ
EDV-SACHVERSTÄNDIGE

Kassenbuch



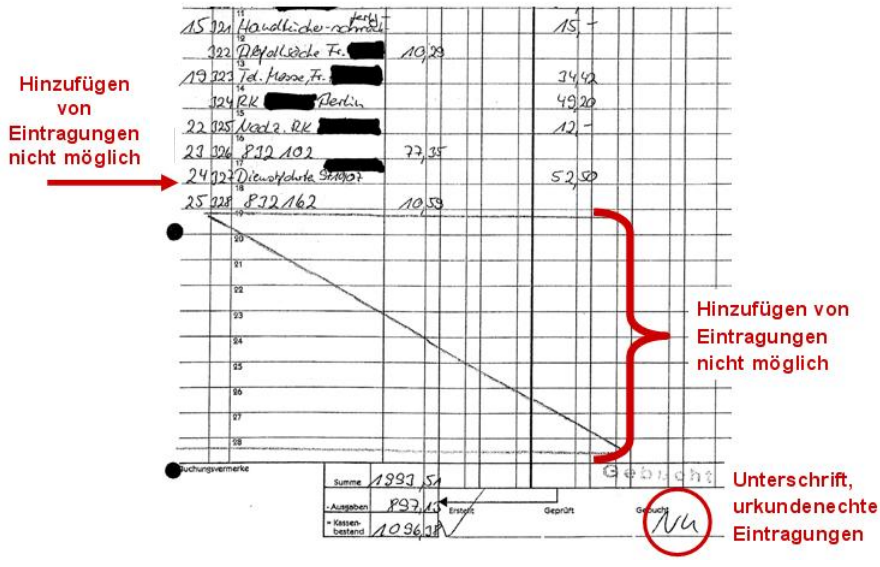
STREITZ
EDV-SACHVERSTÄNDIGE

Aussagekraft I



STREITZ EDV-SACHVERSTÄNDIGE

Aussagekraft II



STREITZ EDV-SACHVERSTÄNDIGE

IT-gestütztes Verfahren I

Seite 1 zum Kassenbuch für Juli 2007 **Datum?**

Datum		Eingangsbe-trag	Ausgangs-betrag
	Bestand	**20,94**	0,00
02	Einlage	430,00	0,00
02	Postwertzeichen v. 14.06.	0,00	9,00
02	Postwertzeichen v. 05.06.	0,00	4,80
02	Postwertzeichen	0,00	3,90
02	Mercure Hotel v. 05.06.	0,00	104,00
05	Benzin	0,00	6,00
06	Benzin	0,00	65,00
06	Metro, Getränke, Reinigungsmittel	0,00	35,68
10	Postwertzeichen	0,00	

Einfügen möglich

Datum ändern möglich

Betrag ändern möglich

Unterschrift?

STREITZ EDV-SACHVERSTÄNDIGE

IT-gestütztes Verfahren II

Seite 1 zum Kassenbuch für Juli 2007

Datum		Eingangsbe-trag	Ausgangs-betrag
	Bestand	**20,94**	0,00
02	Einlage	430,00	0,00
02	Postwertzeichen v. 14.06.	0,00	9,00
02	Postwertzeichen v. 05.06.	0,00	4,80
02	Postwertzeichen	0,00	55,00
02	Mercure Hotel v. 05.06.	0,00	104,00
04	Bewirtung am 01.07.	0,00	115,00
05	Benzin	0,00	6,00
06	Benzin	0,00	65,00
16	Metro, Getränke, Reinigungsmittel	0,00	35,68

Einfügen möglich

Datum ändern möglich

Betrag ändern möglich

STREITZ EDV-SACHVERSTÄNDIGE

IT-gestütztes Verfahren III

Seite 1 zum Kassenbuch für Juli 2007

Datum		Eingangsbe-trag	Ausgangs-betrag
	Bestand	**20,94**	0,00
02	Einlage	430,00	0,00
02	Postwertzeichen v. 14.06.	0,00	9,00
06	Benzin	0,00	65,00
16	Metro, Getränke, Reinigungsmittel	0,00	35,68
10	Postwertzeichen	0,00	3,90
12	Postwertzeichen	0,00	3,90
23	Benzin	0,00	68,02
25	Parkgebühr	0,00	12,00

Einträge gelöscht

STREITZ EDV-SACHVERSTÄNDIGE

IT-gestütztes Verfahren IV

Seite 1 zum Kassenbuch für Juli 2007

Datum		Eingangsbe-trag	Ausgangs-betrag
	Bestand	**20,94**	0,00
02	Einlage	430,00	0,00
02	Postwertzeichen v. 14.06.	0,00	9,00
02	Postwertzeichen v. 05.06.	0,00	4,80
02	Postwertzeichen	0,00	3,90
02	Mercure Hotel v. 05.06.	0,00	94,00
05	Benzin	0,00	16,00
06	Benzin	0,00	65,00
06	Metro, Getränke, Reinigungsmittel	0,00	35,68
10	Postwertzeichen	0,00	3,90

Beträge verändert

STREITZ EDV-SACHVERSTÄNDIGE

Zusammenfassung Papierdokumentation

- Organisatorische Trennung Eingabe, Verarbeitung, Ausgabe
- Bindung der Information an physikalische Materialien, die ohne weitere technische Hilfsmittel erfasst werden können
- Identifikationsmöglichkeit des Autors durch Handschrift
- Reihenfolge von Eintragungen eindeutig
- Kennzeichnung von Zwischenräumen (Vakatzeichen/ Buchhalternase)
- Möglichkeit gebundener Bücher
- Urkundenechte Aufzeichnungsverfahren möglich
- Altersbestimmung durch analytische Methoden möglich

STREITZ
EDV-SACHVERSTÄNDIGE

Zusammenfassung IT-gestützte Verfahren

- Keine organisatorische Trennung von Eingabe, Verarbeitung, Ausgabe
- Keine Bindung der Informationen an physikalische Materialen, die ohne weitere technische Hilfsmittel erfasst werden können
- Keine Identifikationsmöglichkeit des Autors
- Keine Reihenfolge der Eintragungen
- Keine Kennzeichnung von Zwischenräumen
- Beliebige Modifikationsmöglichkeiten
- Keine Altersbestimmung durch analytische Methoden

Sofern nicht geeignete technische und organisatorische Maßnahmen getroffen werden

STREITZ
EDV-SACHVERSTÄNDIGE

Zusätzliche IT-Anforderungen

- Identifikation (Ausweisen des Benutzers gegenüber der IT)
- Authentisierung (Bestätigung der Identifikation)
- Integrität der Daten (keine unprotokollierte Veränderung, keine Löschung)
- Weitere technische Vorkehrungen zur Sicherstellung der Datenintegrität durch Wahl geeigneter nur einmal beschreibbarer Datenträger, Prüfsummenkonzept, Verschlüsselungsmechanismus etc.
- Validierung von Zeitpunkten (Anlegen, Modifizieren, Löschen)
- Protokollierung (Dokumentation wichtiger Bearbeitungsschritte) wie Anmeldung eines Benutzers, Speicherung einer bestimmten Information oder Abschluss eines Vorgangs
- Prüfbarkeit (betrifft organisatorische Anforderungen wie Zulässigkeit von Verarbeitungsläufen) und das Verfahren an sich (beispielsweise Verhinderung von unerlaubten Verarbeitungen)
- Richtigkeit (impliziert Vollständigkeit)

Anforderungen zu E-Mails

Folgerung aus Ordnungsmäßigkeit: → geordnete Ablage notwendig

- E-Mail-/Dokumenten-Managementsystem (DMS)
- Ordnerstruktur
- Archivierungsfunktionalität
  - Einhaltung von (Aufbewahrungs-)Fristen
  - Manipulationssicherheit

Handakte und E-Mails

Papier:

- Trennung beschlagnahmefreier Unterlagen (wie Handakte des Verteidigers)

Rechner:

- Häufig keine Struktur vorhanden
- Suchfunktionalität spärlich (in der Regel nur in einem Postfach, ggf. hohe Trefferzahl, hoher Zeitaufwand)
- Manuelle Durchsicht aufgrund Datenmenge vor Ort nicht durchführbar

→ Eingrenzung vor Ort nicht möglich

→ Mitnahme aller E-Mails zwingende Folge des nachlässigen Umgangs

→ Verletzung des Mandatsgeheimnis

Auswertungsmöglichkeiten

Zusammenführung aller Daten

- Extraktion E-Mails
- Volltextindizierung (Unterstützung vieler Formate)
- Einfache Suche („Google auf Datenbestand“)
- Individuell am Arbeitsplatz nutzbar (Festplatte an USB)

→ Vollständigkeit der Sichtung

→ jederzeitige Verfügbarkeit

Ende

Vielen Dank für Ihre Aufmerksamkeit!