Umsetzung der DS-GVO bei Cloud-Anwendungen

Herzlich willkommen! Die Themen heute:

- Was ist Cloud Computing?
- Vorteile von Cloud Computing
- Risiken und Gefahren des Cloud Computing
- Rechtsgrundlagen - Cloud Computing und Datenschutz
- Internationale Datenverarbeitung, US-Datentransfer
- Datenschutzverletzung (Data Breach)
- Empfehlungen

Cloud Computing

Was ist Cloud Computing?

Beim Cloud Computing werden dynamisch skalierbare Software- und Hardwareressourcen als Service zur Verfügung gestellt.

Dabei werden vor allem Rechenkapazität, Datenspeicher, Software- und Programmieranwendungen und andere an den Bedarf angepassten Serviceangebote über ein Netzwerk frei zur Verfügung gestellt.

Hierbei unterscheidet man zwischen SaaS (**Software as a Service**), PaaS (**Platform as a Service**) und IaaS (**Infrastructure as a Service**).

Cloud Computing

Was ist Cloud Computing?

SaaS
(Software as a Service)

Nutzung einer Softwareapplikation über das Internet
(z.B. Google Docs)

PaaS
(Platform as a Service)

Bereitstellung von Entwicklerplattformen
(z.B. Windows Azure)

IaaS
(Infrastructure as a Service)

Bereitstellung von Rechenleistung und Speicherplatz
(z.B. EC2 und S3 von Amazon)

Cloud Computing

Was ist Cloud Computing?

Geschäftsmodelle beim Cloud Computing:

- **Internal Cloud** (Zusammenschaltung von vorhandenen Systemen zur effizienteren Ressourcennutzung).
- **Hybrid Cloud** (Anmietung von zusätzlichen Ressourcen bei Bedarf).
- **External/Public Cloud** (nahezu vollständige Anmietung von Ressourcen von außen).

Cloud Computing

Vorteile von Cloud Computing

- Hohe Flexibilität.
- Einfacher Erwerb, nutzungsabhängige und transparente Kosten.
- Kostenersparnis in den Bereichen Anschaffung, Betrieb und Wartung von IT-Systemen.
- Geschäftsanwendungen jederzeit an jedem Ort verfügbar.
- Konzentration auf das Kerngeschäft besser möglich, da umständliche Logistikprobleme entfallen.

Aber Cloud Computing hat nicht nur Vorteile…

Cloud Computing

Risiken und Gefahren des Cloud Computing

- Ausfall von Internetverbindungen macht Nutzung unmöglich.
- Verletzung von bestehenden Richtlinien und Gesetzen.
- Viele einander unbekannte Nutzer nutzen ein- und dieselbe Infrastruktur.
- Verlust der Kontrolle über die Daten und Anwendungen möglich.

Cloud Computing

Risiken und Gefahren des Cloud Computing

- Zunahme von „Denial-of-Service“-Angriffen auf Cloud-Computing-Plattformen.
- Missbrauchsgefahr (Auslesen von Daten durch Nicht-Berechtigte).
- Unsichere Schnittstellen.
- hohe Komplexität kann zu Sicherheitslücken führen.
- Fehler in der Bedienung durch Mitarbeiter.
- Vendor Lock-In.

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

Cloud Computing ist eine Auftragsdatenverarbeitung im Sinne von **Art. 28 DS-GVO**.

- **Schriftlicher Auftrag** nach Art. 28 DS-GVO nötig.
- Cloud-Anbieter muss angemessene **technisch-organisatorische Maßnahmen** gem. Art. 32 DS-GVO umsetzen.
- Der Cloud-Anbieter muss den **Schutz der Rechte der Betroffenen** angemessen gewährleisten.
- Der Cloud-Kunde muss den **Cloud-Anbieter sorgfältig auswählen** (Auswahlverantwortung, Bußgeld durch Aufsichtsbehörden).

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Zertifizierung** des Cloud-Anbieters durch fachkundige und unabhängige Dritte, z. B. ISO 27001 - Zertifizierung.

- **Kontrollrechte** des Cloud-Kunden, ob der Cloud-Anbieter die personenbezogenen Daten datenschutzkonform verarbeitet, dürfen nicht ausgeschlossen werden, auch wenn die Kontrolle grundsätzlich durch die Vorlage geeigneter Zertifikate durchgeführt werden soll.

- Bei **fehlender Verlängerung des Zertifikats** und ohne Erwerb eines anderen vergleichbaren Zertifikats besteht ein Indiz dafür, dass die angebotene Cloud-Lösung keine angemessene IT-Sicherheit mehr bietet.

- **Fazit:** Cloud-Kunde muss IT-Sicherheitsmaßnahmen des Cloud-Anbieters regelmäßig prüfen und dokumentieren.

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Auftragsverarbeitungsvertrag gem. Art. 28 DS-GVO**
  - Erfordernis der Schriftlichkeit
  - Wesentliche Vertragsbestandteile
    - Gegenstand der Verarbeitung
    - Dauer der Verarbeitung
    - Zweck und Art der Verarbeitung
    - Kategorien der betroffenen Personen
    - Weisungsrecht des Cloud-Kunden (Dokumentationspflicht des Cloud-Anbieters).
    - Vertragliche Verpflichtung der zur Verarbeitung von personenbezogenen Daten befugten Personen zur Vertraulichkeit (Datengeheimnis).
    - Verpflichtung des Cloud-Anbieters zu technisch-organisatorischen Maßnahmen, um ein angemessenes Schutzniveau zu gewährleisten.

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO**
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle
  - Wiederherstellung
  - Datenintegrität (Beschädigung von Daten, Fehlfunktionen)
  - Trennungskontrolle
  - Portabilität (Recht auf Datenübertragbarkeit)
  - Anonymisierung und Pseudonymisierung von personenbezogen Daten

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Einsatz von Subunternehmern**
  - **Genehmigung von Subunternehmern** durch den Cloud-Kunden. Standardisierte Leistungsangebote bei großen Cloud-Anbietern, hier Allgemeine Geschäftsbedingungen und allgemeine schriftliche Genehmigung der Subunternehmer („take it or leave it“).
  - Allen Subunternehmern müssen **dieselben datenschutzrechtlichen Pflichten** auferlegt bekommen, wie sie zwischen Cloud-Kunde und Cloud-Anbieter geregelt sind.
  - Bei **Eingehen eines Sub-Auftragsverhältnisses** durch einen Sub-Auftragsverarbeiter müssen alle zustimmen, die in der Verarbeitungskette vor ihm stehen. Weiterreichen der datenschutzrechtlichen Pflichten bis zum letzten Subunternehmer in der Kette (kein Aufweichen der datenschutzrechtlichen Pflichten).
  - Kommt der Sub-Auftragsverarbeiter seinen datenschutzrechtlichen Pflichten nicht nach, **haftet der Cloud-Anbieter** gegenüber dem Cloud-Kunden für die Einhaltung dieser Pflichten.

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Kontroll- und Informationsrechte**
  - Cloud-Kunden ist berechtigt alle erforderlichen Dokumente und Informationen zu erhalten, die zum **Nachweis der Einhaltung der datenschutzrechtlichen Pflichten** erforderlich sind.
  - **Kontrollen durch den Cloud-Kunden** beim Cloud-Anbieter vor Ort oder Inspektionen durch beauftragte Dritte.
  - Cloud-Kunde prüft auch das **Durchreichen der datenschutzrechtlichen Pflichten** vom Cloud-Anbieter an dessen Sub-Auftragsverarbeiter.

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Betroffenenrechte gem. Art. 16 - 21 DS-GVO**
  - Pflicht des Cloud-Anbieters durch geeignete technisch-organisatorische Maßnahmen den Cloud-Kunden bei der **Beantwortung von Betroffenen-Anträgen** zu unterstützen.

  - **Betroffenenrechte** sind:
    - Recht auf Auskunft
    - Recht auf Berichtigung
    - Recht auf Löschung
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit (Portabilität)
    - Recht auf Widerspruch gegen die Verarbeitung

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Pflichten gem. Art. 32 - 36 DS-GVO**
  - Pflicht des Cloud-Anbieters den Cloud-Kunden bei der Einhaltung folgender **datenschutzrechtlicher Pflichten** zu unterstützen:
    - Ergreifung geeigneter **technisch-organisatorischer Maßnahmen**.
    - **Meldung von Datenschutzverletzungen** an die zuständige Aufsichtsbehörde für den Datenschutz und die betroffenen Personen (Achtung: 72-Stunden-Frist).
    - **Durchführung der Datenschutzfolgenabschätzung**, soweit erforderlich und ggf. Konsultation der zuständigen Aufsichtsbehörde für den Datenschutz.
- **Löschung und Rückgabe der personenbezogenen Daten**
    - **Rückgabe** der personenbezogenen Daten einschließlich der Art der Rückgabe.
    - **Löschung** der personenbezogenen Daten mit Löschnachweis.

Cloud Computing

Rechtsgrundlagen – Cloud Computing und Datenschutz

- **Weitere Inhalte des Vertrags zur Auftragsverarbeitung**
  - **Haftungsklausel** gem. Art. 82 DS-GVO. (Beachte Haftungsbeschränkung des Cloud-Anbieters im Servicevertrag!).
  - **Außerordentliches Kündigungsrecht** für den Cloud-Kunden bei schwerwiegenden Pflichtverletzungen des Cloud-Anbieters.
  - Definition des **Orts der Verarbeitung** (ausschließlich innerhalb des EWR oder Drittland).
  - **Verzeichnis von Verarbeitungstätigkeiten** dokumentiert vom Cloud-Anbieter.
  - **Regelung zur Vertraulichkeit**, insoweit keine Vertraulichkeitsvereinbarung besteht.

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Nutzung von Cloud-Anwendungen in Unternehmensgruppen**
  - **Datenübermittlung im Konzern**.
  - **Datasharing**.
  - **Matrixförmige Datenzugriffe**.

- **Datenübermittlungen in unsichere Drittstaaten außerhalb der EU**
  - **Zugriff aus unsicheren Drittstaaten** bedeutet ebenfalls eine Datenübermittlung.
  - **Sichere Datenempfänger** sind Unternehmen innerhalb der EU.
  - **Außerhalb der EU** lokalisierte Unternehmen sind unsichere Datenempfänger.
  - Schaffung eines **einheitlichen Schutzniveaus** im Rahmen eines internationalen Datentransfers erforderlich.

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Datenübermittlungen in Drittstaaten**
  - **Zweistufen-Prüfung** ist vor dem geplanten Drittstaaten-Transfer durchzuführen:
    - Prüfung, ob die **Zulässigkeit der Datenverarbeitung als solche** sicherzustellen ist.
    - Prüfung, ob die **Voraussetzungen für eine Übermittlung ins Drittland** vorliegen.

  - Wie bei Sub-Auftragsverarbeitung ist der Verantwortliche für **etwaige weitere Weiterübermittlungen** durch den Cloud-Anbieter verantwortlich.

  - **Angemessenheitsbeschluss** der Europäischen Kommission für folgende Länder:
    - Canada, Argentinien, Israel, Uruguay, Neuseeland, Schweiz, Japan, Jersey, Faröer-Inseln.
    - **Rechtsfolge** des Angemessenheitsbeschlusses ist, dass der Datentransfer in dieses Land einem **Datentransfer in einen EU-Mitgliedsstaat gleichgestellt** ist (Vertrag zur Auftragsverarbeitung reicht aus).

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Geeignete Garantien gem. Art. 45 DS-GVO**
  - Falls **kein Angemessenheitsbeschluss** der Europäischen Kommission für den Daten-Empfänger (Data Importer) vorliegt, müssen Verantwortliche (Data Exporter) **geeignete Garantien** vorsehen, um ein angemessenes Datenschutzniveau zu gewährleisten.

  - **Geeignete Garantien** sind:
    - Standarddatenschutzklauseln.
    - Genehmigungspflichtiger Vertrag (Ad-hoc-Vertrag).
    - Verbindliche unternehmensinterne Datenschutzvorschriften (BCR).

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Standarddatenschutzklauseln**
  - Controller to Processor (C2P) - Verantwortlicher zu Datenverarbeiter.
  - Controller to Controller (C2C) - Verantwortlicher zu Verantwortlicher.

  - **Einsatz der Standarddatenschutzklauseln** für den Transfer personenbezogener Daten in den Drittstaat ohne das Erfordernis einer zusätzlichen Genehmigung möglich.

  - Die **Standarddatenschutzklauseln** dürfen in ihrem **Wortlaut nicht verändert** werden, können jedoch in einen Gesamtvertrag eingebettet werden (Intra-Group-Agreement).

  - Der Gesamtvertrag darf die **Standarddatenschutzklauseln nicht kontakarieren**!

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Standarddatenschutzklauseln**
  - Controller to Processor (C2P) - Verantwortlicher zu Datenverarbeiter.
  - Controller to Controller (C2C) - Verantwortlicher zu Verantwortlicher.

  - **Einsatz der Standarddatenschutzklauseln** für den Transfer personenbezogener Daten in den Drittstaat ohne das Erfordernis einer zusätzlichen Genehmigung möglich.

  - Die **Standarddatenschutzklauseln** dürfen in ihrem **Wortlaut nicht verändert** werden, können jedoch in einen Gesamtvertrag eingebettet werden (Intra-Group-Agreement).

  - Der Gesamtvertrag darf die **Standarddatenschutzklauseln nicht kontakarieren**!

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Ad-hoc-Verträge gem. Art. 46 Abs. 3 lit. a DS-GVO**
  - Ad-hoc-Verträge sind geeignete Garantien für die Übermittlung personenbezogener Daten in Drittstaaten.
  - Ad-hoc-Verträge sind vorab **genehmigungspflichtig**. Die Aufsichtsbehörden für den Datenschutz haben hier eine **Prüfungspflicht**.
  - Ad-hoc-Verträge müssen bestimmten datenschutzrechtlichen Voraussetzungen gerecht werden. Es muss detailliert dargelegt werden, wie der Datenempfänger im Drittstaat den **Grundsätzen der DS-GVO** gerecht wird. Individuelle Gestaltbarkeit möglich.
  - Das **Genehmigungsverfahren** erfolgt nicht nur durch nationale Aufsichtsbehörden. Gem. Art. 46 Abs. 4 DS-GVO muss die zuständige Aufsichtsbehörde das **Kohärenzverfahren** gem. Art. 63 DS-GVO anwenden.

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Binding Corporate Rules gem. Art. 47 DS-GVO**
  - **Verbindliche unternehmensinterne Datenschutzvorschriften** (BCR‘ s) sind als geeignete Garantien für den Transfer von personenbezogenen Daten in ein Drittland anerkannt.
  - Geeignet für **große Unternehmensgruppen**. Hier ist ein Eingehen auf die **individuellen Bedürfnisse** der Unternehmensgruppe möglich.
  - Verbindliche unternehmensinterne Datenschutzvorschriften sind **genehmigungspflichtig**. Das Genehmigungsverfahren und der Mindest-Regelungsgehalt von BCR‘ s ist geregelt in Art. 47 Abs. 1 DS-GVO.
    Die **Genehmigung** erfolgt durch die **zuständige Aufsichtsbehörde** im Rahmen eines **Kohärenzverfahrens**.
  - Schaffung einheitlicher unternehmensinterner **Datenschutzstandards**.

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **US-Datentransfer**
  - Weitere **Angemessenheitsentscheidung** der Europäischen Kommission für den Transfer von personenbezogenen Daten in die USA ist das **EU-US-Privacy-Shield**.
  - Für das EU-US-Privacy-Shield ist **keine Genehmigung** der Aufsichtsbehörden erforderlich.
  - Zusicherung seitens der USA zur Einrichtung eines **Ombudsmannverfahrens.**
  - Schreiben zur **rechtsstaatlichen Geheimdiensttätigkeit** seitens des Geheimdienstes.
  - Einhaltung der **Privacy-Shield-Principles**. Diese stellen ein eigenes Regelwerk für den EU-US-Datentransfer dar.
  - Abschluss eines **zusätzlichen Vertrags zur Auftragsverarbeitung**, wenn ein in den USA gelegener Auftragsverarbeiter beteiligt ist.

Cloud Computing

Internationale Datenverarbeitung, US-Datentransfer

- **Cloud-Act (Clarifying Lawful Overseas Use of Data Act)**
  - **Zugriffe** auf personenbezogene Daten, die innerhalb und **außerhalb der USA** gespeichert sind, durch **US-Ermittlungsbehörden** wurden durch den US-Gesetzgeber gebilligt.
  - **Auskunftsverfahren**, mit denen US-Ermittlungsbehörden an anderen Staaten vorbeinavigieren kann. Konfrontation anderer Staaten mit einem **Durchsuchungsbefehl von US-Behörden**.
  - Bestimmungen des **Cloud-Acts** stehen **Widerspruch mit Art. 48 DS-GVO**.
  - DS-GVO bezieht sich auf in Kraft **befindliche verbindliche internationale Übereinkünfte**, z. B. Rechtshilfeabkommen. Eine Regelung dazu fehlt im Cloud-Act.
  - Cloud-Act schwer mit den **Grundprinzipien des EU-US-Privacy-Shields** in Einklang zu bringen.

Cloud Computing

Data Breach

- **Data Breach (Datenschutzverletzung) gem. Art. 33, 34 DS-GVO**
  - Datenschutzverletzung ist jegliche Verletzung des Schutzes personenbezogener Daten. Erfasst ist jegliche **Verletzung der Sicherheit**, die zur **Vernichtung, Verlust, zu einer unbefugten Veränderung, Offenlegung oder Zugriff** durch einen Nicht-Berechtigten führen.

  - **Schnelle Meldung** an die zuständige Aufsichtsbehörde für den Datenschutz frühestmöglich, jedoch innerhalb von **72 Stunden** nach Kenntnis der meldepflichtigen Ereignisses.

  - **Information an die von der Datenschutzverletzung betroffenen Personen** mit Hinweisen zur Behebung der Verletzung und zur Minderung der aus der Verletzung entstehenden Folgen.

Cloud Computing

Data Breach

- **Zusammenarbeit mit dem Cloud-Anbieter**
  - **Unverzügliche Information des Cloud-Kunden** durch den Cloud-Anbieter bei Feststellung einer Datenschutzverletzung gem. Art. 33 Abs. 2 DS-GVO.
  - **24/7-Verfügbarkeit von Kontaktinformationen** auf beiden Seiten (Cloud-Kunde -Cloud-Anbieter).
  - **Strukturierter Meldeweg des Cloud-Anbieters** an den Cloud-Kunden bei einer erkannten Sicherheitsverletzung (Formular zur Meldung).
  - **Wechselseitige Gewährleistung durchgehender Kontaktaufnahme** nach Mitteilung einer Sicherheitsverletzung durch den Cloud-Anbieter.
  - **Durchgehendes Eskalationsmanagement** auf der Seite des Cloud-Kunden. Alle von der Sicherheitsverletzung betroffenen Fachabteilungen, z. B. IT, Recht, HR Marketing und Vertrieb, müssen eingebunden werden.

Cloud Computing

Empfehlungen

- Bestimmen Sie vorab, welche Art von Daten Sie im Rahmen der Nutzung einer Cloud an den Dienstleister weitergeben!

- Lesen Sie in jedem Falle die AGB‘ s und Nutzungsbedingungen der Cloud-Anbieter genau! Viele US-amerikanische Anbieter behalten sich das Recht vor, Daten im Rahmen der Durchführung des Dienstleistungsverhältnisses zu verwenden, zu ändern, zu speichern, zu kopieren, zu vertreiben (!) und zu veröffentlichen (!).

- Informieren Sie sich vorab über den Standort des Cloud-Anbieters und der Administratoren! Diese sollten immer innerhalb der EU - idealerweise in Deutschland - liegen!

- Vermeiden Sie die Inanspruchnahme von Dienstleistern in Drittstaaten. Falls sich dies nicht umgehen lässt, schaffen Sie geeignete Garantien für den Transfer von personenbezogenen Daten in den Drittstaat.

- Laden Sie nur verschlüsselte Daten in eine Cloud!

Cloud Computing

Empfehlungen

- Schließen Sie in jedem Fall die gesetzlich vorgeschriebenen Verträge im Rahmen der Cloud-Nutzung ab (AV-Vereinbarung, EU-Standarddatenschutzklauseln etc.)!
- Klären Sie vorab die Haftungsbedingungen und achten Sie insbesondere auf die Vermeidung eines Zurückbehaltungsrechts der Daten für den Cloudanbieter!
- Bestehen Sie auf ein Kontrollrecht bzgl. der Umsetzung abgestimmter Sicherheitsmaßnahmen durch den Cloudanbieter! Lassen Sie sich aktuelle und aussagekräftige Nachweise (Zertifikate etc.) für entsprechende Informations- und Datensicherheit vorlegen!
- Bestehen Sie auf offene, transparente und detaillierte Informationen des Cloud-Anbieters über technische, organisatorische und rechtliche Rahmenbedingungen einschließlich der Sicherheitskonzeption!
- Klären Sie vorab Beziehungen des Anbieters mit Subunternehmen!

Cloud Computing

Fazit

- Cloud Computing birgt datenschutzrechtlich erhebliche Risiken, denen mit entsprechenden Verträgen entgegengewirkt werden muss!
- Immer die geltenden Datenschutzgesetze beachten und in Verträgen berücksichtigen!
- Subunternehmen stets vertraglich berücksichtigen!
- Cloud-Anbieter sind vom Cloud-Kunden sorgfältig auszusuchen!
- Cloud-Anbieter sollten im eigenen Interesse nach hoher Transparenz sowie der Umsetzung und Einhaltung der Datenschutzgesetze streben!

Fragen

- Wenn Sie weitere Fragen zu diesem Thema haben, wenden Sie sich gerne an

Rechtsanwaltskanzlei Costard
Kanzlei für IT-Recht & Datenschutz
Rechtsanwalt Thomas Costard
EUROCOM Businesspark
Lina-Ammon-Straße 9
90471 Nürnberg
Tel : 0911/790 30 34
E-Mail: costard@it-rechtsberater.de