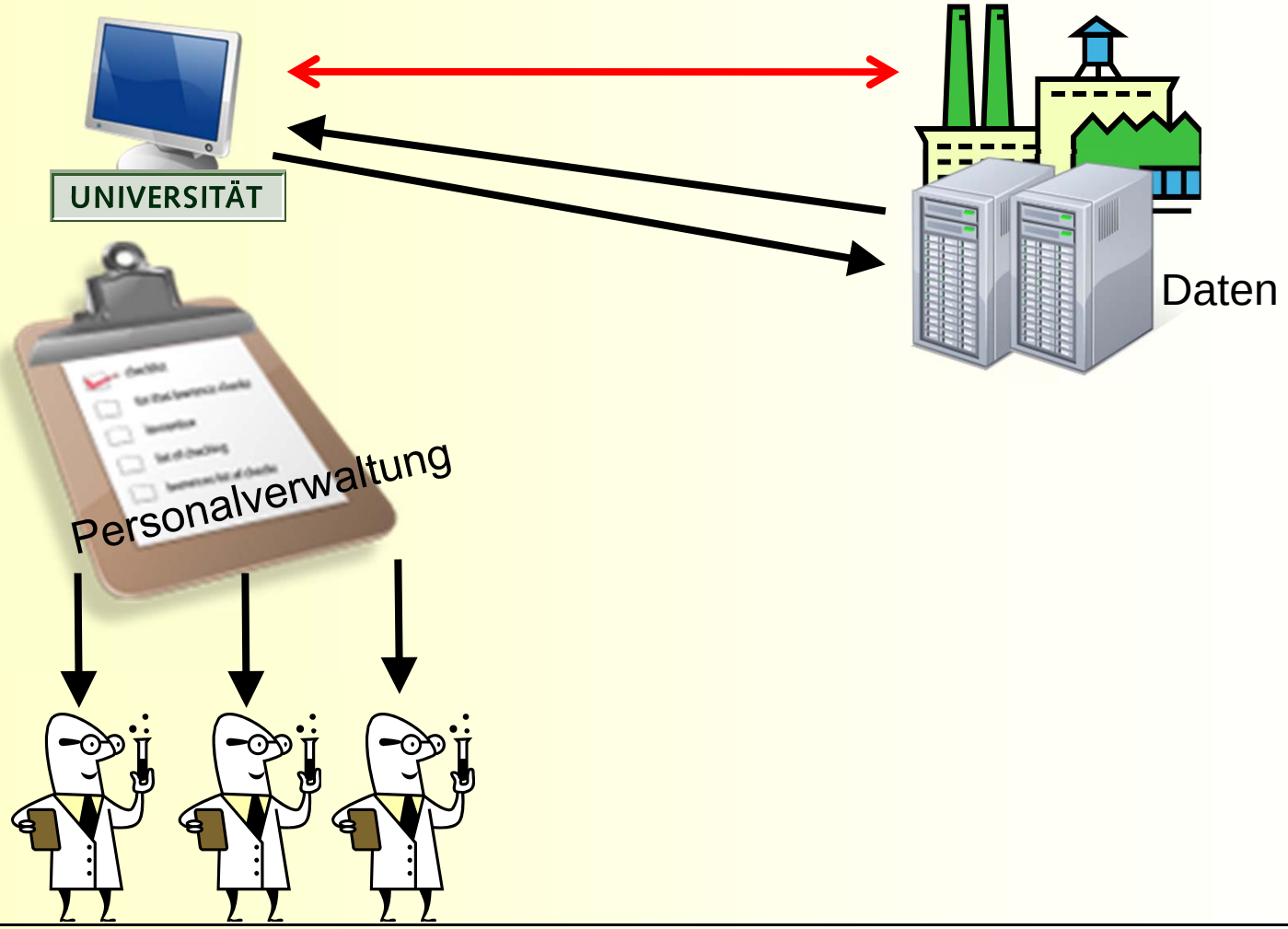
Die Kehrseite der Einschaltung von Dienstleistern:

Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag

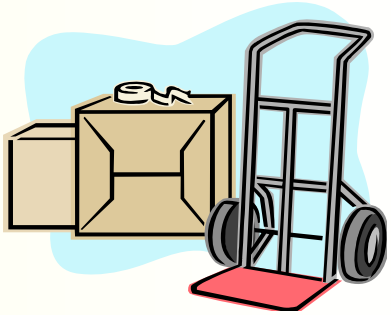


Kennzeichen der Datenverarbeitung im Auftrag

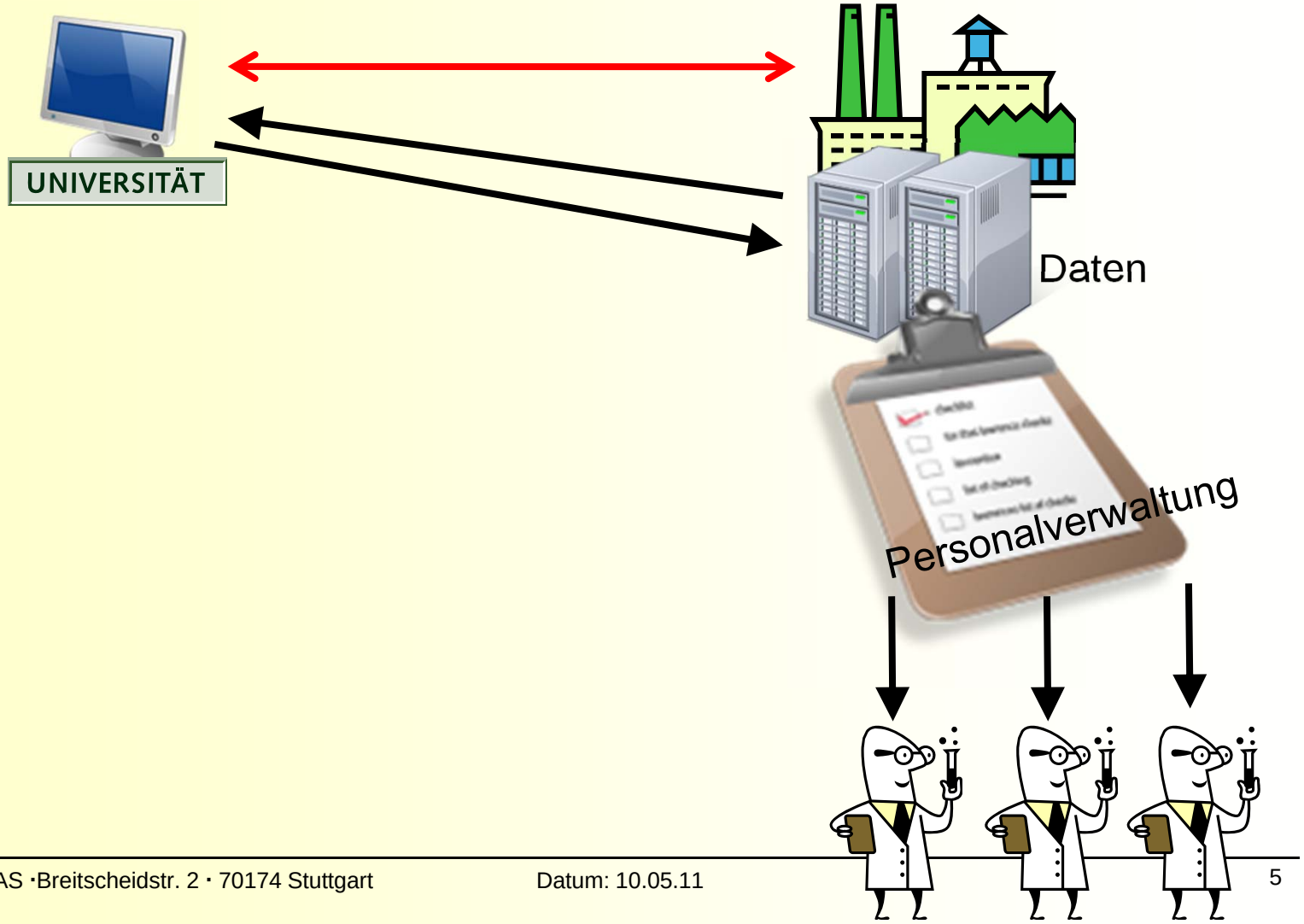
- Datenverarbeitung wird lediglich in ihrer **„Hilfsfunktion“** zur Erfüllung der Aufgabe der Universität ausgelagert.
- **Keine Aufgabenverlagerung**
- Datenverarbeiter nutzt Daten **nicht** überwiegend für **eigene Geschäftszwecke**
- Datenverarbeiter erbringt über technische Durchführung der Verarbeitung **keine materiellen vertraglichen Leistungen** mithilfe der Daten

Beispiele für Datenverarbeitung im Auftrag

- Hosting einer Software, wahlweise als Application Service Providing oder nur als Hosting (Alumni, Campus Management Software, Online-Bewerbung, etc.)
- (Managed) Homeing in einem Service-Rechenzentrum
- Einkauf von Diensten (z.B. Betrieb von E-Mailservern)
- Jegliche Form von Wartung an Systemen mit personenbezogenen Daten
- Umzug von Papierakten
- Aktenvernichtung



Abgrenzung zur Funktionsübertragung



Abgrenzung zur Funktionsübertragung

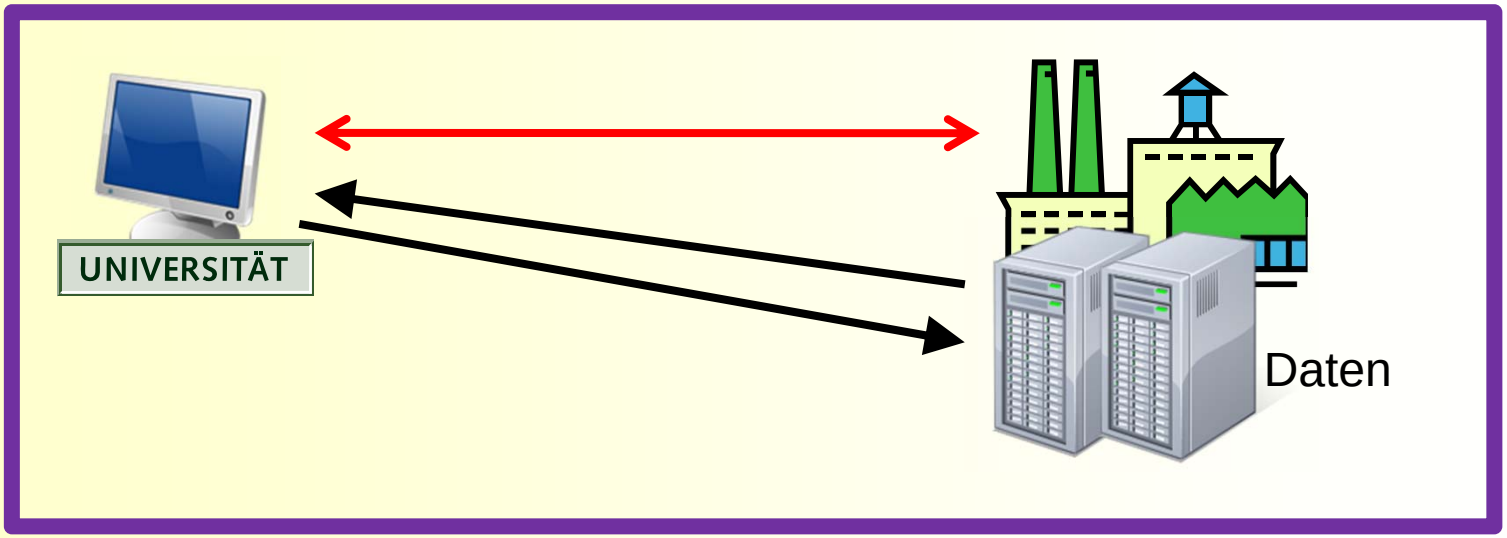
- **gesamte Aufgabe** der Hochschule wird **ausgelagert**
- Datenverarbeiter nutzt Daten ganz überwiegend für **eigene Geschäftszwecke**
- Datenverarbeiter erbringt über technische Durchführung der Verarbeitung **materielle vertragliche Leistungen** mithilfe der Daten

Beispiele für Funktionsübertragung

- Personalbuchhaltung: Übertragung an Landesamt für Besoldung und Versorgung (durch Rechtsvorschrift)

  In unserer Beratungspraxis bei der IT so gut wie keine Fälle, in der Regel liegt Datenverarbeitung im Auftrag vor

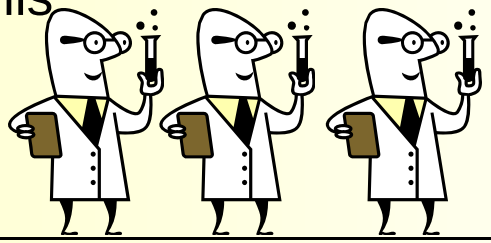
Verantwortlichkeit bei Datenverarbeitung im Auftrag



Hochschule ist verantwortliche Stelle:

- Anspruchsgegner
  (ggf. Regress im Innenverhältnis)
- Verfahrensverzeichnis

Anspruch auf Auskunft



Anforderungen an Datenverarbeitung im Auftrag

1. Sorgfältige Auswahl des Auftragnehmers
2. Schriftlicher Vertrag:
   a. Gegenstand und Umfang der DV
   b. Technische und organisatorische Maßnahmen (TOMs)
   c. (etwaige) Unterauftragsverhältnisse
   d. z.T. Weisungsrecht des Auftraggebers
   e. z.T. Unterwerfung des Auftragnehmers unter Kontrolle der Datenschutzaufsichtsbehörde der Hochschule
3. (Regelmäßige) Kontrolle der Einhaltung der TOMs

Alle Bundesländer haben entsprechende Regelungen in ihren Datenschutzgesetzen!

Sorgfältige Auswahl des Auftragnehmers

- **Datenschutz- und Datensicherheitskonzept vorlegen lassen**
  (Verweigerung aus Sicherheitsgründen nicht akzeptabel)
- bei Hosting, Fernwartung u.ä.:
  nach Vertrag hinsichtlich Auftragsdatenverarbeitung fragen
  (aber nicht ungeprüft unterschreiben)
- AGBs prüfen!
- Auftragnehmer muss innerhalb EU/EWR seinen Sitz haben
- möglichst **vor Vertragsschluss Software prüfen** (lassen)

Nicht zu früh auf einen Anbieter festlegen, alternative Anbieter im Auge behalten!

Sorgfältige Auswahl des Auftragnehmers (Software)

- allgemeines **Berechtigungskonzept** erstellen:

  ➡ WER soll mit der Software WIE arbeiten?

  ➡ Grundlage für Bewertung: Kann die Software das Berechtigungskonzept überhaupt abbilden?

- Wer ist verantwortlich für das Einspielen von Updates? (Betriebssystem, Webserver, Web-Anwendung)

Sorgfältige Auswahl des Auftragnehmers (Software)

Anforderung in Leistungsbeschreibung

(Pflichtenheft, Ausschreibung …):

➡ **Software muss hinsichtlich Datensicherheit dem aktuellen Stand der Technik entsprechen**!

dabei z.B. Orientierung am BSI (siehe folgende Folie)

Vertraglich regeln:

Maßnahmen des Herstellers, die der **Beseitigung von Sicherheitsmängeln** dienen, sind **kostenfrei und haben unverzüglich** (Zeiten definieren!) zu erfolgen.

Sorgfältige Auswahl des Auftragnehmers (Software)

BSI-Standard zur Internet-Sicherheit (ISi-Reihe)

Modul „Sicheres Bereitstellen von Web-Angeboten“

https://www.bsi.bund.de/cln_165/ContentBSI/Themen/Internet_Sicherheit/WWW/Webserver/Dokumente/isi-web-server-doc.html

- lassen Sie sich zumindest die „Produktunabhängige Checkliste“ ausfüllen
- Webanwendungen sollten die in „Sicherheit von Webanwendungen: Maßnahmenkatalog und Best Practices“ gestellten Anforderungen erfüllen

Sorgfältige Auswahl des Auftragnehmers

- **Bitte daran denken:**
  Einschaltung von Dienstleistern mag später eigene Ressourcen sparen, vor Vertragsschluss sind jedoch einige zu investieren (Zeitfaktor nicht unterschätzen!).

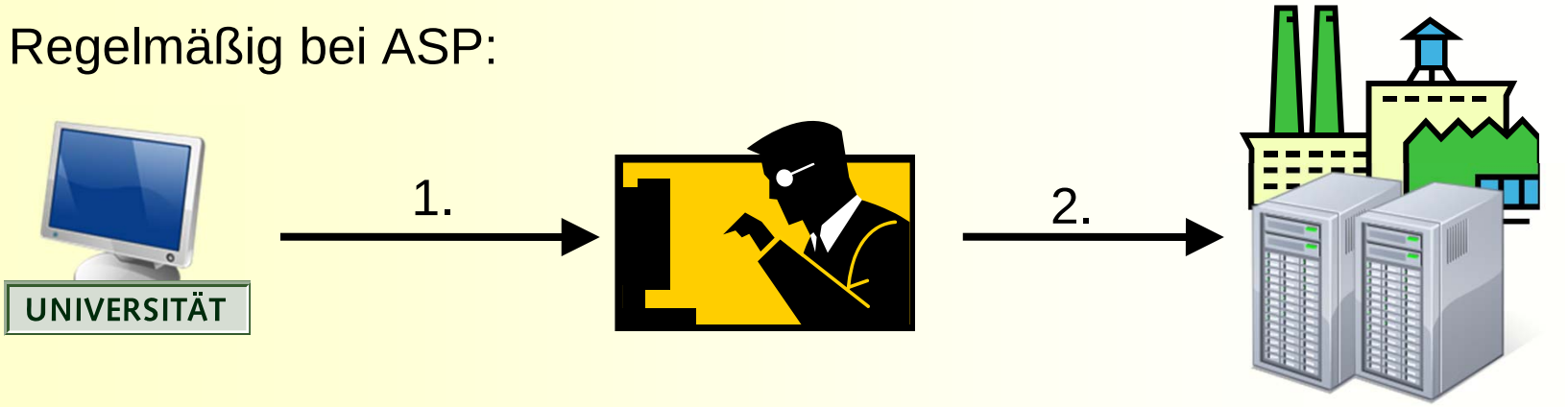
- **Datenschutzbeauftragten** o.a. Stelle mit Kompetenz in Sachen Datenschutz und Datensicherheit **frühzeitig hinzuziehen**

Schriftlicher Vertrag - Muster

- Vertragsmuster auf den **Internetseiten** der zuständigen Datenschutzaufsicht
- Beachten: Vertrag für **öffentliche Stellen** als Auftraggeber (nicht für nicht-öffentliche Stellen)!
- Vertrag nicht einfach übernehmen, Muster bedürfen immer der **Anpassung**
- Muster der Auftragnehmer basieren meist auf BDSG, Hochschule braucht eines, das auf **Landesdatenschutz** basiert

Schriftlicher Vertrag - Unterauftragsverhältnisse

Regelmäßig bei ASP:

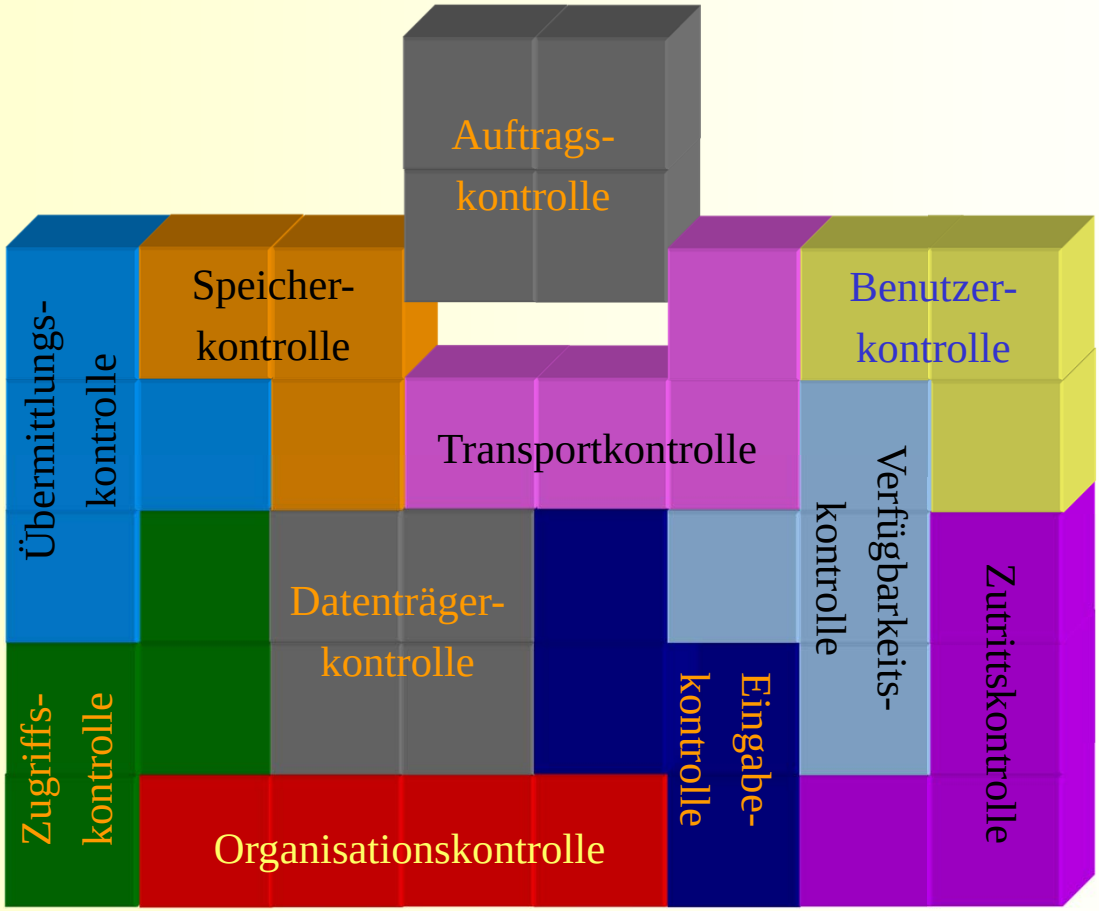


1. Vertrag über Auftragsdatenverarbeitung nach DSG des Landes mit gestattetem Unterauftragsverhältnis
2. Vertrag über Auftragsdatenverarbeitung nach § 11 BDSG

Schriftlicher Vertrag - Unterauftragsverhältnisse

- Grundsätzlich Unterauftragsverhältnisse **ausschließen**.
- Wenn von vorneherein notwendig: **Vertrag** nach § 11 BDSG **vorlegen lassen** (im Rahmen der sorgfältigen Auswahl des Auftragnehmers)
- Im Vertrag mit dem Auftragnehmer festlegen, dass die **vertraglichen Regelungen** auch gegenüber **Unterauftragnehmern** gelten.
- Auftragnehmer/Unterauftragnehmer, der die Daten in der **Cloud** hält, ist grundsätzlich **nicht akzeptabel** (die verantwortliche Stelle muss stets wissen, wo ihre Daten sind).

Schriftlicher Vertrag - TOMs



Weitere Infos

ZENDAS Info-Server:

- **Seite „Sicherheit von Web-Applikationen“**
  http://www.zendas.de/themen/server/www/sicherheit/index.html
- **Seite „Datenverarbeitung im Auftrag - Allgemeine Hinweise“**
  http://www.zendas.de/service/auftragsdatenverarbeitung/hinweise.html

BSI (Bundesamt für Sicherheit in der Informationstechnik):

- „**Sicherheit von Webanwendungen**.
  Maßnahmenkatalog und Best Practices“
- **Checklisten** „Produktabhängige Checkliste“

beides unter:

https://www.bsi.bund.de/cln_165/ContentBSI/Themen/Internet_Sicherheit/WWW/Webserver/Dokumente/isi-web-server-doc.html

Fragen oder Anmerkungen zu diesem Thema?