«VOI»

TeleTrusT
Pioneers in IT security.

Informationstag "Elektronische Signatur"

Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 14.09.2012

Rechtliche Aspekte der Cloud-Archivierung

Ulrich Emmert

esb Rechtsanwälte / VOI e.V.

Informationssicherheit
Datenschutz
Telekommunikationsrecht
Haftungsrecht / AGB
Lizenzverträge
Kapitalgesellschaftsrecht

Ulrich Emmert

Partner der Sozietät
esb Rechtsanwälte
Lehrbeauftragter für
Wettbewerbs-, Urheber-
und Onlinerecht an der
Hochschule für Wirtschaft
und Umwelt in Nürtingen
Vorstand der Reviscan AG
Vorstand des VOI e.V.

Schockenriedstr. 8A
70565 Stuttgart
Tel. 0711/469058-0
Fax 0711/469058-99

ulrich.emmert@kanzlei.de
www.kanzlei.de
www.esb-rechtsanwaelte.de
www.emmert.de

esb Referenzen

e|s|b Rechtsanwälte

Schadensfälle

- **Nichtverfügbarkeit von Emails und Beweislastumkehr wegen Nichtvorlage elektronischer Geschäftspost**
  - ERP-Projekt Universitäten Stuttgart, Heidelberg
    - Verstoß gegen HGB und kaufmännische Sorgfaltspflicht, Nichtverfügbarkeit beweiserheblicher Mailkorrespondenz
    - Organisationsverschulden: Leiter des Hoheitsträgers Universität v. CEO Germany des ERP-Softwareanbieters
- **Auffindbarkeit nicht aufbewahrungspflichtiger Informationen (interne Mails)**
  - Beweisbarkeit eines Verstoßes gegen EU-Kartellrecht
  - Strafe der EU-Kommission 80 Mio. €

Strafvorschriften

- §283 b Strafgesetzbuch: Verletzung der Aufbewahrungspflicht, z.B. durch Mailquota ohne Archivierungsmöglichkeit
- § 203 Verletzung von Privatgeheimnissen
- § 133 StGB Verwahrungsbruch: z.B. durch Mailquota im öffentlichen Dienst
- § 274 StGB Urkundeunterdrückung
- § 206 Bruch des Fernmeldegeheimnisses bei Postfachkontrolle
- § 201 StGB Verletzung der Vertraulichkeit des Wortes bei UMS/VoIP-Anrufbeantworter
- § 201a StGB Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen bei Postfachkontrolle
- § 44 BDSG vorsätzliche Datenschutzverletzung in Bereicherungs- oder Schädigungsabsicht

Aufbewahrungspflichten

e|s|b Rechtsanwälte

- Aufbewahrungspflichten nach § 257 HGB und § 147 AO für geschäftliche Korrespondenz inkl. geschäftliche E-Mails
- Aufbewahrung von elektronisch verfügbaren Dokumenten elektronisch nach GoBS/GDPdU
- Aufbewahrung von eingehenden Papierdokumenten auf Papier oder bei Wahrung der Beweissicherheit auch elektronisch zulässig

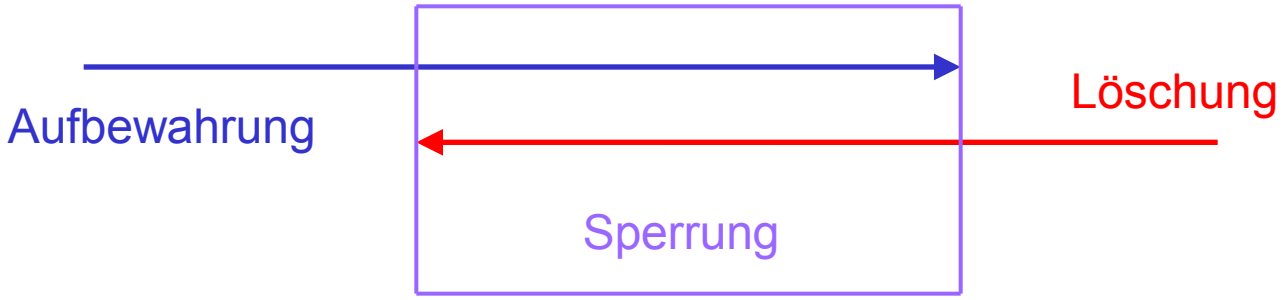
Abgrenzungsproblem HGB/AO und 6/10 Jahre

(P) Buchungsunterlagen/Handelsbriefe

- E-Mails ./. steuerrelevante Unterlagen
  - Belegfunktion?
- 6 Jahre ./. 10 Jahre, GDPdU-Konformität
  - Originäre Aufgabe von WP und StB
  - Automatisiert kaum möglich
  - Individuelle Prüfung unsicher und teuer
- revisions- und fälschungssicher lese- und auswertbar

Speicherung contra Datenschutz

- Bei datenschutzrechtlichen Löschungsverpflichtungen tritt an die Stelle der Löschung die Sperrung
- Nach Ende der Sperrfrist sind die Daten zu löschen!
- Bei Einschaltung eines Dienstleisters zur Archivierung tritt bei vertraglichen Vereinbarungen keine Löschpflicht ein



Vorschriften zur Prüfung der IT-Compliance

- Gewährleistung von Transparenz, Revisions- und Datensicherheit
- Durch Handelsgesetzbuch HGB und Abgabenordnung AO in Verbindung mit:
  - GOBS 1995
    - Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (alle Buchungspflichtigen!); abgeleitet aus HGB-Vorgaben der Ordnung, Nachvollziehbarkeit und Unverfälschbarkeit
  - GDPdU 2002
    - Grundsätze zum Datenzugriff und zur Prüfbarkeit originär digitaler Unterlagen (alle Buchungspflichtigen!); Entstehung im Zuge der AO-Änderung 2001

Aufbewahrung *nach* HGB (GoBS)

Digitale Archivierung nach § 257 Handelsgesetzbuch

- GoBS-Konformität (Auffindbarkeit, Index, Sicherheit, Vertraulichkeit)
- Sicherstellung, dass Daten
  - mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich
  - mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden
  - während der Aufbewahrungsfrist verfügbar sind
  - jederzeit innerhalb angemessener Frist lesbar gemacht können

Anforderungen Steuerrecht

- §§ 146 ff. Abgabenordnung
  - GDPdU:
  - maschinelle Auswertbarkeit,
  - revisionssichere Aufbewahrung
  - Verfügbarkeit
  - 6/10 Jahre ab Jahresende
  - Angabe des Speicherortes
  - Speicherort innerhalb Deutschlands oder Amtshilfe nachgewiesen

Aufbewahrung nach AO

Folge: Aufbewahrung (auch) nach § 147 AO, GoBS und **GDPdU**

- ***Bildliche*** *Übereinstimmung mit den empfangenen Handels-/Geschäftsbriefen und den Buchungsbelegen wenn lesbar gemacht*
- *GOBS: unveränderbarer Index, unter dem die Mail verwaltet und bearbeitet werden kann*
- *GdPDU: maschinelle Auswertbarkeit über mindestens 10 Jahre*
- *D.h. wahlfreier Zugriff über den nach GOBS nötigen Index auf die im Originalformat zu archivierende Email*

Archivierung öffentlicher Dienst

- Grundsätze ordnungsgemäßer Aufbewahrung sind ungeschriebenes Verwaltungsrecht nach Art. 33 GG
- Verweise darauf an vielen Stellen, z. B. SGB
- Archivierung z.T. verstreut geregelt in
  - Informationsfreiheitsgesetz
  - Bundes-/Landesarchivierungsgesetz
  - Runderlassen
  - HH-Ordnungen
  - Verwaltungsvorschriften
  - Richtlinien, Vereinbarungen mit Personalrat
- z.T. Pflicht zur Aufbewahrung von Unterlagen nach Maßgabe der handelsrechtlichen Vorschriften (§ 257 HGB) und Steuerrichtlinien (GOB, GOBS, GDPdU) ...

§ 35 SRVwV Verwaltungsvorschrift über das Rechnungswesen

- Die Jahresrechnung, das Zeitbuch und das Sachbuch mit ihren Tagesnachweisungen, Sammelnachweisungen und Vorbüchern sowie das Beitragsbuch sind mindestens 10 Jahre, die sonstigen Bücher, die Belege, die Nachweise über das Bestehen einer Familienversicherung und die Niederschriften über die Prüfungen der Kasse sowie die Bescheinigungen über die Tages- und Monatsabstimmung sind mindestens sechs Jahre aufzubewahren. Die Aufbewahrungsfrist beginnt mit dem Ende des Geschäftsjahres, auf das sich die in Satz 1 genannten Unterlagen beziehen.

SRVwV Verwaltungsvorschrift über das Rechnungswesen

- § 36 Aufbewahrung
- Eine Vernichtung von Unterlagen sowie der Verzicht auf die Ausfertigung einer schriftlichen Unterlage nach §§ 110a bis 110d des Vierten Buches Sozialgesetzbuch sind unzulässig, wenn die Unterlagen für andere als Buchführungszwecke in Papierform aufzubewahren sind.

§ 40 SRVwV Datensicherheit

e|s|b Rechtsanwälte

(1) Automatisierte Verfahren sind durch besondere technische und organisatorische Maßnahmen vor unbemerkter und unberechtigter Veränderung zu schützen.

(2) Die zur Sicherheit der Verfahren zu erlassende Dienstanweisung (§ 17 der Sozialversicherungs-Rechnungsverordnung) muss die in der Anlage zu § 78 a des Zehnten Buches Sozialgesetzbuch erforderlichen technischen und organisatorischen Maßnahmen regeln sowie die Einzelheiten qualifizierter elektronischer Signaturen nach dem Signaturgesetz.

(3) Darüber hinaus hat die Dienstanweisung Einzelheiten zu enthalten über

1. die Abgrenzung von Verantwortungsbereichen im Bereich der automatisierten Datenverarbeitung,
2. Vorkehrungen für die Sicherheit bei der Datenfernübertragung und digitaler Aufzeichnung,
3. Datenträger und Datenformat,
4. Regelungen zu maximalen Zugriffszeiten auf Dateien, Wiederauffrischen der Daten und Berücksichtigung von technischen Veränderungen (Verfügbarkeitsanforderungen),
5. Dokumentation zu Art und Umfang der Archivierung,
6. und bei elektronischer Archivierung über die zusätzlich zu den Belegen zu archivierenden Angaben (insbesondere Namen des Archivierenden und Zeitpunkt der Archivierung)

(4) Einzelheiten von Verfahrensänderungen und neu eingeführter Verfahren sind entsprechend der Anlage 9 zu dokumentieren.

§ 41 SRVwV Elektronische Signatur

e|s|b Rechtsanwälte

(1) Soweit nach dieser Verwaltungsvorschrift eine Unterschrift verlangt wird, kann diese durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz geleistet werden. Ausgenommen ist die in § 4 Abs. 5 vereinbarte Doppelzeichnung; hier kann anstelle der qualifizierten elektronischen Signatur auch eine fortgeschrittene elektronische Signatur nach dem Signaturgesetz zur Anwendung kommen, wenn diese eine hinreichende Sicherheit gewährleistet.

(2) Das qualifizierte Zertifikat muss die ausschließliche Anwendung zu dienstlichen Zwecken vorsehen; Ausnahmen sind in einer Dienstanweisung zu regeln. Die Verwendung eines Pseudonyms nach § 5 Abs. 3 des Signaturgesetzes ist ausgeschlossen.

(3) Wird die Unterschriftsberechtigung entzogen oder geändert, so ist unverzüglich eine Sperrung des betreffenden Zertifikats zu veranlassen.

(4) Bei elektronisch signierten Daten ist vor einer weiteren Verarbeitung die qualifizierte elektronische Signatur und anhand des betreffenden Zertifikats die Unterschriftsberechtigung zu prüfen.

(5) Bei der automatischen Erzeugung von Signaturen (Massensignaturen) muss sichergestellt sein, dass die Gültigkeit der qualifizierten elektronischen Signatur stichprobenartig überprüft wird. Näheres ist in einer Dienstanweisung (§ 40) zu regeln.

Papierloses Büro – was darf digitalisiert werden?

- Grundsatz der Formfreiheit
  - In der Regel existieren weder ausdrückliche Verbote hinsichtlich der Daten, die ein Unternehmen digitalisieren will.
  - Die Aufbewahrungsvorschriften schreiben meist keine bestimmte Form vor.
  - In diesem Fall ist von der Zulässigkeit der Digitalisierung und ausschließlichen elektronischen Aufbewahrung auszugehen.
  - Hinsichtlich der Form der Aufbewahrung ist auf die allgemeinen technisch-organisatorischen Regeln (s.o.) und die Datensicherheit zu verweisen.
  - Wird Schriftform der Aufbewahrung vorgeschrieben, kann diese in der Regel durch die elektronische Form mit qualifizierter Signatur ersetzt werden

Gesetzliche und vertragliche Schriftform

e|s|b Rechtsanwälte

- Nur bei gesetzlicher Schriftform sind Unterschrift auf Papier oder qualifizierte elektronische Signatur erforderlich
- Bei vertraglicher Schriftform ist ausreichend, dass nach § 127 BGB der Aussteller des Dokuments und das Ende des Dokuments kenntlich gemacht sind, es reicht telekommunikative Übermittlung
- Auch die vertragliche Schriftform kann durch die vertragliche elektronische Form ersetzt werden.
- Das kann auch z.B. durch Unterschriften auf Tablets oder Smartphones erreicht werden.

Besondere Beweisvorschriften

- § 416 ZPO Privaturkunde kann durch qualifizierte Signatur weitgehend beweiswerterhaltend digitalisiert werden (Verfahrensbeschreibung erforderlich)
- § 437 ZPO Öffentl. Urkunde birgt auch Vermutung der Richtigkeit
- § 371a ZPO die §§ 416 und 437 ZPO sind auf elektronische Dokumente bei Verwendung elektronischer Signaturen entsprechend anwendbar
- Erschütterung der Beweiskraft ist möglich, wenn durch Tatsachen ernstliche Zweifel am Aussteller bestehen

Höhere Beweiskraft

- Öffentliche Beglaubigung nach § 129 BGB
  - Beglaubigung ist auch elektronisch möglich, aber keine nachträgliche Archivierung in digitaler Weise mit gleicher Beweiskraft
- Notarielle Beurkundung nach § 128 BGB
  - Beweiskraft für die beurkundete Tatsache, kann nicht auf elektronischem Wert erreicht werden
- Titel nach § 794 ZPO können auch nicht mit gleicher Beweiskraft archiviert werden

Scannen

- Geltung der GOBS
- vollständige und richtige Übernahme
- GOBS (VIII b Nr. 1) verlangt Anweisung:
  - wer scannen darf,
  - zu welchem Zeitpunkt gescannt wird,
  - ob eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich ist,
  - wie die Qualitätskontrolle auf Vollständigkeit und
  - wie die Protokollierung von Fehlern zu erfolgen hat.

Ersetzendes Scannen nach TR-Entwurf TR-RESISCAN

- Risikoanalyse
- Klassifizierung von Dokumenten
- Schutzbedarfsfeststellung
- Verfahrensdokumentation
- Erforderlichkeit des Scannens nach Datenschutzrecht
- Spezialgesetzliche Anforderungen an Datenschutz und Geheimhaltung (z.B. § 30 AO oder LBG)
- Besondere Beachtung von Urkunden und Titeln bzw. Nachweis der Dokumentenverbindung

Scannen und Beweisrecht

e|s|b Rechtsanwälte

- Verlust der Urkundenqualität
  - Titel, Verträge, Bescheide etc ausnehmen?
  - Titel im Original verwahren
  - Verträge, Bescheide: elektronische Signatur und GoBS
- Augenscheinsobjekt / freie richterliche Beweiswürdigung
- Datenschutzrechtliche Löschungspflicht nach Ende der Aufbewahrungsfristen
  - Ausnahme: berechtigtes Interesse, insbes. an Beweissicherung
  - Setzt hinreichend konkretes Eskalationsrisiko voraus

Beweisqualität von Dokumenten

- Beweiskraft stark eingeschränkt durch leichte Fälschbarkeit und Löschbarkeit
- Erhöhung der Beweiskraft durch
  - Digitale Signaturen
  - Verkettete Hashwerte und digitale Zeitstempel
  - Read-Only-Datenträger oder zertifizierte WORM-Systeme wie Netapp Snaplock oder EMC Centera
- Sperrung der Daten bis zum Ende der Aufbewahrungsfrist gegen Löschung
- Verlängerung der Aufbewahrungsfrist möglich
- Indizierung möglich
- Bildung von Hashwertketten über ganze Datenträger
- Zeitstempel auf Hashwerte gegen nachträgliche Manipulation

Archivierung nach TR-ESOR

- Richtlinie des BSI zur revisionssicheren Archivierung kryptographisch gesicherter Dokumente TR 03125
- Sicherung der Datensätze ggf. durch qualifizierte Signatur
- zeitliche Sicherung durch Erstellung von Hashbäumen und qualifizierte externe Signatur mit einem Zeitstempel zur Integritätssicherung
- Ermittlung veränderter Dokumente durch Hashbaumanalyse

TR-ESOR

- Verbindlich für Langzeitarchivierung von Bundesbehörden
- Keine Allgemeinverbindlichkeit (VOI)
- Langzeitsicherung von Daten mit elektronischen Signaturen
- Verfahren der Nachsignatur bei Kompromittierung von Hashwert bzw. Signaturalgorithmus
- Beweisbarkeit der Sicherheit jedes einzelnen Datensatzes durch Evidence Record

Vorteile Cloud-Archivierung

- Automatisierbare Konvertierung von Dokumenten
- Einmaliger Aufbau einer Infrastruktur zur
  - Verarbeitung und Prüfung von Elektronischen Signaturen
  - Prüfung von Beweiswerten einzelner Dokumente
  - Volltextsuche auch in eingescannten und signierten Dokumenten
  - Konvertierung in Langzeitarchivformate
  - Verwendung von hochkomprimierenden Speicherverfahren zur Kosteneinsparung

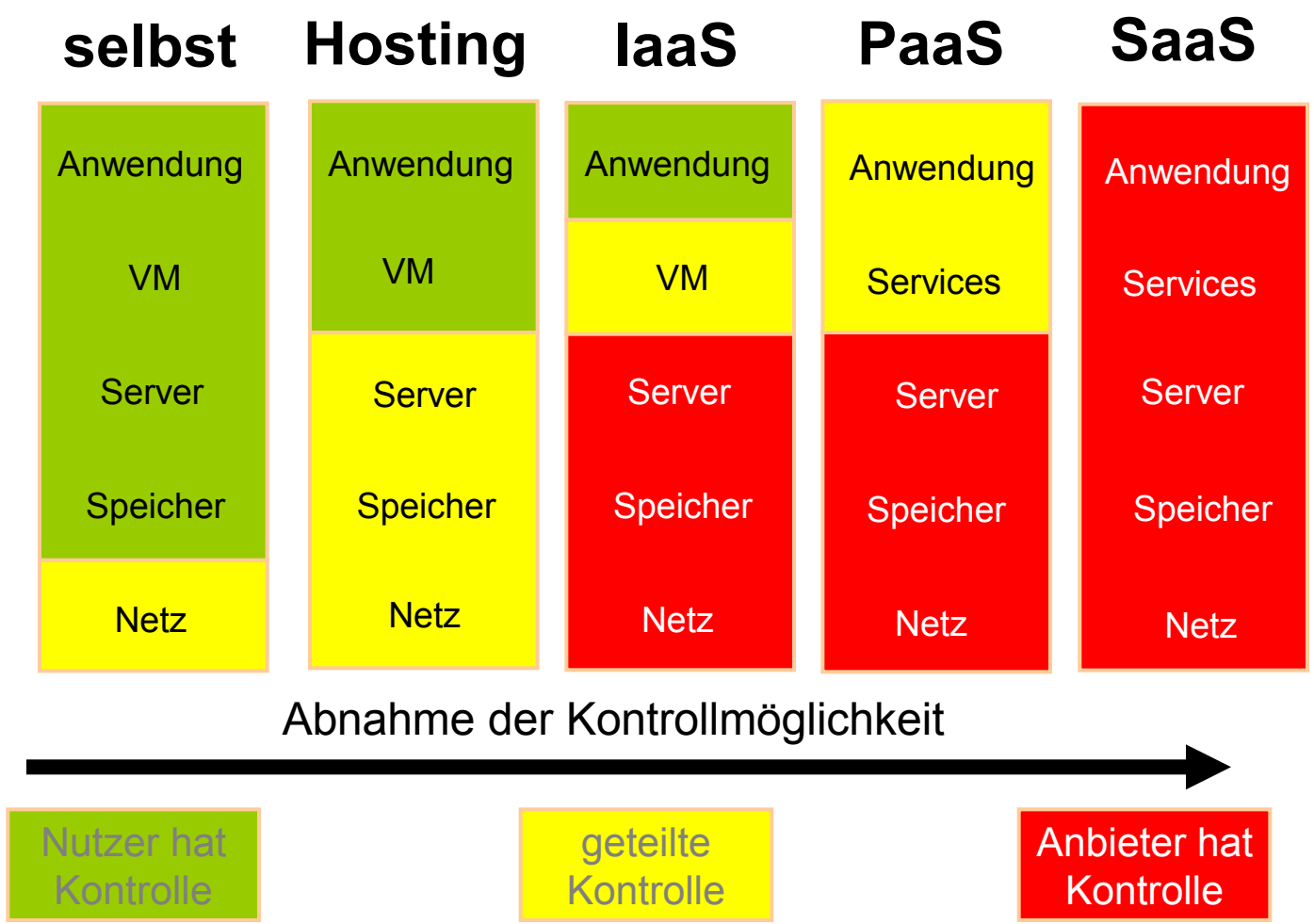
Vorteile Cloud Archivierung

- Verwendung von teuren Pseudo-WORM Speichern nur zur Verhinderung von Datenverlusten möglich, aber nicht zur Erhöhung des Beweiswertes erforderlich
- Höherer Beweiswert durch Verkettung von Hashwerten auch mit fremden Dokumenten, daher keine nachträgliche eigene Nacherstellung eines Tagesarchivs möglich
- Keine eigenen Zeitstempelanfragen erforderlich

Cloud Archivierung und Datenschutz

- Zentrale Speicherung möglich
- Täglicher Download des Archivs auf eigene Speichermedien und Löschung im zentralen Archiv möglich
- Hashwerte müssen vollständig auf zentralem System gespeichert sein, lassen aber keinen Rückschluss auf Dokumente zu
- Verschlüsselte Speicherung auf zentralem System mit eigenem Schlüssel möglich
- Durch Dienstleister können vertragliche Aufbewahrungsfristen definiert werden, so dass nicht gegen Löschungspflichten verstoßen wird

Kontrolle in der Cloud

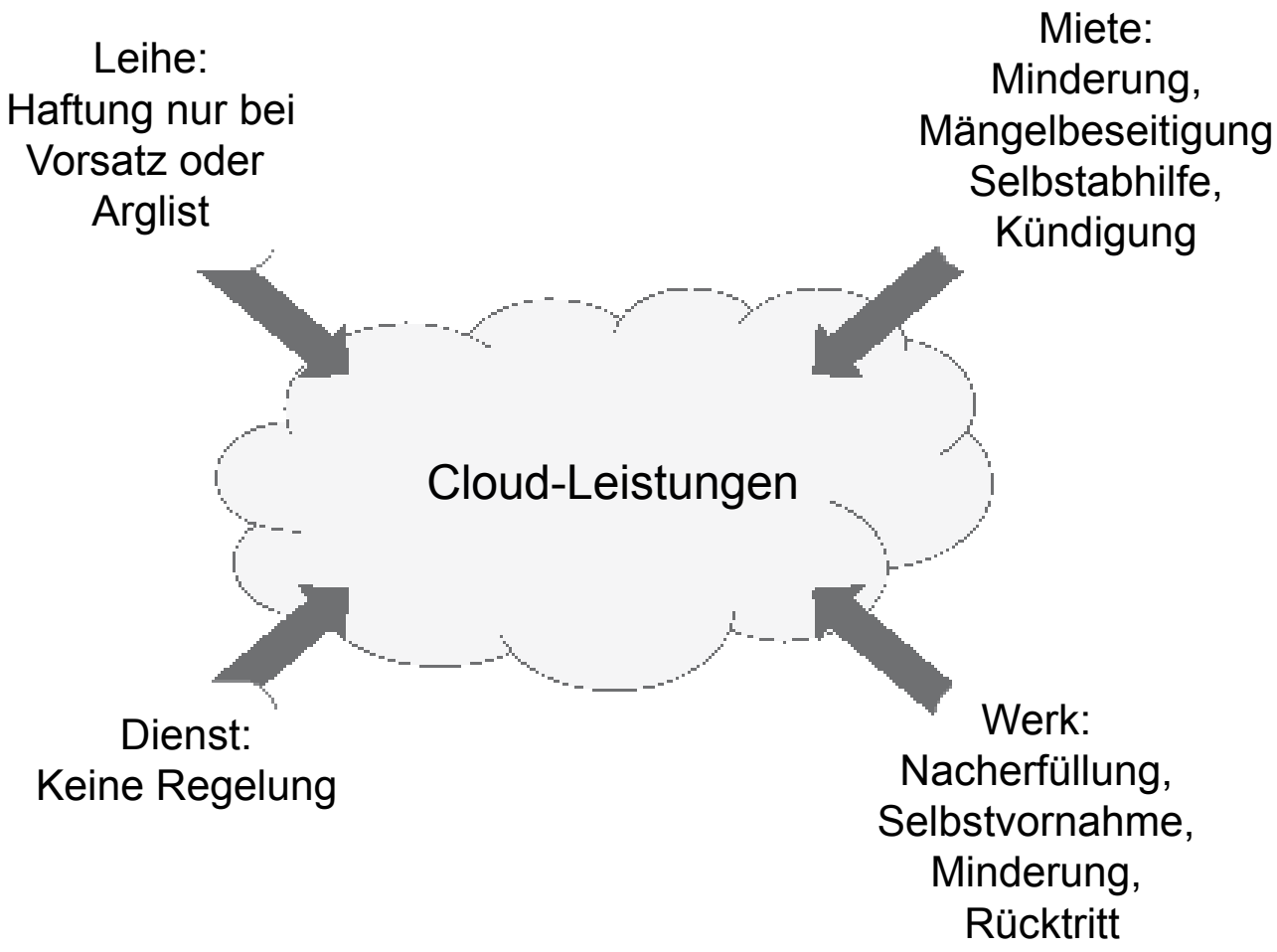


Quelle: Tim Mather „Cloud Security and Privacy“

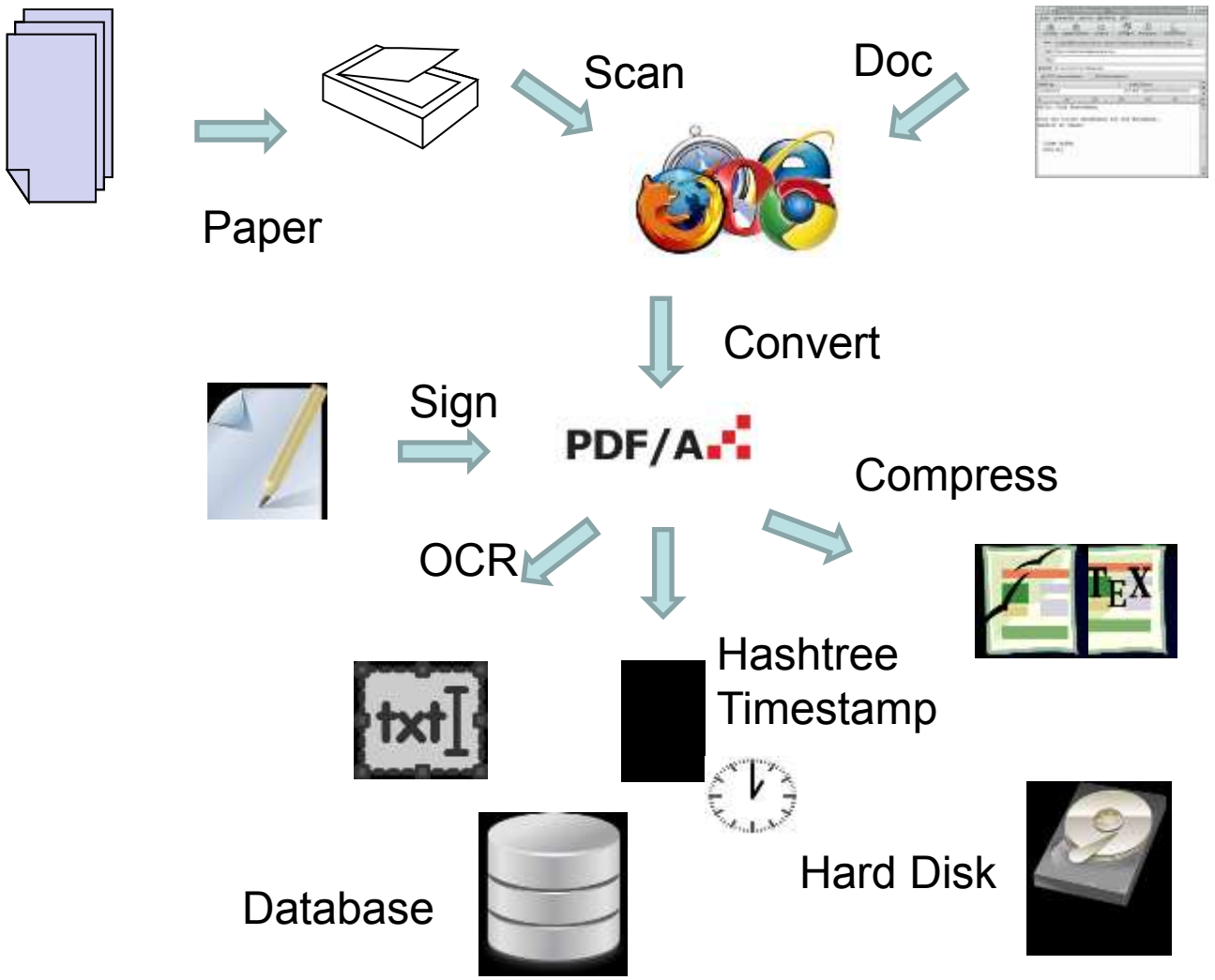
Vertragstypen

	Mietvertrag (ohne Entg. Leihe)	Dienstvertrag	Werkvertrag
SaaS	Zugriff auf ASP	Überwachungs- und Betriebs-leistungen	-
PaaS	Bereitstellung von Zugriff und Speicherplatz	Überwachungs- und Betriebs-leistungen	BGH: Abrufbarkeit bei Webhosting
IaaS			

Gesetzliche Gewährleistung



Beispiel Reviscan Archiv



Dienstleistungen esb Rechtsanwälte – www.kanzlei.de

Schulungen
- Internet-Sicherheit
- Datenschutz
- Urheberrecht

Workshops
- Security Policies
- Nutzungsbedingungen
- Haftungsklauseln
- Einführung von PKI-Systemen
- Datenschutz- und Datensicherheitskonzepte
- E-Mail Archivierungslösungen

Beratung
- Internet-Sicherheit
- Datenschutz
- AGB
- Vertragsgestaltung, z.B. Lizenzverträge, ASP-, Outsourcing-, Hosting-, Wartungs-Verträge
- Existenzgründungsberatung
- Business Pläne

Auditing
- Security Policies
- IT Risk Management
- Datenschutzaudit
- Datenschutzbeauftragter