



# **DMS heute und morgen : Unternehmenskritische Daten in der Cloud**

**Ulrich Emmert  
esb Rechtsanwälte**



**Ulrich Emmert**

Rechtsanwalt  
Lehrbeauftragter für  
Wettbewerbs-, Urheber-  
und Onlinerecht an der  
Hochschule für Wirtschaft  
und Umwelt in Nürtingen

Informationssicherheit  
Datenschutz  
Haftungsrecht / AGB  
Lizenzverträge  
Unternehmensverkäufe  
Kleine AG  
Umwandlung  
Existenzgründungsberatung  
Erstellung von Business Plänen

Vaihinger Str. 153  
70567 Stuttgart  
Tel. 0711/469058-0  
Fax 0711/469058-99

[ulrich.emmert@kanzlei.de](mailto:ulrich.emmert@kanzlei.de)  
[www.kanzlei.de](http://www.kanzlei.de)  
[www.esb-rechtsanwaelte.de](http://www.esb-rechtsanwaelte.de)  
[www.emmert.de](http://www.emmert.de)

## Referenzen



SIEMENS



EMC<sup>2</sup>  
where information lives<sup>®</sup>



FUJITSU

EnBW



DIHK

Bundeswehr



*Ohne Feind im Gesicht*

Roland Berger  
Strategy Consultants



DEKRA



Deka  
Investmentfonds



nextiraOne

ALCATEL





## Vorteile Cloud-Computing (1)

- Nutzer kann auf Daten von überall zugreifen ohne komplexe SW-Installation und regelmäßige Anschaffung leistungsfähigerer HW
- Informationen, die Nutzer zur Verfügung haben muss, werden nicht mehr lokal oder im Intranet abgelegt sondern auf Zentralservern im Internet
- Auch ganze Programme können so via Fernzugriff genutzt werden:
  - Werden einfach im Browser ausgeführt und nehmen Arbeitsplatz-PC insbes. die oft zum HW-Austausch führende, zeitaufwändige Rechenleistung ab
  - Oft entfallen auch lästige Updates



## Vorteile Cloud-Computing (2)

- Notwendigkeit für eine lokale IT (Server, Netzwerk- und Datenbanksoftware etc.) entfällt.
  - Unternehmen können durch den Wegfall von Rechenzentren Fläche, Wartungsleistungen, HW-/SW-Kosten sowie Strom- und Kühlungskosten einsparen.
  - Cloud-Server-Farmen rechnen zudem nur tatsächliche Zugriffe, d.h. wirklich in Anspruch genommene Serverleistung, ab.
- Unternehmen können
  - Investitionskosten pro Anwendung durchschnittlich um min. 50%
  - Betriebskosten (Personal) sogar um 60% senken.



## Rechtliche Fallstricke

- Intransparente, technologisch nicht klar bestimmbare **Übermittlung von Daten über Grenzen hinweg** und deren **Aufbewahrung an einem oft nicht definierten Ort** irgendwo auf einem Server außerhalb der Rechtsordnung des Nutzers
- **Definierter Ort** der Bereitstellung von Speicherplatz und Ort der Steuerung des Up-/Downloads?
- **Jederzeit Verfügungsgewalt** über Datenzugriff und -löschung?
- **Durchsetzbarkeit** auch ohne Mitwirkung bzw. gegen Willen des Anbieters; Sicherheiten?
- **Gesichertes Rechtmanagement?**
- Anwendbares **Vertragsrecht?**



## Therapievorschläge?

### Detaillierte Leistungsspezifikationen

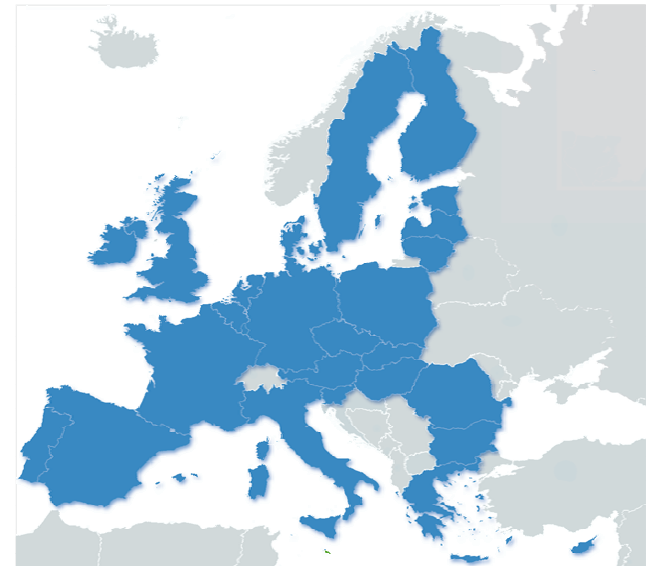
- Leistungsbeschreibung  
Softwareanwendungen und  
Rechnerkapazitäten
- Rechteverwaltung Nutzer
- Rechtsgarantien Anbieter
- Datenverfügbarkeit; Schutz & Sicherheit
  - Garantien zu Ort, Zeit, Art der  
Datenübermittlung- und -  
administration,  
Zugriffsberechtigungen inkl.  
Fernwartung etc.!!!



## Wo ist die Cloud?

### Definition der Art und der Orte der Datenübermittlung

Wie sensibel sind die Daten?  
Wie sicher sind diese Daten?  
Zeit, Art, Inhalt der Zugriffsrechte **und** der Audit- bzw. Kontrollrechte  
Kann der Vertragspartner unbeschränkt Subunternehmer einsetzen?





## Was tun wenns regnet?

Welche Leistungen muss  
Provider bei Vertragsende  
erbringen?

Zurückbehaltungsrechte?

Migrationskosten?

Formate?

Verschlüsselung der  
Übertragung?

Geschwindigkeit der  
Migration?





## Vertragsgestaltung / Vertragsrecht allgemein (1)

- Vielzahl von Komponenten
- AGB-Recht greift, da Leistung mehrfach angeboten wird
- Vertragsrisiken liegen im Fehlen allgemeinverbindlicher oder branchenüblicher Leistungsstandards
- detaillierte Leistungsbeschreibung erforderlich
- Haftungsbeschränkung für Cloud Anbieter nur über Leistungsbeschreibung



## Abhängigkeit von Cloud Services?

- Technisch-organisatorische Leistungsvorgaben
  - » *Vertraulichkeit, Integrität, Verfügbarkeit, Migration und Löschung*
- jederzeitige Audit- und sonstige Kontrollmaßnahmen
- Maßnahmenkatalog im DR-/BC- und Eskalationsmanagement
- Vergütungskriterien
  - » *Zeit/Volumen/Kombi; Vertragsstrafen?*
- Regelungen über Subunternehmer, Teilleistungen und Kündigung
- Bonitätsnachweis und rechtliche Durchsetzbarkeit wenn Anbieter im Ausland
  - » *Rechtswahl, Gerichtsstandsbestimmung, unmittelbar vollstreckbare Sicherheiten (z.B. analog Bauunternehmer)*



## Haftung für die Cloud

- Organisationshaftung verbleibt bei Unternehmensführung
- Konventionelle Audits analog § 9 BDSG (Auditrechte zur Prüfung der Zutritts-, Zugangs- und Zugriffskontrolle) laufen in der Cloud ins Leere
- Vertragsanpassung an die tatsächlichen virtuellen Verhältnisse erforderlich!



## Regreßhaftung und Vertragsstrafen

### Sicherung durch Vertragsstrafen

- die Pflicht zur Geheimhaltung
- die Implementierung verbindlicher Sicherheitskonzepte
- die Einhaltung von IT-Notfallkonzepten
- Pflichten im Reporting und Auditing
- Regress und Schadloshaltung bei Schadensfällen
- Sicherheiten



## Datenschutz und Datensicherheit

- Sensible Bereiche: Personenbezogene und steuerrelevante Daten
  - Bußgelder bis 250K für jeden Einzelfall der Zugriffsverhinderung oder der unzulässigen Datenverlagerung ins Ausland; Einzelheiten s.u.
- Vereinbarungen zu Datenschutz und Datensicherheit
  - Detaillierung der vertraglichen Maßnahmen betr. Betriebssicherheit, Datensicherheit, Datenschutz, Berechtigungskonzept und dazugehörige Kontrollrechte
- Geheimhaltungsvereinbarung
- Vertragsstrafenregelungen; Regress und Freistellung
- Generelle Compliance
- Reporting, Monitoring, Auditing

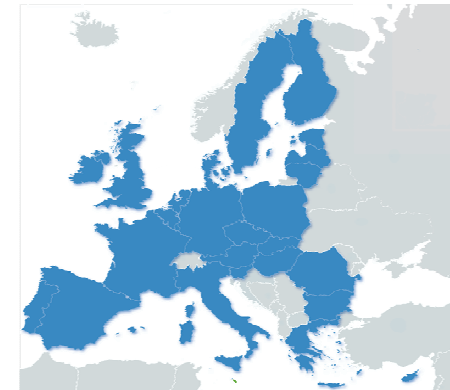
# Vertragstyp

- Für Cloud-Dienste gilt grundsätzlich **Mietrecht**:
  - Nutzung von verteilten Servern
  - Aber zugleich Nutzung diverser, weltweit verteilter **dienstvertrag**stypischer Leistungen
- **Eingeschränkte Verfügbarkeitszusage**
  - Nach Mietrecht würde der Cloud-Anbieter eine 100% Verfügbarkeit garantieren müssen.
  - Dies lässt sich jedoch technisch nicht abbilden. Daher kann nur eine detaillierte Leistungsbeschreibung die Gesetzeslage an die faktischen Gegebenheiten anpassen.
    - Vertragsverhältnis sehr genau im Lastenheft zu spezifizieren
    - Rechtswahl- und Gerichtsstandsvereinbarung.
    - SLRs und SLAs



## Europäisches Datenschutzniveau

- EU verlangt, dass personenbezogene Daten nur in Länder mit gleichem Datenschutzniveau übertragen werden dürfen
- generelle Anerkennung zB Schweiz, Norwegen
- EUGH: Veröffentlichung im Internet keine Übertragung außerhalb der EU
- Cloud-Dienste nur außerhalb der EU erlaubt, wenn Selbstverpflichtungserklärungen (Safe Harbour) abgegeben wurden und Vereinbarungen getroffen sind, dass europäisches Datenschutzniveau eingehalten wird





## Safe Harbour

- Selbstverpflichtungserklärung von Unternehmen außerhalb der EU zur Einhaltung europäischer Datenschutzstandards
- politischer Kompromiss mit USA
- Liste beim amerikanischen Handelsministerium im Internet verfügbar

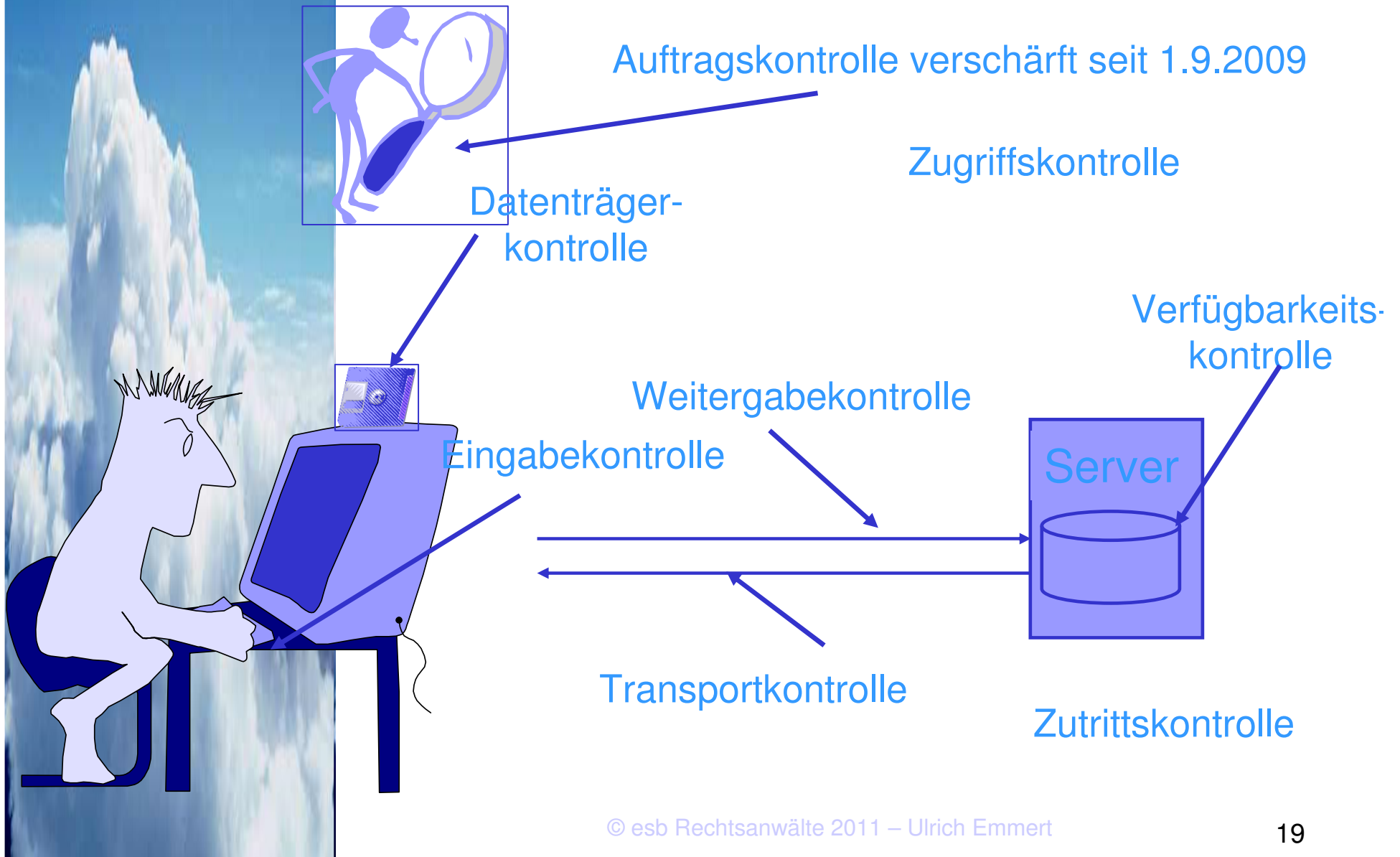




## Bundesdatenschutzgesetz § 9

- Technische und organisatorische Maßnahmen
- gültig für alle Unternehmen und Behörden
  - Anlage (zu § 9 Satz 1): Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die **innerbehördliche** oder **innerbetriebliche** Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
  - Neu seit 1.9.2009 : bei jedem Vertrag mit personenbezogenen Daten im Auftrag zu dokumentieren, vorab und regelmäßig zu kontrollieren

## Kontrollen der Datensicherheit (§ 9 BDSG)



## Cloud und Haftung

- Haftungsentlastung (Exkulpation, s.o.) ?
  - Originäre Verpflichtungen IT-Sicherheit, Datenschutz, Geheimnisschutz etc. bleiben im Grundsatz beim Träger der Dienststelle; Delegierbarkeit entbindet nicht von Verantwortlichkeit
  - Verantwortungsverlagerung käme sonst einer Aufgabenübertragung gleich. Dies geht jedoch grundsätzlich nur durch ein Gesetz oder aufgrund eines Gesetzes (vgl. z.B. § 23 LVwG)
  - Auch bei der Einschaltung Externer muss also der Auftraggeber Herr des Verfahrens bleiben
  - Ansprüche Betroffener auf Berichtigung, Löschung, Sperrung, Vertraulichkeit/Datengeheimnisschutz richten sich weiterhin gegen Auftraggeber



## Cloud und Kontrolle

- Zu den bestehenden Sorgfaltspflichten kommen sogar weitere hinzu, die zum 1.9.2009 drastisch verschärft worden sind:
- Der Auftragnehmer ist sorgfältig auszuwählen und dabei besonderes Augenmerk auf seine *Sicherheitsvorkehrungen* zu legen
- Die Datenschutzvorkehrungen sind bereits vor Beginn des Auftrags zu kontrollieren, so genannte Vorabkontrolle
- Auch während des Auftrags sind die technischen und organisatorischen Maßnahmen des Auftragnehmers regelmäßig zu kontrollieren
- Die Kontrolle ist zu dokumentieren
- Die Prüfung darf nicht dem Auftragnehmer überlassen werden
- Der Auftrag selbst ist **schriftlich** zu erteilen
- Der Auftragnehmer hat den Auftraggeber auf Datenschutzverstöße hinzuweisen
- nach außen haftet fast ausschließlich der Auftraggeber



## Cloud Computing und Kontrolle

### Anzugeben sind

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.



## Outsourcing: Haftung des RZ?

- Muss dieselben technisch-organisatorischen Maßnahmen treffen (vgl. Anlage zu § 9 BDSG)
- Straf- und Bußgeldhaftung; grundsätzliches Haftungsrisiko
- Daher ist auf Seiten des Externen ein Katalog von Hinweis- und Risikoverteilungsklauseln geboten
  - Möglichst detaillierte Leistungsbeschreibung
  - Wenn der Ansicht, dass eine Weisung gegen Datenschutz etc. verstößt, ist unverzüglich darauf hinzuweisen
  - Einige Beispiele: Angehöriger freier Berufe oder Amtsträger trifft Gebot besonderer Vertraulichkeit (§ 203 StGB), aber:
  - Eine an einen Geheimnisträger gerichtete E-Mail unterliegt beim Externen nicht dem Beschlagnahmenschutz durch Strafverfolgungsbehörden

## Datenzugriff im Ausland

Voraussetzungen sind, dass

1. der Steuerpflichtige die Zustimmung zur Durchführung eines Zugriffs auf elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen der zuständigen Stelle des Staates, in den die elektronischen Bücher und Aufzeichnungen verlagert werden sollen, vorlegt,
2. der Steuerpflichtige der zuständigen Finanzbehörde den Standort des Datenverarbeitungssystems und bei Beauftragung eines Dritten dessen Namen und Anschrift mitteilt,
3. der Steuerpflichtige seinen sich aus den §§ 90, 93, 97, 140 bis 147 und 200 Abs. 1 und 2 ergebenden Pflichten ordnungsgemäß nachgekommen ist und
4. der Datenzugriff nach § 147 Abs. 6 in vollem Umfang möglich ist.

Eine Änderung der unter Satz 3 Nr. 1 und 2 benannten Umstände ist der zuständigen Finanzbehörde unverzüglich mitzuteilen. Liegen die Voraussetzungen der Sätze 1 und 2 oder Satz 3 Nr. 1 oder Nr. 2 nicht vor, kann die zuständige Finanzbehörde die Führung und Aufbewahrung elektronischer Bücher und sonstiger erforderlicher elektronischer Aufzeichnungen außerhalb des Geltungsbereichs dieses Gesetzes nur bewilligen, wenn die Besteuerung hierdurch nicht beeinträchtigt wird. Fällt der Bewilligungsgrund weg, hat die zuständige Finanzbehörde die Bewilligung zu widerrufen und die unverzügliche Rückverlagerung der elektronischen Bücher und sonstigen erforderlichen elektronischen Aufzeichnungen in den Geltungsbereich dieses Gesetzes zu verlangen; den Vollzug hat der Steuerpflichtige nachzuweisen.

## Datenschutzrechtliche Löschungspflichten

### Unternehmen

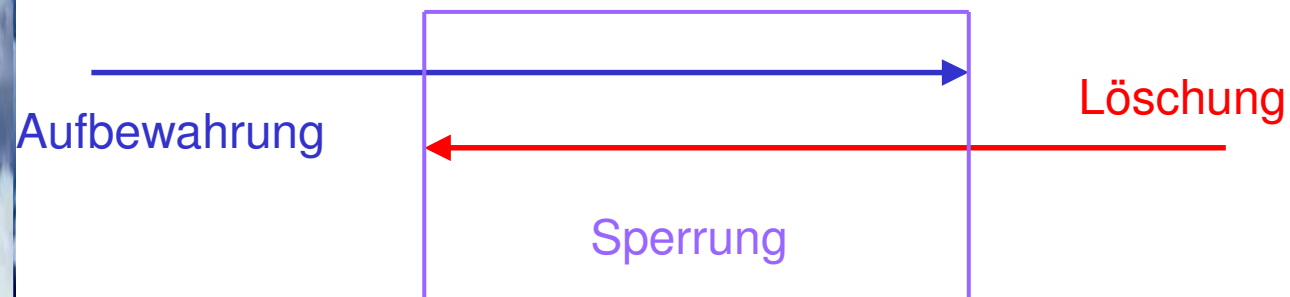
#### § 35 Berichtigung, Löschung und Sperrung von Daten

- (2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn
  - 1. ihre Speicherung unzulässig ist,
  - 2. es sich um Daten über die rassistische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
  - 3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder
  - 4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.
- (3) An die Stelle einer Löschung tritt eine Sperrung, soweit
  - 1. im Fall des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
  - 2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
  - 3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.
- (4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. [...]
- (8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
  - 1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
  - 2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.



## Speicherung contra Datenschutz

- Bei datenschutzrechtlichen Lösungsverpflichtungen tritt an die Stelle der Löschung die Sperrung
- Aufbewahrungsverpflichtung ohne Recht zur eigenen Datennutzung
- Kaum Kontrolle möglich
- Persönlichkeitsprofile von Kunden und Mitarbeitern möglich



## Offenlegungspflichtige Datenpannen



§ 3 Nr. 9 BDSG  
z.B. Daten zu  
Gesundheit, Religion  
Sexualleben



Daten zu Straftaten  
und Ordnungswidrigkeiten



Bank- und Kreditkartendaten

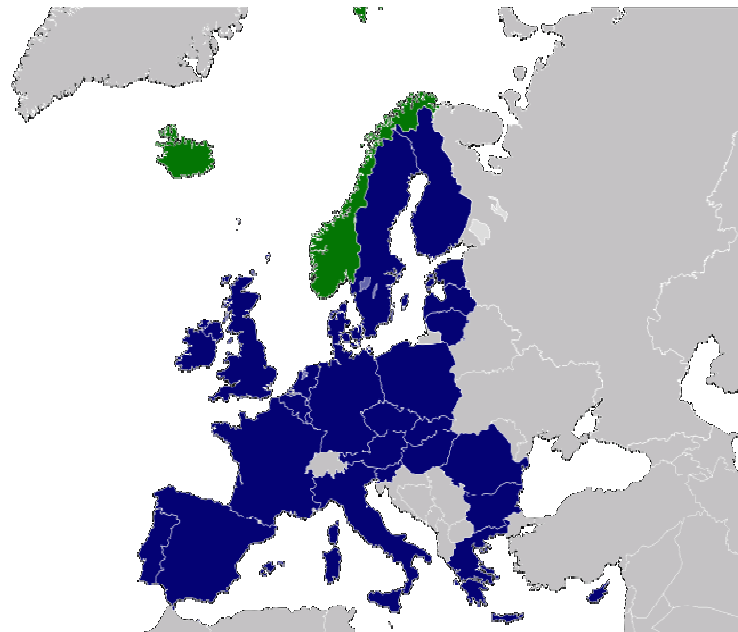


Berufsgeheimnisse



## Datenzugriff im Ausland

- bisher war es nach § 146 Abs.2 verboten, Steuerunterlagen im Ausland aufzubewahren.
- seit 2009 bei Vorlage von Unterlagen, dass örtliche Behörden Zugriff sichern, Aufbewahrung im EWR zulässig (alte Fassung 146 Abs. 2a AO), falls Amtshilfevereinbarungen existieren



- Seit 1.1.2011 unter gleichen Voraussetzungen auch außerhalb des EWR zulässig (neue Fassung 146 Abs. 2a AO)



## Dienstleistungen esb Rechtsanwälte – [www.kanzlei.de](http://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