

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

# Informationelle Selbstbestimmung im Wolkenkuckucksheim

Dr. Imke Sommer

20. Europäischer Verwaltungskongress  
Bremen, 5. März 2015

---

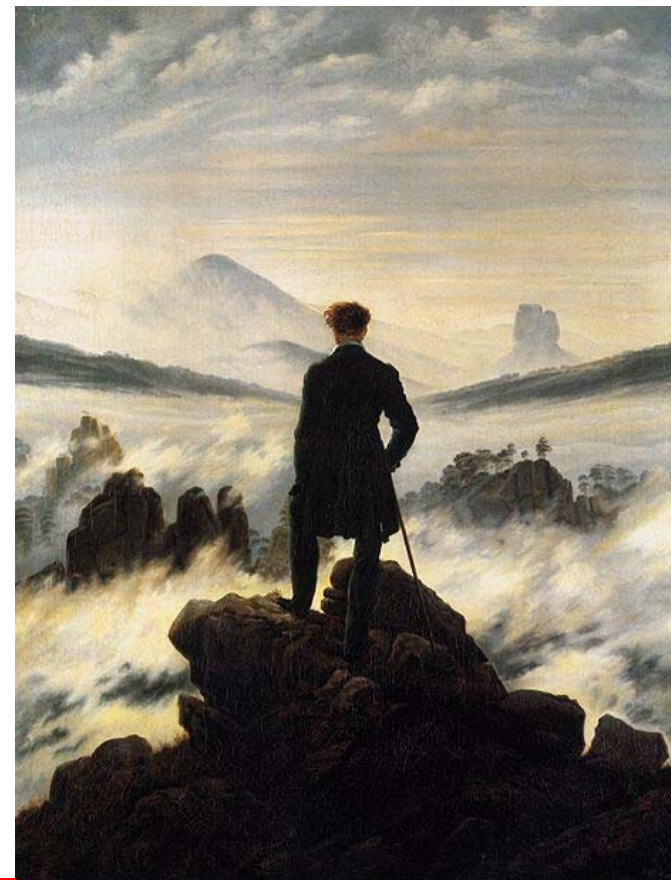
# Das Wolkenkuckucksheim gestern...

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- Die Vögel,  
Komödie von Aristophanes 414 v. Chr.:  
Das Wolkenkuckucksheim ist  
eine Stadt in den Wolken,  
die sich die Vögel gebaut haben.
- Wolkenkuckucksheim steht für  
eine Utopie ohne Bodenhaftung  
und Realitätssinn



# ...das smarte cloud-cuckoo-land heute

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

In der Popkultur bezeichnet Wolkenkuckucksheim eine "[...] Welt voller Merkwürdigkeiten und exzentrischer Charaktere" (Wikipedia)

Lego Movie  
Wolkenkuckucksheim-  
Palast



---

<http://7onashoestring.com/lego-movie-cloud-cuckoo-palace/>

# Cloudcomputing

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Wolke = Gebräuchliches Bild der Informatik für formlose Netze mit nur bedingt von den NutzerInnen erkennbaren Strukturen
  - Die Cloud: eine über Netze angeschlossene Rechnerlandschaft, in welche eigene Datenverarbeitungen ausgelagert werden können
  - Cloudcomputing: Bereitstellung von IT-Dienstleistungen (Infrastrukturen, Plattformen, Anwendungssoftware) in der Cloud
    - aufeinander abgestimmt, schnell und dem tatsächlichen Bedarf angepasst
    - nach tatsächlicher Inanspruchnahme abrechenbar
-

# Informationelle Selbstbestimmung beim Cloudcomputing

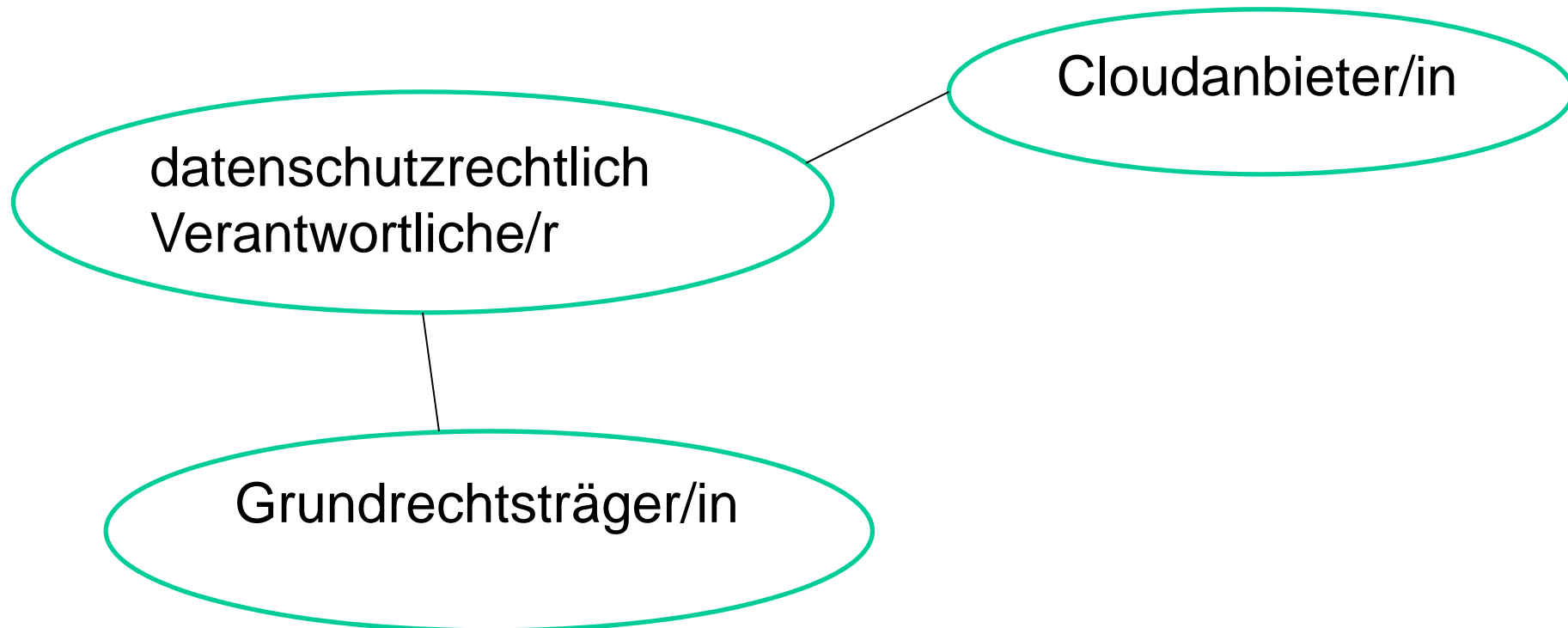
---

Die Landesbeauftragte für Datenschutz und Informationsfreiheit



Freie Hansestadt Bremen

## Dreierkonstellation:



# Datenschutz ist Grundrechtsschutz (1)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

**Grundrecht auf  
Vertraulichkeit und Integrität  
informationstechnischer Systeme  
(= “IT- Grundrecht”)**



# Datenschutz ist Grundrechtsschutz (2)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

*„Darauf verzichtet, etwas im Netz erneut nachzuschlagen, aus Angst, die Google-Mitarbeiter könnten mich für doof halten.“\**

## Grundrecht auf informationelle Selbstbestimmung

= „das Recht, selbst zu bestimmen, wer wann was über mich weiß“

\*Zitat / Tweet von Benjamin Nickel, veröffentlicht im Twitterbuch

# Wann liegen Grundrechtsverletzungen vor?

---

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- **Greifen Datenverarbeitungen** in das Grundrecht auf informationelle Selbstbestimmung ein?
    - Bundesverfassungsgericht: Weiter Schutzbereich, umfasst ist schon der Schutz vor dem “diffusen Gefühl des Beobachtetseins”
    - Mark Zuckerberg (Gründer + Miteigentümer facebook): „Die Privatsphäre ist tot“
    - Lösung der Probleme neuer Techniken erfolgt nach dem Grundgesetz anders als durch apodiktische Setzung Einzelner
  - Ist der **Eingriff gerechtfertigt** und daher **keine Verletzung** des Grundrechtes? Rechtfertigungsmöglichkeiten:
    1. **Einwilligung** der/des Betroffenen als Ausdruck der individuellen Selbstbestimmung
    2. **Gesetzliche Grundlagen** als Ausdruck der kollektiven Selbstbestimmung
-



# Individuelle Selbstbestimmung: Einwilligung

---

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

## Wirksamkeitsvoraussetzungen:

- **Freiwillig** (z.B. im Beschäftigungsverhältnis grundsätzlich nicht gegeben)
- **Informiert**
- Schriftlich
- Jederzeit **widerruflich**
- Vor der Datenverarbeitung

Fehlt eine der Wirksamkeitsvoraussetzungen, liegt keine den Eingriff rechtfertigende Einwilligung vor und der Eingriff ist **rechtswidrig**.

---

# Kollektive Selbstbestimmung: Gesetze

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

z.B. § 3 Absatz 1 Bundesmeldegesetz:

„Zur Erfüllung ihrer Aufgaben nach § (...) speichern die  
Meldebehörden folgende Daten (...) im Melderegister

1. Familienname,
2. früherer Namen,
3. Vornamen (...)
4. (...)“

# Erinnerung: Informationelle Selbstbestimmung beim Cloudcomputing

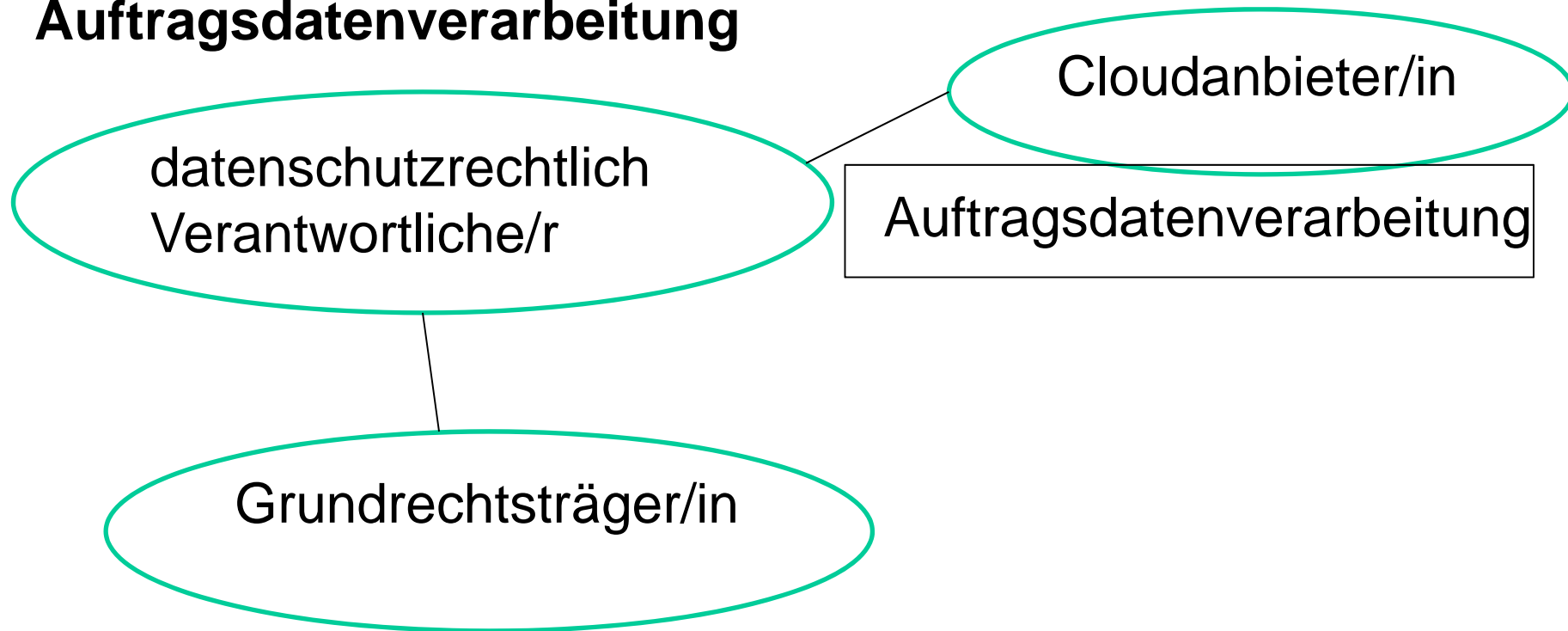
Die Landesbeauftragte für Datenschutz und Informationsfreiheit



Freie Hansestadt Bremen

---

## datenschutzrechtliche Lösung für Dreierkonstellation: Auftragsdatenverarbeitung



# Voraussetzungen für rechtmäßige Auftragsdatenverarbeitung

---

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

Verarbeitung personenbezogener Daten im Auftrag durch andere Personen oder Stellen – **datenschutzrechtliche Verantwortung verbleibt beim Auftraggeber**

- **Auswahl des Auftragnehmers:** Eignung des Auftragnehmers (Berücksichtigung der **technischen und organisatorischen Maßnahmen**)
  - **Steuerung:** Schriftliche Auftragserteilung (**Festlegung** der technischen und organisatorischen Maßnahmen und etwaige **Unterauftragsverhältnisse**)
  - **Kontrolle:** Auftraggeber muss sich von der Einhaltung der Maßnahmen **überzeugen**
  - Auftraggeber muss Unterwerfung unter Landesdatenschutzgesetz und Kontrollzuständigkeit der zuständigen Landesbeauftragten für Datenschutz durchsetzen
-

# Probleme der Auftragsdatenverarbeitung

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Die datenschutzrechtliche Verantwortung kann nicht an den Clouddiensteanbieter abgegeben werden.
  - Risikoeinschätzung durch Auftraggeber
  - Auftragsdatenverarbeitung funktioniert nach einer **privatrechtlichen Logik, also auf Augenhöhe**
    - Zur Weitergabe rechtlicher Anforderungen können keine Verwaltungsakte erlassen werden.
    - Zur Weitergabe rechtlicher Anforderungen gibt es nur vertragsrechtliche Möglichkeiten (Drohung mit Vertragsstrafen)
-

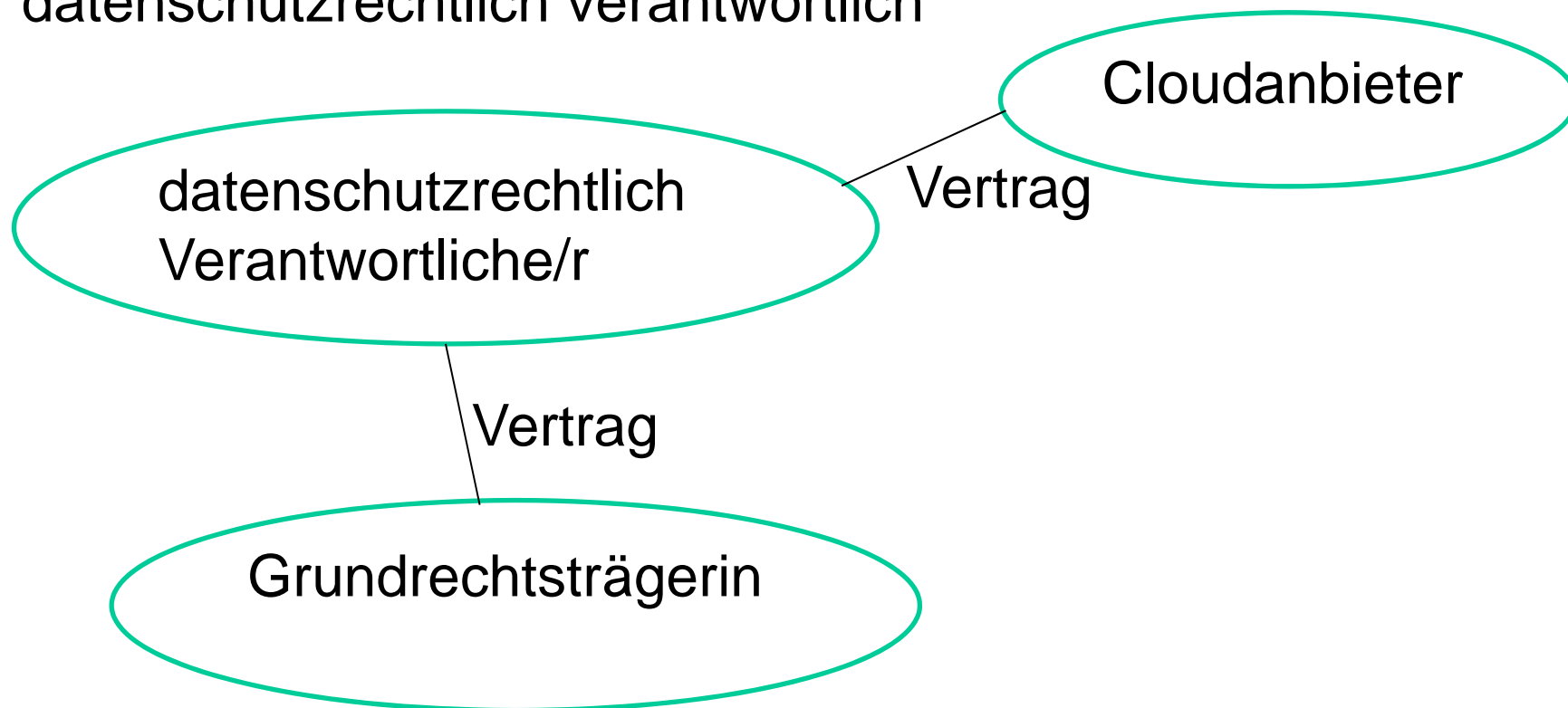
# Informationelle Selbstbestimmung beim Cloudcomputing (1)

Die Landesbeauftragte für Datenschutz und Informationsfreiheit



Freie Hansestadt Bremen

Private Stelle ist datenschutzrechtlich verantwortlich



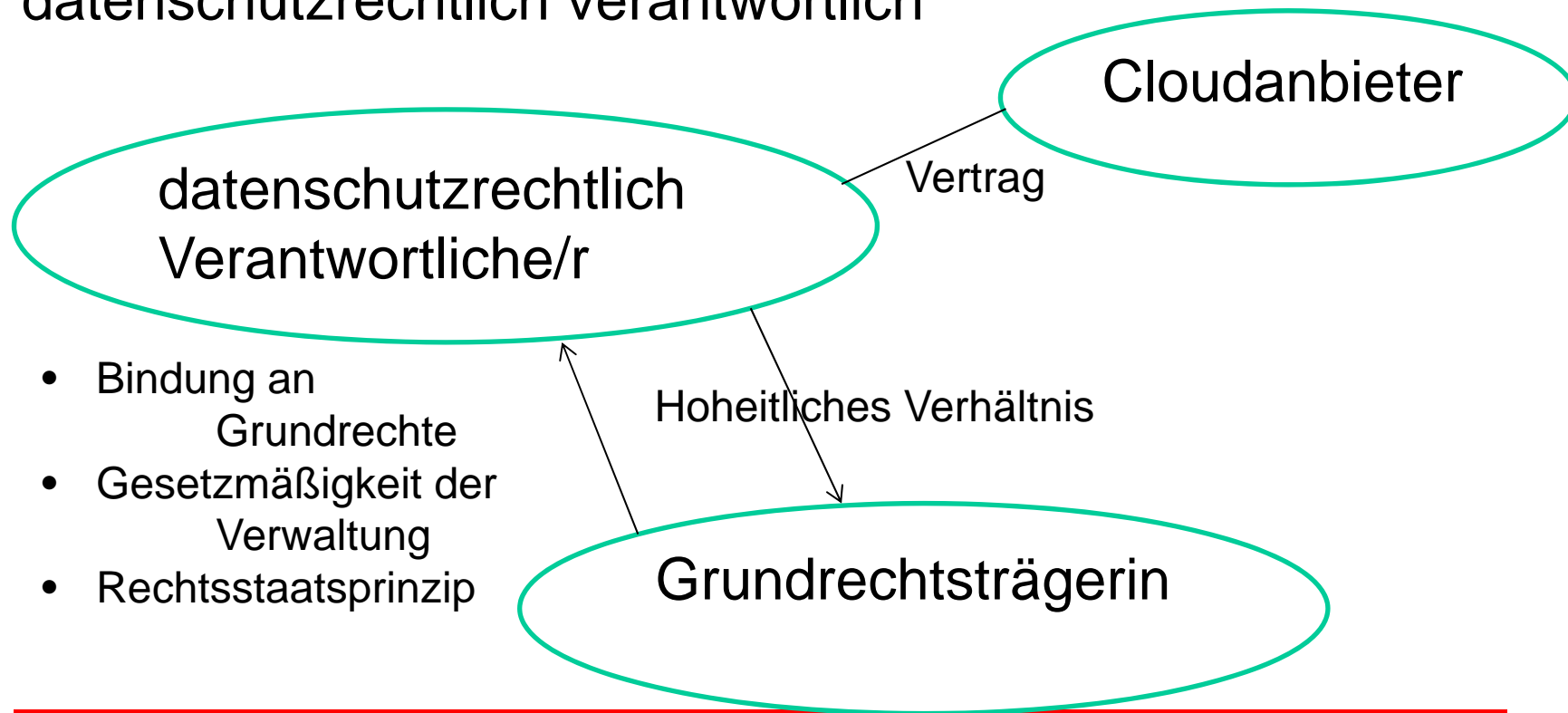
# Informationelle Selbstbestimmung beim Cloudcomputing (2)

Die Landesbeauftragte für Datenschutz und Informationsfreiheit



Freie Hansestadt Bremen

Öffentliche Stelle ist datenschutzrechtlich verantwortlich



# öffentliche Stellen als Auftraggeber von Auftragsdatenverarbeitung: Das „Ob“

---

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

Auftragsdatenverarbeitung funktioniert nach einer **privatrechtlichen Logik**. Das macht es schwerer, der datenschutzrechtlichen Verantwortung nachzukommen.

- **Wann ist AuftragsDV für öffentliche Stellen erlaubt?**
    - Bindung der öffentlichen Verwaltung an Gesetz und Recht (Art. 20 III Grundgesetz), grundsätzlich hat der Gesetzgeber zu entscheiden
    - Artikel 33 Absatz 4 Grundgesetz: Ausübung hoheitsrechtliche Befugnisse idR durch BeamtInnen
      - > wenn durch die Datenverarbeitung der Kernbereich hoheitlicher Tätigkeit berührt ist (z.B. Steuergeheimnis, § 30 Abgabenordnung, nur Verarbeitung durch öffentliche Stellen), scheidet Auftragsdatenverarbeitung (ganz oder durch private Dienstleister) aus.
-



# öffentliche Stellen als Auftraggeber von Auftrags- datenverarbeitung: Das „Wie“

---

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

Mit **geeigneten Auftragnehmern** gute Verträge  
machen,  
die alle **Risiken** so minimieren,  
dass es **verantwortbar** ist, die  
Datenverarbeitung von Dritten ausführen zu lassen

---

# „Klassische“ Risiken beim Cloudcomputing (1)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Legale und illegale **Zugriffe** von Behörden (NSA, GCHQ) und Gerichten der Länder, in denen die Cloudserver stehen
  - **Fahrlässiges oder vorsätzliches missbräuchliches Handeln** von **MitarbeiterInnen** des Cloudanbieters und **Unterauftragnehmern** des Cloudanbieters, z.B. unberechtigtes Kopieren oder Klonen von Systemen, unberechtigte Manipulation oder Herunterfahren von virtuellen Maschinen, Herunterfahren von Hosts, unberechtigte Manipulation von Konfigurationsdateien
  - Unzureichendes Patchmanagement beim Provider und bei Kundensystemen
  - Vorsätzliche Nutzung von **Sicherheitslücken** durch Angriffe Dritter
-

# „Klassische“ Risiken beim Cloudcomputing (2)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Vorsätzliche Nutzung von **Sicherheitslücken beim Provider** durch **andere Kunden**, z.B. zur Übernahme der Kontrolle über andere virtuelle Maschinen, durch Zugriff auf das Dateisystem des Hosts, zur Denial-of-Service-Angriffe auf den Hypervisor, zum Abhören der Datenkommunikation zwischen virtuellen Maschinen, durch unberechtigte Speicherzugriffe
  - Missbrauch der Plattform des Providers, z.B. für Brute-Force-Angriffe auf Passwörter, den Aufbau von Botnetzen, die Einschleusung von Schadsoftware, das Versenden von SPAM
  - Nutzung von Sicherheitslücken auf den Übertragungswegen via Internet zwischen Kunden und Providern
-

# „Klassische“ Risiken beim Cloudcomputing (3)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Unbeabsichtigte oder vorsätzliche Nutzung von **Sicherheitslücken** in den vom Provider zur Nutzung durch die Kunden bereit gestellten Software-Schnittstellen und APIs
  - Angriffe durch **Schadsoftware** auf die Dienste in der Cloud,
  - Risiken jeglicher Form von **Computerkriminalität** durch schlecht kontrollierte Registrierungsmodalitäten zur Nutzung von Clouddiensten
  - Cloud-unabhängige **Sicherheitsmängel der technischen Infrastruktur** – bedingt durch fehlende oder unzureichende Sicherheitskonzepte, wie z.B. eine unsere Stromversorgung, eine mangelhafte Klimatisierung der Infrastrukturräume oder der Zutrittskontrolle zu Gebäuden und Räumen
-

# Cloudspezifische Risiken beim Cloudcomputing

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

Cloudspezifische Risiken bei

- Löschung von Daten
- Nachvollziehbarkeit durch Protokollierung und Dokumentation
- Vervielfältigung und Verteilung der Daten
- Datentrennung
- Transparenz der Datenverarbeitung in der Cloud
- Verfügbarkeit in der Cloud

# Besondere Probleme im Wolkenkuckucksheim über den USA...

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

01100101 01100001  
01100110 01110100  
011**B1G D0T0**0000  
101**F0R** 01001000  
011**B0ND 2.0**11101  
01101110 01110011  
01100110 01110100  
10101010 01010101  
01111010

- Massenhafte und anlasslose Überwachung von BürgerInnen und offiziellen Stellen durch ausländische Geheimdienste durch (unter anderem National Security Agency (NSA))
- Insbesondere wichtig im Zusammenhang mit Auftragsdatenverarbeitung durch Dienstleister in den USA: Datenübermittlung von Daten europäischer BürgerInnen, die diese US-Firmen gegenüber offenbart haben, an den US-Nachrichtendienst NSA.

# Übermittlung personenbezogener Daten ins Nicht-EU-Ausland (1)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- § 4b II BDSG „Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn (...) ein angemessenes Datenschutzniveau nicht gewährleistet ist.
  - Europäische Datenschutzrichtlinie 95/46 EG: Daten von EU-Bürgerinnen und EU-Bürgern dürfen in Staaten außerhalb der EU übermittelt werden, wenn im Empfängerstaat ein dem EU-Recht vergleichbares Datenschutzniveau besteht.
  - Europäische Kommission: Kein vergleichbares Datenschutzniveau in den USA.

# Übermittlung personenbezogener Daten ins Nicht-EU-Ausland (2)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

Verbleibenden Übermittlungsmöglichkeiten:

- Im Jahr 2000 „**Safe-Harbor**“-Entscheidung der Europäische Kommission: Daten dürfen ausnahmsweise in die USA übermittelt werden, wenn sie dort in einem „sicheren Hafen“ („safe harbor“) landen.
- § 4c BDSG, Ausnahmen: „(...) kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen (...) genehmigen, wenn die verantwortliche Stelle ausreichende Garantien (...) vorweist; die Garantien können sich insbesondere aus Vertragsklauseln (=Standardvertragsklauseln) oder verbindlichen Unternehmensregelungen (= Binding Corporate Rules) ergeben. Sofern die Übermittlung durch öffentlichen Stellen erfolgen soll, nehmen diese die Prüfung vor.“



# Safe Harbor

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Um sich als „sicherer Hafen“ zu qualifizieren, können sich US-Unternehmen auf einer Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die in der entsprechenden Entscheidung der Kommission niedergelegten Grundsätze und die dort formulierten FAQ (frequently asked questions) zu beachten.
  - Zu den Grundätzen der Safe-Harbor- Entscheidung gehören
    - die Verpflichtung, Sicherheitsvorkehrungen zu treffen, um die personenbezogenen Daten vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.
    - das Verbot, personenbezogene Daten in einer Weise zu verarbeiten, die mit dem ursprünglichen Erhebungszweck unvereinbar ist.
-

# Probleme von Safe Harbor

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- gegenwärtig unter 3000 „sichere Häfen“, ständiges Kommen und Gehen
  - Die Safe-Harbor-Grundsätze werden entgegen der Behauptung nicht erfüllt (Galexia-Studien)
  - Fälschliche Behauptungen, sicherer Hafen zu sein (Galexia-Studien)
    - 2008: 208
    - 2010: 331
    - Sept 2013: 427 (darunter Organisationen, die zu den top 100 des webtraffic gehören)
  - Viele Datenarten sind ausgeschlossen (Finanzdienstleistungsdaten, Reisedaten, Telekommunikationsdaten)
-

# Safe Harbor – Befugnisse der nationalen Aufsichtsbehörden

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Nationale Aufsichtsbehörden können die Datenübermittlung in die USA aussetzen, wenn eine "hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze verletzt sind.
  - Zwar ist die Geltung der Grundsätze des "sicheren Hafens" begrenzt, sofern es die nationale Sicherheit erfordert oder Gesetze solche Ermächtigungen vorsehen. Ein umfassender und anlassloser Zugriff auf personenbezogene Daten kann durch Erwägungen zur nationalen Sicherheit in einer demokratischen Gesellschaft aber nicht gerechtfertigt werden.
  - **Hohe Wahrscheinlichkeit der Verletzung der Safe-Harbor-Grundsätze** ist nach Auffassung der **Datenschutzkonferenz** angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste eingetreten (gemeinsame Presseerklärung vom 24.Juli 2013).
-

# Was tun, um informationelle Selbstbestimmung im Wolkenkuckucksheim zu gewährleisten?

Die Landesbeauftragte für Datenschutz und Informationsfreiheit



Freie Hansestadt Bremen



Entschließung der  
Datenschutzkonferenz  
vom 9.10.2014:  
„Orientierungshilfe  
Cloud-Computing  
Version 2.0“

# Risiken sorgfältig abschätzen

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Im Zweifel **gegen** das Wolkenkuckucksheim entscheiden.
  - Abstufung der Risiken zwischen von „verbeamteten“ und „privaten“ Wolkenkuckucks betriebenen Wolkenkuckucksheimen beachten: Im Zweifel für das „**verbeamtete**“ Wolkenkuckucksheim entscheiden
  - Bei Entscheidung für von Privaten betriebene Wolkenkuckucksheime Abstufung zwischen Wolkenkuckucksheimen im und außerhalb des Schengen-Raumes (= „Safe-Harbor-Problematik“): Im Zweifel für das Wolkenkuckucksheim im **Schengen-Raum** entscheiden
-

# informationelle Selbstbestimmung bei Nutzung von Clouddiensten (1)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

Die Wahrnehmung der datenschutzrechtlichen Verantwortung (Datenschutz, Informationssicherheit) setzt **Kontrollierbarkeit, Transparenz, Beeinflussbarkeit** voraus.

- Offene, transparente und detaillierte **Informationen der Anbieter** über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption ermöglichen Entscheidung über das Ob der Nutzung von Clouddiensten und den Anbieter
- Detaillierte, transparente und eindeutige **vertragliche Regelungen** der cloudgestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z.B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen“ kann.

# informationelle Selbstbestimmung bei Nutzung von Clouddiensten (2)

---

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- Die Umsetzung von abgestimmten Sicherheitsmaßnahmen auf beiden Seiten (Cloudanbieter und Cloudanwender)
- Vorlage aktueller Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird, zur Gewährleistung der Informationssicherheit und der Portabilität und Interoperabilität durch anerkannte und unabhängige Prüforganisationen

Soweit öffentliche Stellen **Clouddienste in Drittstaaten** in Anspruch nehmen, ist eine besonders sorgfältige Prüfung der **Rechtsgrundlage** geboten, weil es einen dem § 28 Absatz 1 Satz 1 Nr. 2 BDSG entsprechenden Erlaubnistatbestand in den Landesgesetzen nicht gibt.

---

# Weitere Ausprägungen der informationellen Selbstbestimmung in der Cloud

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

## Vermeidung personenbezogener Daten

- **Verzicht** – keine personenbezogenen Daten erheben
- **Anonymisierung** – ursprünglich vorhandenen Personenbezug nachträglich verhindern

## Erschwerter Zugang zu personenbezogenen Daten

- **Verschlüsseln**
- Nutzung von **sicheren Übertragungswegen**
- Alle anderen Maßnahmen des **technischen und organisatorischen Datenschutzes**



# Verzicht auf personenbezogene Daten

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- 
- Für die legitimen Ziele ist der Personenbezug häufig irrelevant. (Datensparsamkeit, privacy by design)
  - **Problem:** Mächtige Gegenspieler
    - Im Jahr 2014 werden weltweit 190 Mrd. € allein in „Smart-City-Projekte“ fließen
    - Jahresumsatz SAP 16,815 Mrd. € (2013)
  - **Problem:** Steigender Einfluss für den verfassungsrechtlichen Ansatz, „unbedeutende“ personenbezogene Daten aus dem Schutzbereich des Grundrechtes herauszudefinieren
    - Dagegen Bundesverfassungsgericht, Volkszählungsurteil (1983): „Durch die Verarbeitungs- und Verknüpfungsmöglichkeiten der Informationstechnologien kann ein für sich alleine als belanglos beurteiltes Datum einen neuen Stellenwert bekommen.(...) Eine abstrakte Einteilung in schützenswerte und freizugebende Daten ist nicht möglich.“
-

# Anonymisierung (1)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen



- Vom Grundrecht auf informationelle Selbstbestimmung werden (nur) **personenbezogene** Daten geschützt
- Dazu gehören **auch** personen**beziehbare** Daten
- Zu den personenbeziehbaren, also geschützten Daten gehören **auch Pseudonyme**
- **Nicht** vom Grundrecht auf informationelle Selbstbestimmung geschützt werden **anonymisierte** Daten

## Anonymisierung (2)

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- “**Anonymisieren** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr **oder** nur mit einem unverhältnismäßig hohen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.”
- Anonymisierung verhindert den zunächst/grundsätzlich herstellbaren Personenbezug
- > eine **erfolgreiche Anonymisierung** beachtet das Grundrecht auf informationelle Selbstbestimmung



# Keine Anonymisierung ...

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen



# Verschlüsseln, verschlüsseln, verschlüsseln

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- Kryptographische Schutzverfahren
- Schon einfache Sicherheitsmaßnahmen (statt "http" "https") steigern die Komplexität und die Kosten von Angriffen
- Bundesamt für Sicherheit in der Informationstechnik ([https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesstkommunizieren/verschluesst\\_kommunizieren\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/Verschluesstkommunizieren/verschluesst_kommunizieren_node.html))



# Sichere Netze... ?

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

---

01100101 01100001  
01100110 01110100  
011**B1G D0T0**0000  
101**F0R** 01001000  
011**B0ND 2.0**11101  
01101110 01110011  
01100110 01110100  
10101010 01010101  
01111010

---

# Fazit: Die Wolke Sieben – Cloud liegt ziemlich nah am Wolkenkuckucksheim

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen



# ... um nicht aus allen Wolken zu fallen

Die Landesbeauftragte  
für Datenschutz und  
Informationsfreiheit



Freie  
Hansestadt  
Bremen

- Was ist zu klären?
  - Das Ob
  - Das Wie
    - Anbietersauswahl
    - Steuerung
    - Kontrolle

→ Orientierungshilfe Cloud Computing Version 2.0,  
Entscheidung der Datenschutzkonferenz vom 9.10.2014

[www.datenschutz.bremen](http://www.datenschutz.bremen) unter „Aktuelles“ oder

→ <https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen02.c.730.de>





---

**Vielen Dank für die Aufmerksamkeit !**

**Gibt es noch Fragen an mich?**

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Dr. Imke Sommer

Arndtstraße 1

27570 Bremerhaven

Tel. 0421/ 361-2010

E-Mail: [office@datenschutz.bremen.de](mailto:office@datenschutz.bremen.de)

[www.datenschutz.bremen.de](http://www.datenschutz.bremen.de)