

# **Cloud Computing und seine Konsequenzen für den Datenschutz und die betriebliche Mitbestimmung**

**Vortrag im Rahmen der Tagung  
Green IT und Industrialisierung der IT**

**IGBCE; HBS; Borderstep; Stiftung Arbeit und Umwelt**

**Jürgen Fickert, TBS NRW e. V.**

- **Rahmenbedingungen und Begriffe**
- **Datensicherheitsanforderungen des BSI**
- **Datenschutzrechtliche Einordnung**

**Die TBS NRW e.V. wird von den Gewerkschaften in NRW sowie dem Ministerium für Arbeit, Integration und Soziales getragen und handelt im Rahmen eines Landesauftrages.**

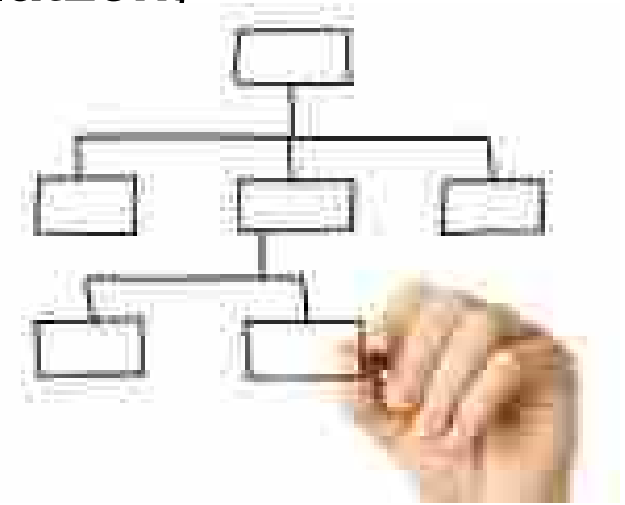
**35 Beschäftigte arbeiten  
In den Regionalstellen  
Düsseldorf, Dortmund und Bielefeld**



- **Outsourcing ERP-Systeme, zum Beispiel SAP (nur Betrieb, Datenbanken, Datensicherung, ...)**
- **externe Gewährleistung der Internetsicherheit (Zugriff Internet, E-Mail, Firewall, Spam, ...)**
- **SaaS - Software as a Service - Zugriff zu Softwaredienstleistungen aus dem Internet**
- **Cloud Computing**
- **unterschiedliche vertragsrechtliche Varianten, Kauf und Eigentum, Miete von Hardware oder Software, ...**



- **Verlagerung und Abbau von Arbeitsplätzen, Rationalisierung**
- **Änderung von Arbeitsabläufen, Geschäftsprozessen, Umstrukturierungen**
- **Unterstützung der Nutzer bei Probleme Software-Ergonomie, aber auch**
- **kurzfristig zusätzliche Auswertungen**
- **Qualifizierungsmaßnahmen**
- **verbleibende IT-Kernkompetenz im Unternehmen**
- **Innovation und Investitionen im Unternehmen**



**Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle.**



**Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.**

**Quelle: Eckpunktepapier - Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit); BSI 2011**

### Infrastructure as a Service (IaaS)

Angebot von IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst. Ein Cloud-Kunde kauft diese in hohem Maß standardisierten Services und baut darauf eigene Services auf.

### Plattform as a Service (PaaS)

Ein PaaS-Provider stellt eine komplette IT-Infrastruktur bereit. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen.

### Software as a Service (SaaS)

Sämtliche Angebote von **IT-Anwendungen**, wie Vertriebsmanagement, FiBu, Textverarbeitung oder Entgeltabrechnungen.



Einfluss Auftraggeber nimmt ab

Das BSI empfiehlt, dass der Cloud Service Provider CSP ein zuverlässiges und sicheres Management der Informationssicherheit (Information Security Management System, ISMS) betreibt. Beispiele sind für Aufbau und Betrieb eines ISMS an ISO 27001/2 oder bevorzugt am BSI Standard 100-2 zur IT-Grundschutz-Vorgehensweise (der ISO 27001/2 abdeckt) zu orientieren.

- **BSI-Standard 100-1:Managementsysteme für Informationssicherheit**
- **BSI-Standard 100-2: Vorgehensweise nach IT-Grundschutz**



# Datensicherheitsanforderungen bei Cloud Computing (2)

Sicherheitsmanagement beim Anbieter	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Definiertes Vorgehensmodell für alle IT-Prozesse (z. B. nach ITIL, COBIT)	✓			✓		
Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. nach BSI-Standard 100-2 (IT-Grundschutz), ISO 27001)	✓			✓		
Nachhaltige Umsetzung eines Informationssicherheitskonzepts für die Cloud	✓			✓		
Nachweis einer ausreichenden Informationssicherheit (Zertifizierung)		✓	✓		✓	✓
Angemessene Organisationsstruktur für Informationssicherheit beim CSP (inklusive Benennung von Ansprechpartnern für Kunden zu Sicherheitsfragen)	✓			✓		

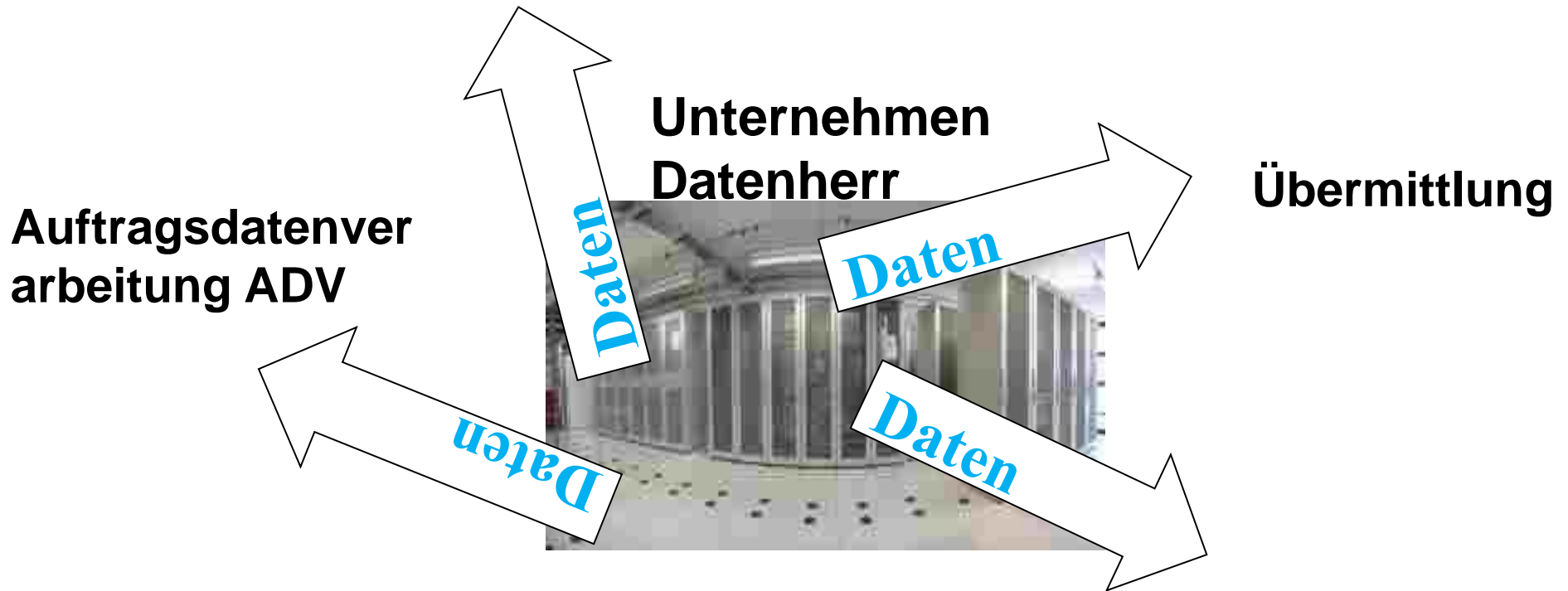
**Erläuterungen: B Basisanforderungen**

**C+ erhöhte Anforderungen bei erhöhter Vertraulichkeit**

- **Sicherheitsarchitektur**
- **Rechte-Management**
- **Monitoring, Protokolle und Revision**
- **Sicherheitsprüfungen, Kontrollen**
- **Notfallmanagement**

- **Klassische Auftragsdatenverarbeitung durch externen IT-Dienstleister, zum Beispiel SAP-Personalwesen**
- **gemeinsame Datenverarbeitung in einer Unternehmensgruppe, gemeinsame Eigentümer/Familienunternehmen**
- **„Shared services“ - Zentralisierung z. B. FiBu, Einkauf, Personalentwicklung bei Konzernmutter**
- **konzernweites Management von IT-Projekten, mit Personaleinsatz, Personalbewertung**
- **internationale Konzerne mit Anwendungen wie Wissensdatenbanken, Facebook, Beschäftigtenprofilen**
- **Ansätze zur konzernweiten Personalentwicklung und -einsatzplanung, zum Beispiel für F&E-Beschäftigte**

- ... die datenschutzrechtliche Bewertung von der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten außerhalb des **Unternehmens (!)**



- **ADV erfolgt für eigene Zwecke des Unternehmens / der GF**
- **GF bleibt „Herr der Daten“, verantwortliche Stelle**
- **GF hat Überwachungspflichten**
- **Es gibt kein Konzernprivileg**
- **Angemessene **Dokumentation** (Beteiligte; Art / Umfang der Kontrollen; Feststellungen; Maßnahmen; Nachhaltigkeit, ...)**
- **Bußgeld nach § 43**
- **ADV ist nur in EU- und EWR-Staaten zulässig!  
(vgl. § 3 (8) BDSG)**

# §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag <sup>(1)</sup>

**(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.**

**(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen 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,**

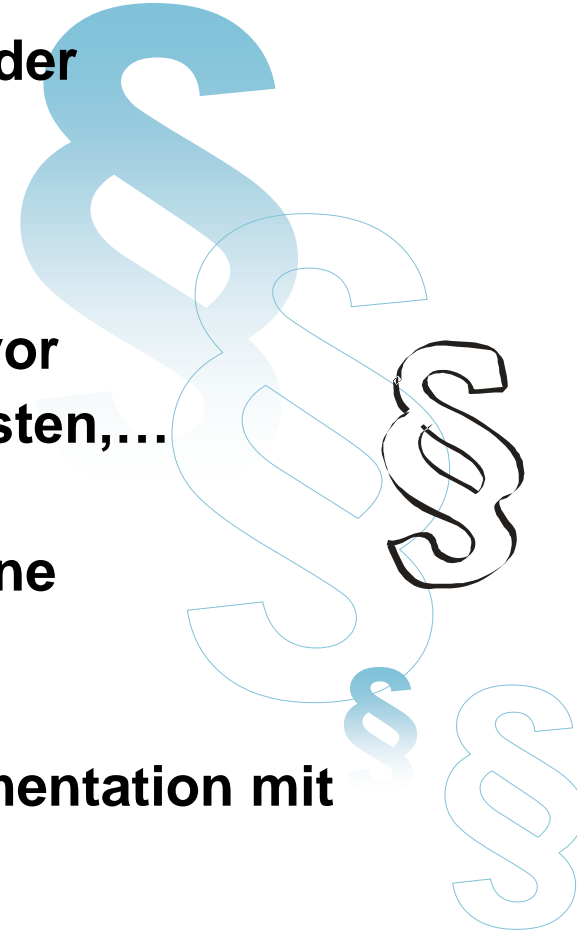
# §11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (2)

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.

... 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.

## §3 (4) Begriffsbestimmungen

- Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen **Dritten** ...
- Daten liegen bereits in elektronischer Form/Datei vor
- Bekanntgabe: Auch durch Gespräch, Fax, Papierlisten,...
- Veröffentlichung ist keine Datenübermittlung
- Auftragsdatenverarbeitung nach § 11 BDSG ist keine Datenübermittlung
- Automatisches Abrufverfahren: Schriftliche Dokumentation mit Zweck, Empfänger,...



## § 28 Datenerhebung und –speicherung für eigene Geschäftszwecke

- (1) Das Erheben, Speichern, Verändern oder **Übermitteln** personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig
1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen **erforderlich** ist,
  2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das **schutzwürdige Interesse des Betroffenen** an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder ...

- **Nach der EU-Datenschutzrichtlinie gelten einheitliche Datenschutz-Mindeststandards in allen EU- und EWR-Staaten; grenzüberschreitende Auftragsdatenverarbeitung und Übermittlung grundsätzlich zulässig**
- **ADV in einem Drittstaat außerhalb EU /EWR nicht zulässig**
- **Nach § 4b BDSG ist Datenübermittlung nur in Drittstaaten mit „angemessenen Datenschutzniveau“ zulässig; der Einzelfall muss geprüft werden**
- **Die Datenverarbeitung personenbezogener Daten ist in weltweit verteilten Cloud-Rechenzentren unzulässig**
- **Hier ist der betriebliche Datenschutzbeauftragte gefordert!**

## § 80 (1) Allgemeine Aufgaben

... darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, ... durchgeführt werden

## § 87 Mitbestimmungsrechte

(1) Der Betriebsrat hat ... in folgenden Angelegenheiten mitzubestimmen:

6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen;

## § 94 Personalfragebogen, Beurteilungsgrundsätze

(1) Personalfragebogen bedürfen der Zustimmung des Betriebsrats.

- **Welche Qualität, welches Überwachungspotenzial haben die Daten?**
- **Was ist die genaue Zweckbestimmung?**
- **Wer sind die Berechtigten und Empfänger, im In- und Ausland?**
- **Sind Vorgesetzte beteiligt?**
- **Gibt es gutes Datenschutzkonzept?**
- **Handelt es sich um Überwachung oder „nur“ um ein Datenschutzproblem?**

# Finger weg von meinen Daten!



## Beratung zum Beschäftigtendatenschutz

Die TBS NRW kümmert sich, die Mitbestimmung der Betriebsräte und den Datenschutz von Beschäftigten zu sichern.

- Fachtagung am 10. Mai 2011 in Bochum
- Seminare
- Aktuelles unter [www.tbs-nrw.de](http://www.tbs-nrw.de)
- Handlungshilfe
- ...

- **www.bfd.bund.de**
- **www.bsi.de Bund**      **www.bsi-fuer-buerger.de**
- **www.datenschutzzentrum.de**
- **[www.datenschutz.de](http://www.datenschutz.de)**
- **www.datenschutzverein.de**
- **www.gdd.de**
- **www.bitkom.de**
- **www.tbs-netz.de**