

# **Cloud Computing nach der DSGVO**

Modul 346, BBZW

---

Patrick Bucher

Auf manchen Folien befinden sich Verweise auf die jeweils relevanten Kapitel (z.B. **[K3]** für “Kapitel 3”), die in der Zusammenfassung nachgeschlagen werden können.



**Abbildung 1:** Cloud Computing nach der Datenschutz-Grundverordnung

Diese Folien enthalten keine belastbaren rechtlichen Ratschläge.

Bei Fragen zum Datenschutz wenden Sie sich an den **Datenschutzbeauftragten** Ihres Lehrbetriebs!

## *GDPR: General Data Protection Regulation*

- EU-weite Datenschutzregelung
- am 25. Mai 2018 in Kraft getreten
- soll Schutz personenbezogene Daten gewährleisten
- soll Europa “Cloud-freundlich” machen
- [Gesetzestext](#)

Beim Cloud Computing werden Daten **grenzübergreifend** verarbeitet.

Der Datenschutz ist jedoch **länderspezifisch** geregelt.

Wie kann ich personenbezogene Daten datenschutzkonform in der Cloud verarbeiten?

## Ziel

- bewahrt die Freiheit natürlicher Personen, selbst über den Umgang ihrer personenbezogenen Daten zu entscheiden
- schützt das Recht auf informationelle Selbstbestimmung

## Gegenstand

- personenbezogene Daten: Informationen, die sich auf eine Person beziehen und diese **identifizierbar** machen
- Verarbeitung: Erhebung, Speicherung, Übermittlung, Nutzung, Löschung

## Grundsatz

- Verbot mit Erlaubnisvorbehalt: Die Verarbeitung ist verboten, wenn sie nicht explizit erlaubt ist (*Erlaubnistatbestand*)

- **Rechtmässigkeit:** z.B. durch Einwilligung des Betroffenen (Erlaubnistatbestände)
- **Treu und Glauben:** die betroffene Person wurde über die Verarbeitung informiert
- **Transparenz:** Zweck der Datenverarbeitung sind für Betroffene nachvollziehbar
- **Zweckbindung:** Daten werden nur für festgelegte Zwecke verarbeitet
- **Datenminimierung:** nur nötige Daten werden verarbeitet (Verhältnismässigkeit)
- **Richtigkeit:** Daten sind aktuell zu halten; alte Daten zu berichtigen oder löschen
- **Speicherbegrenzung:** Daten nur so lange aufbewahren wie für den Zweck nötig
- **Integrität und Vertraulichkeit:** Gewährleistung angemessener Datensicherheit
- **Rechenschaftspflicht:** Dokumentation der Verarbeitung zwecks Nachweis

## Akteure (gemäß DSGVO) [K3]

- **betroffene Person** (*Data Subject*): eine natürliche Person, die über schützenswerte personenbezogene Daten verfügt
- **Verantwortlicher** (*Controller*): natürliche/juristische Person, die über Zweck und Mittel einer Datenverarbeitung entscheidet
- **Auftragsverarbeiter** (*Processor*): Dienstleister, der personenbezogene Daten im Auftrag eines Verantwortlichen übernimmt
- **Dritte** (*Third Party*): Aussenstehende, die nicht in die Verarbeitung eingebunden sind
- **Empfänger** (*Recipient*): jeder, dem personenbezogene Daten offengelegt werden
- **Datenschutzbeauftragter** (*Data Protection Officer*): Ansprechpartner für Datenschutzfragen in einer Organisation
- **Aufsichtsbehörde** (*Supervisory Authority*): staatliche Stelle, welche die Einhaltung der DSGVO überwacht und durchsetzt



1. Es werden personenbezogene Daten verarbeitet.
2. Die personenbezogenen Daten werden mit Informatikmitteln verarbeitet – manuell oder (teilweise) automatisch.
3. *Marktortprinzip*: Die Verarbeitung ...
  - erfolgt durch eine Niederlassung im EU-Raum
  - betrifft Personen, die sich im EU-Raum aufhalten

siehe auch [Anwendbarkeit auf Schweizer Unternehmen](#)

### Ausnahmen

- anonymisierte (aber nicht pseudonymisierte) Daten
- Daten bereits verstorbener Personen, die sonst keine lebenden Personen betreffen
- *Haushaltsausnahme*: Verarbeitung, die zu rein privaten Zwecken stattfindet
  - z.B. Versand von Fotos einer Geburtstagsfeier in einen Gruppenchat
- *Colocation*: Einmieten in Rechenzentrum im EU-Raum ohne lokales Personal

Grundsatz: *Verbot mit Erlaubnisvorbehalt*

Ein *Erlaubnistatbestand* liegt vor bei:

- **Einwilligung:** Die betroffene Person stimmt der (widerrufbaren) Datenverarbeitung zu. Bedingungen:
  1. Freiwilligkeit: keine Zwangssituation
  2. Bestimmtheit: bestimmter Zweck der Verarbeitung
  3. Informiertheit: in klarer und verständlicher Sprache
  4. Einwilligungsbewusstsein: explizite Einwilligung (per Opt-In)
- **Vertragserfüllung:** z.B. Adressangabe nötige bei Warenversand
- **rechtliche Verpflichtung:** z.B. Aufbewahrungspflicht von Informationen
- **Wahrung berechtigter Interessen:** z.B. Weitergabe innerhalb eines Konzerns
- **Auftragsverarbeitung:** Verarbeitung im Auftrag eines Verantwortlichen

Auslagerung der Verarbeitung personenbezogener Daten an einen externen Dienstleister (den *Auftragsverarbeiter*, kurz: AV; z.B. Cloud-Provider) unter folgenden Bedingungen:

- Der Verantwortliche hat die Einwilligung der betroffenen Person zur Datenverarbeitung eingeholt.
- Der AV richtet sich nach dem Verantwortlichen, was Mittel und Zweck der Datenverarbeitung betrifft. (“Bedingungen reisen mit den Daten”)
- Der AV ist ein Empfänger der Daten und als solcher vom Verantwortlichen aufzuführen.
- Der AV darf keine personenbezogenen Daten zu eigenen Zwecken verarbeiten.
- Verantwortlicher und AV schliessen einen *Auftragsverarbeitungsvertrag* (AV-Vertrag) ab.

Bei der länderübergreifenden Datenübertragung unterscheidet man zwischen:

1. Datenübertragung innerhalb der EU (und Island/Norwegen/Liechtenstein)
  - DSGVO ist verbindlich
  - Datenübertragung ist grundsätzlich möglich
2. Datenübertragung in ein Drittland
  - sichere Drittländer mit angemessenem Datenschutzniveau: z.B. Schweiz, Japan, UK (noch?)
  - unsichere Drittländer mit unzureichendem Datenschutzniveau: z.B. USA

Der Datenzugriff aus einem Drittland (z.B. durch Supportpersonal) kommt einer Datenübertragung gleich!

## Die USA als Drittland [K12, K13]

- USA: schwach im Datenschutz, stark im Cloud-Geschäft
- **Safe-Harbor-Vereinbarung:** 2000-2015 zwischen EU und USA
  - Ziel: Abbau von Handelshemmnissen
  - basierend auf Selbstzertifizierung der US-Vertragspartner
  - Schrems-I-Urteil (EuGH): **ungültig!**
- **EU-U.S. Privacy Shield:** 2016-2020 zwischen EU und USA
  - Nachfolgeregelung von kassierter Safe-Harbor-Vereinbarung
  - wieder auf Basis von Selbstzertifizierung
  - Schrems-II-Urteil (EuGH): **ungültig!**
- **Trans-Atlantic Data Privacy and Security Framework**
  - in Ausarbeitung

Lösung: besondere Vereinbarungen (BCR) und Standardvertragklauseln (SCC)

## Datenzugriffe durch US-Behörden [K13]

- Einführung von Office 365: Microsoft kann Datenzugriff durch US-Behörden nicht ausschliessen.
- Internationaler Drogenhandel: Microsoft sollte kompletten Mailverkehr rausrücken (Daten in Irland und in den USA gehostet)
  - rückte nur US-Daten raus
  - Microsoft in 1. Instanz verurteilt, in 2. Instanz Recht bekommen
  - “Lösung”: USA führt **CLOUD-Act** ein

**CLOUD-Act:** Extraterritorialer Zugriff von US-Sicherheitsbehörden auf Tochtergesellschaften von US-Unternehmen (z.B. im EU-Raum) im Rahmen von Strafverfahren:

- steht in Konflikt mit der DSGVO
- Cloud-Anbieter in der Zwickmühle: Strafen drohen beiderseits!

## Welche Rechte haben betroffene Personen? [K14]

Eine betroffene Person, deren personenbezogene Daten verarbeitet werden, hat verschiedene Rechte. Im Cloud Computing besonders relevant sind:

1. **Recht auf Information:** Verantwortlicher informiert Betroffenen über Datenverarbeitung
  - Direkterhebung: zu eigenen Zwecken
  - Dritterhebung: zu Zwecken eines Dienstleisters (z.B. durch Google Analytics)
  - Datenschutzerklärung: Information erfolgt bei Vertragsabschluss (Bestätigung z.B. mit Checkbox)
2. **Recht auf Auskunft:** Betroffener erhält erhobene Daten
  - erste Stufe: Auskunft, ob Daten zur jeweiligen Person vorliegen
  - zweite Stufe: Herausgabe der vorliegenden Daten
  - Identitätsprüfung: zur Vermeidung unbefugter Auskünfte

## Brauchen wir einen Datenschutzbeauftragten? [K16]

Ein Datenschutzbeauftragter unterstützt die Firma in Fragen zum Datenschutz. Er muss von der Geschäftsleitung unter folgenden Bedingungen ernannt werden:

1. **Beschäftigtenzahl:** mind. 20 Personen, die an der automatischen Datenverarbeitung mitwirken
2. **Art der Daten:** es werden besonders sensible Daten wie z.B. Gesundheitsdaten verarbeitet (unabhängig der Beschäftigtenzahl)



Eine Datenschutzverletzung liegt in folgenden Fällen vor:

1. **Vernichtung:** Daten existieren nicht mehr bzw. sind nicht mehr lesbar
2. **Verlust:** Daten existieren noch, aber nicht mehr für Verantwortlichen zugänglich
3. **Veränderung:** Daten wurden durch Unbefugte verändert
4. **unbefugte Offenlegung, unbefugter Zugang:** unautorisierte Personen nehmen Daten zur Kenntnis oder können darauf zugreifen

## Was tun bei einer “Datenpanne”? [K17]

1. Datenschutzbeauftragten einbeziehen
2. Risiko für betroffene Personen einschätzen
3. Vorfall dokumentieren
4. je nach Risiko: Aufsichtsbehörde oder betroffene Personen informieren
5. Bei abgeschlossener Cybercrime-Versicherung: Versicherung informieren!
6. Bei besonders schweren Fällen: Aktivierung weiterer Behörden (z.B. Polizei)

**Notfallplan:** Vorgehen wird vor Eintreten durchgeplant (und geübt).

Die DSGVO ist kein “zahnloser Tiger”. Es drohen hohe Bussen! siehe [GDPR Enforcement Tracker](#)

Für die Höhe der Bussen werden verschiedenste Faktoren berücksichtigt:

- Schadensausmass, Anzahl Betroffener, Zeitraum
- Fahrlässigkeit, Vorsätzlichkeit, Wiederholungsfall
- Zusammenarbeit mit und Information der Aufsichtsbehörden
- Kategorien betroffener Daten

Betroffene können Anspruch auf Schadensersatz geltend machen.