Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Cloud Computing rechtlich sicher

Cebit 2014

Rechtsanwalt Thomas Feil

Vorstellung

Feil Rechtsanwaltsgesellschaft mbH

Beratung mit Erfahrung u.a. in den Bereichen

- IT- Verträge/ IT- Projekte
- IT- Sicherheit
- Datenschutz (auch als externer Datenschutzbeauftragter)
- Wettbewerbs-, Urheber- und Markenrecht
- Vergabeverfahren
- Arbeitsrecht

Definition

Wikipedia zu „Cloud Computing“ (sinngemäß)

Cloud Computing bzw. **Rechnerwolke** ist primär der Ansatz, abstrahierte IT-Infrastrukturen (z. B. Rechenkapazität, Datenspeicher, Netzwerkkapazitäten oder auch fertige Software) dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen. Die Verarbeitung der Daten durch Anwendungen verblasst somit für den Nutzer gewissermaßen in einer „Wolke“, undurchsichtig und verhüllt.

Erscheinungsformen

- Vielzahl unterschiedlicher Cloud Computing-Produkte
- wesentliche Merkmale
  - zeitnahe Zurverfügungstellung, mit „geringem administrativen Aufwand“ [as a Service]
  - von Ressourcen im jeweils benötigten Umfang [elastic scaling]
  - über das Internet bzw. Internettechnologien, also ortsunabhängig (aber damit auch ohne tatsächliche Kontrolloption für den eigentlich Verantwortlichen)
  - auf Anforderung des Kunden [on demand]

Erscheinungsformen

- Infrastructure as a Service

Zurverfügungstellung von Rechenleistung und Speicherplatz auf Nachfrage („on demand“)

Keine Notwendigkeit zur Anschaffung und Vorhaltung von Hardware für rechenleistungs- oder speicherplatzintensive Spitzenzeiten

- Plattform as a Service

Kunden werden Plattformen angeboten, z.B. Software-Entwicklungsplattformen

- Software as a Service

Nutzung von Software auf Infrastruktur des Anbieters, ohne Installation von Software auf Rechner des Kunden; Parallelen zum ASP

- Business Process as a Service

Beispiele: Management von Kundenbeziehungen (CRM-Lösungen, HR-Planung oder Ressourcenplanung)

Bündelung verschiedener Leistungen

- Bündelung mehrerer IT-Leistungen aaS ist möglich
- Bündelung durch einen Anbieter oder Netzwerk von Anbietern innerhalb der Wolke möglich
- trennscharfe Abgrenzungen der verschiedenen Modelle oft nicht möglich

Private Cloud

- Private Cloud bezeichnet eine standardisierte und sichere IT-Umgebung, die von einem Benutzerunternehmen – hinter der Firewall – betrieben wird und ausschließlich Mitarbeitern oder Partnern dieses Unternehmens zur Verfügung steht.
- Die Dienste in der Private Cloud werden üblicherweise an die Geschäftsprozesse des Benutzerunternehmens angepasst.
- Ausschließlich autorisierte Benutzer – Mitarbeiter, Geschäftspartner, Kunden und Lieferanten – greifen auf die Dienste zu, und zwar via Intranet beziehungsweise, wenn sie sich außerhalb des Unternehmens befinden, über ein Virtual Private Network (VPN). Werden dabei Ressourcen extern durch einen 3rd-Party Service Provider (zum Beispiel Hoster, Outsourcer) gehostet, bezeichnet man dies als „Hosted Private Cloud“.

Public Cloud

- Public Cloud bezeichnet eine IT-Umgebung, die von einem IT-Dienstleister betrieben wird.

- Die Kunden (Privatpersonen und Unternehmen) greifen via Internet auf die Ressourcen zu und teilen sich eine virtualisierte Infrastruktur.

- Die Public Cloud stellt eine Auswahl von Geschäftsprozess-, Anwendungs- und/oder Infrastrukturservices auf einer variablen, nutzungsabhängigen Basis bereit.

Hybrid Cloud

- Hybrid Cloud ist eine Mischform aus Private Cloud, Public Cloud und traditioneller IT-Umgebung, denn in der Realität werden auf absehbare Zeit überwiegend Mischformen (Hybrid Clouds) genutzt. In Hybrid Clouds finden sich jeweils unterschiedliche Grade der Nutzungskombination von Private Clouds, Public Clouds und traditioneller IT-Umgebung.

  - Beispiel: Ein Unternehmen betreibt einen Webshop mit eigenen Servern, die zum Teil im eigenen Rechenzentrum, zum Teil bei einem Hoster betrieben werden. Für Nachfragespitzen, etwa im Saisongeschäft, werden Ressourcen aus einer Public Cloud hinzugebucht.

Und wie sehen Juristen die Cloud?

Problematisch…

- Juristen suchen die Einordnung in bekannte „Vertragsmodelle“ des BGB
  - Kaufvertrag
  - Werkvertrag
  - Dienstvertrag
  - Mietvertrag
  - ?

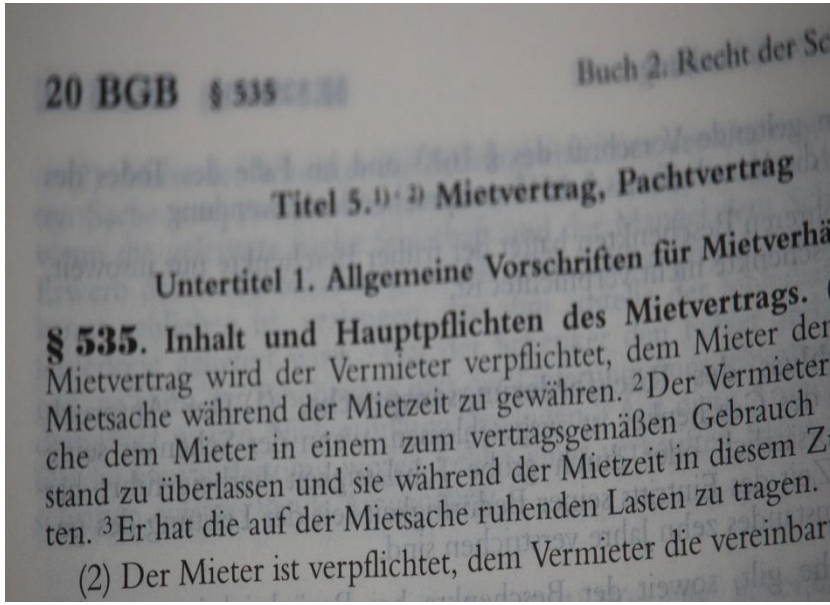
. . . Eines davon muss es doch sein!

Verträge ähneln oftmals Mietverträgen…

§ 535 BGB - Inhalt und Hauptpflichten des Mietvertrags

(1) Durch den Mietvertrag wird der Vermieter verpflichtet, dem Mieter den Gebrauch der Mietsache während der Mietzeit zu gewähren. Der Vermieter hat die Mietsache dem Mieter in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu überlassen und sie während der Mietzeit in diesem Zustand zu erhalten. Er hat die auf der Mietsache ruhenden Lasten zu tragen.

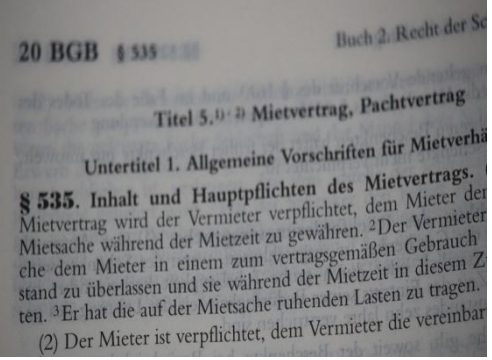
(2) Der Mieter ist verpflichtet, dem Vermieter die vereinbarte Miete zu entrichten.


20 BGB § 535 Buch 2. Recht der Sc

Titel 5. Mietvertrag, Pachtvertrag

Untertitel 1. Allgemeine Vorschriften für Mietverhä

§ 535. Inhalt und Hauptpflichten des Mietvertrags.
Mietvertrag wird der Vermieter verpflichtet, dem Mieter der
Mietsache während der Mietzeit zu gewähren. [2]Der Vermieter
che dem Mieter in einem zum vertragsgemäßen Gebrauch
stand zu überlassen und sie während der Mietzeit in diesem Z
ten. [3]Er hat die auf der Mietsache ruhenden Lasten zu tragen.
(2) Der Mieter ist verpflichtet, dem Vermieter die vereinbar


20 BGB § 535 Buch 2. Recht der Sc

Titel 5. Mietvertrag, Pachtvertrag

Untertitel 1. Allgemeine Vorschriften für Mietverhä

§ 535. Inhalt und Hauptpflichten des Mietvertrags.

Mietvertrag wird der Vermieter verpflichtet, dem Mieter der Mietsache während der Mietzeit zu gewähren. 2Der Vermieter che dem Mieter in einem zum vertragsgemäßen Gebrauch stand zu überlassen und sie während der Mietzeit in diesem Z ten. 3Er hat die auf der Mietsache ruhenden Lasten zu tragen.

(2) Der Mieter ist verpflichtet, dem Vermieter die vereinbar

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Wie im richtigen Leben:

Nicht der Titel, sondern der Inhalt ist entscheidend!

für Cloud-Verträge gilt also:

Nicht der Titel, sondern das Leistungsportfolio ist entscheidend für die rechtliche Einordnung.

Danach bemessen sich dann auch die Rechte und Plichten aus den Gesetzen.

inhaltliche Anforderungen an die Verträge

zentrale Fragen für das Cloud Computing und hierzu zu schließende Verträge:

- Welche Risiken sehe ich im Vertragsverhältnis?
- Welche Inhalte sind mir wichtig, z.B. Vergütung, Laufzeit,…?

→ Wie kann ich die Risiken minimieren und meine Inhalte unterbringen, ohne die Flexibilität der Cloud- Anwendung zu verlieren?

Haben Sie Antworten auf diese Fragen?

- Welche Leistungen sollen erbracht werden und wie soll die Erfüllungskontrolle erfolgen?
- Welche technischen und organisatorischen Maßnahmen sorgen für den Zugriff auf Daten?
- Wie ist das Berechtigungskonzept für den Zugriff ? Wie werden unberechtigte Zugriffe ausgeschlossen?
- Welcher Typ des Cloud Computing soll vereinbart werden? Je nach Cloud-Typ sind unterschiedliche Leistungen und Überprüfungen erforderlich.
- Welche Daten und Datenmengen werden übermittelt, verarbeitet und abgerufen?
- Welche Einzelheiten zur IT-Sicherheit sind im IT-Sicherheitskonzept geregelt? Sind Zugangs- und Zugriffsabsicherungen eingerichtet?
- Sind Einzelheiten zur Passwortnutzung geregelt? Wird die Anmeldung zur Cloud protokolliert? Werden Verschlüsselungstechnologien eingesetzt und welche Qualität haben diese?
- Erfolgen Überwachungen von Firewalls und ist ein präventives Log-File-Monitoring eingerichtet? Werden sicherheitsrelevante Vorfälle, insbesondere Hackerangriffe dokumentiert ?

Sie brauchen…

... eine richtig gute Leistungsbeschreibung!

Leistungsbeschreibung

- Leistungsbeschreibung gibt detailliert Umfang und Qualität der Leistung wieder,

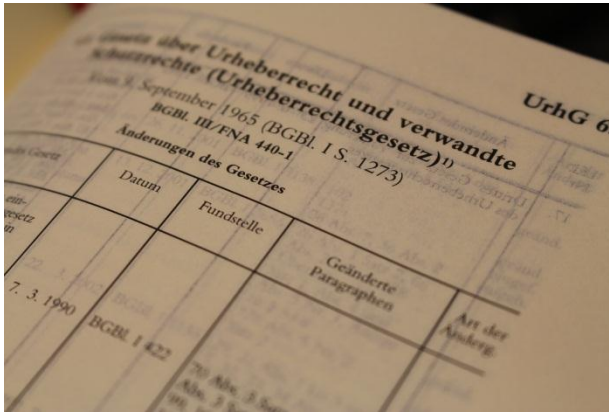
  neben den technischen Details

- Insbesondere zu regeln: Service Levels
  - Reaktionszeit (Achtung!: ≠ Wiederherstellungszeit)
  - Entstörzeit
  - Wiederherstellungszeit

weitere Inhalte der Leistungsbeschreibung

- Zugangszeiten
- Datenvolumina
- Transparenz: Wo und von wem werden die Daten tatsächlich verarbeitet?
- Definition von Standards
- Maßnahmen zur IT-Sicherheit
- Bearbeitung von Notfällen

Urheberrecht: Nutzungsrechte an der Software

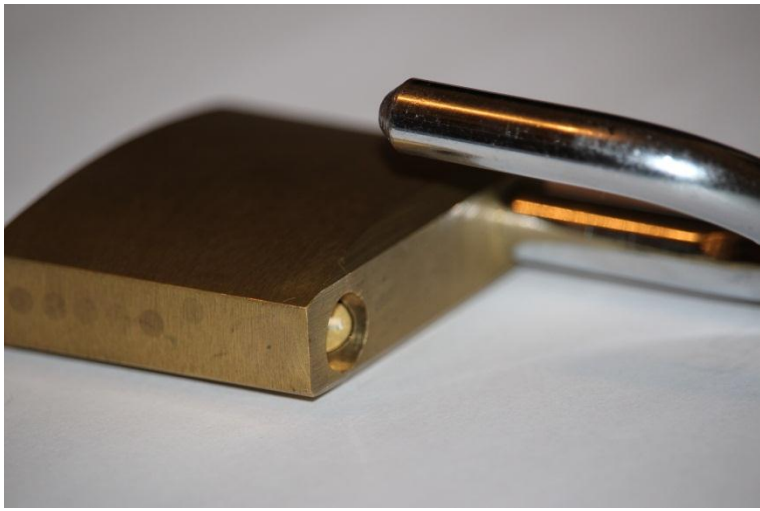


- Nutzungsrechte sind auch in der Cloud zu klären

- Grundsatz: Der Auftraggeber erhält nur die Nutzungsrechte, die er sich vertraglich gesichert hat.
  - Darf beim Kunden vorhandene Software temporär auf Rechnern des Cloud-Anbieters (und gar durch diesen) genutzt werden?
  - Welche Nutzungsrechte erwirbt der Kunde vom Anbieter?
  - Von wie vielen Arbeitsplätzen darf zeitgleich zugegriffen werden?
  - Dürfen die Nutzungsrechte auf andere Anwender übertragen werden?

Ausfallsicherheit

- Muss eine Softwarehinterlegung vereinbart werden, um bei Anbieterinsolvenz abgesichert zu sein ?
  - Was bekommt der Kunde?
- Wer haftet bei Ausfall der IT-Systeme ?
- Wer ist für das Notfallmanagement verantwortlich?



Vergütung…

… nach Gesetz?

Das BGB hält Vergütungsregelungen bereit, aber sind diese ausreichend?

- Vertrag Cloud Computing als Dienstvertrag
  - § 612 BGB: im Zweifel übliche Vergütung
- Vertrag Cloud Computing als Werkvertrag in Form eines Dauerschuldverhältnisses
  - § 632 BGB: im Zweifel übliche Vergütung
- Was gilt bei „gemischt-typischen“ Verträgen?

Subunternehmer

- Vertraglich klären, ob der Einsatz von Subunternehmer erlaubt ist.

- Wenn der Einsatz von Subunternehmer erlaubt ist, dann müssen die mit dem Generalunternehmer vereinbarten Sicherheits- und Qualitätsstandards auch vom Subunternehmer beachtet werden.
  → auch die „Weiterverpflichtung“ ist notwendig
- Audit- und Überwachungsrechte beim GU und bei den Subunternehmern (Pflicht des Auftraggebers zur Auditierung)
- Anforderungen an den Datenschutz

Change Request

- Verträge können ohne Zustimmung des Vertragspartners nicht geändert werden

- In IT-Verträgen werden häufig Prozessabläufe für ein Change Request beschrieben.
- Was ist zu beschreiben?: Ansprechpartner, Formerfordernisse, zeitliche Abläufe, Kosten…

Vertragsdauer, Kündigung

Vereinbarung einer festen Laufzeit

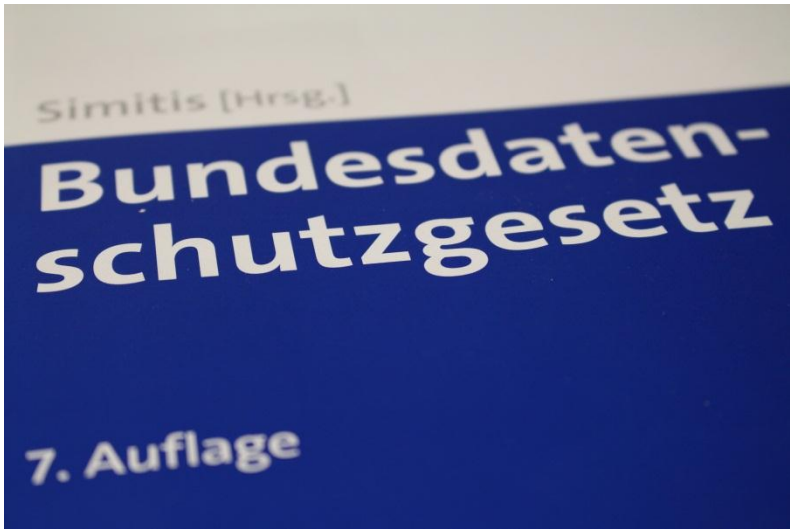
- Kündigung während der Laufzeit unzulässig, sofern keine Regelung besteht;
- Ausnahme: fristlose Kündigung

Automatische Verlängerung?

Formvorgabe für Kündigung?

Fristlose Kündigung nur nach vorheriger Abmahnung?

Datenschutz



- Was sind personenbezogene Daten ?
- Datenschutzkonzept
  - Geheimhaltungspflicht
  - Verpflichtung gemäß § 5 BDSG (Datengeheimnis)
  - Organisatorische Maßnahmen nach § 9 BDSG (Anlage zu § 9 beachten)
  - Auftragsdatenverarbeitung § 11 BDSG

Anforderung Auftragsdatenverarbeitung

Hier ist der Auftraggeber in der Pflicht!

Regelungen im BDSG

§ 11 BDSG

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder **Wartung** automatisierter Verfahren oder **von Datenverarbeitungsanlagen** durch andere Stellen im Auftrag vorgenommen wird und **dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann**.

heißt u.a.:

(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,

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.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. 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**.

Geldbußen

§ 43 BDSG - Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig 1.entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

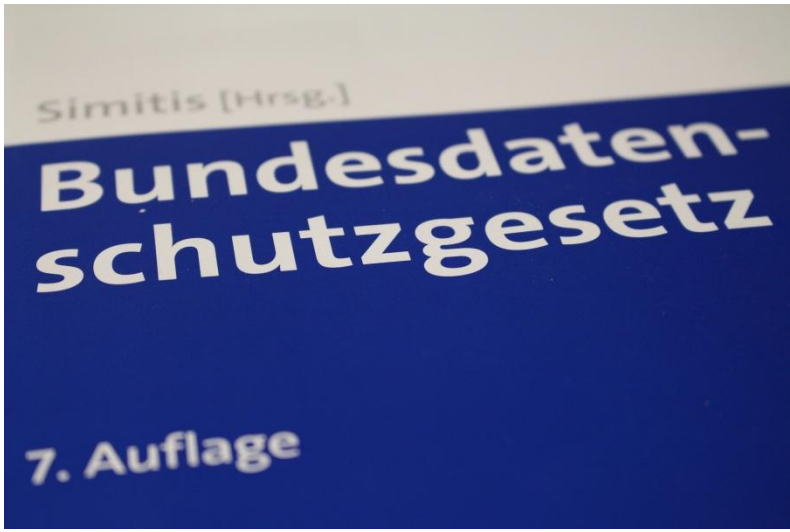
[…]

2b.entgegen § 11 Absatz 2 Satz 2 **einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt** oder entgegen § 11 Absatz 2 Satz 4 **sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,**

[…]

- (3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu **fünfzigtausend Euro**, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. **Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen.** Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

Technische und organisatorische Lösungen (TOM)



- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Daten getrennt verarbeitet werden können

Anlage (zu § 9 Satz 1 BDSG):

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
2. zu verhindern, daß Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten **getrennt verarbeitet werden können**.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Wohin gehen die Daten?

- Clouds außerhalb EU/EWR-Raum sind generell unzulässig

  > Optionsmöglichkeit der räuml. Beschränkung

- Ausnahmemöglichkeit bei festgestellter Angemessenheit des DS-Niveaus (§ 4b II 2, 3 BDSG): CH, CN

- Safe-Harbor-Selbst-Zertifzierung von US-Unternehmen genügt nicht

Geltendes Recht

- Klare Verhältnisse beim geltenden Recht notwendig
- Verweis auf deutsches Recht
- Gerichtsstand Hannover oder andere schöne Städte

Wie wirkt sich die Vereinbarung auf die Konfliktlösung aus?

Exit-Management

Wie, wann und weshalb kommt der Kunde aus dem Vertrag heraus?

Wie soll der Kunde an seine Daten kommen?

Checkliste

Fragen und Bitten an Ihren Cloud-Computing-Anbieter:

- Wo sind die Daten?
- Bitte überreichen Sie uns ein Exemplar des Datenschutzkonzeptes, des IT-Sicherheitskonzeptes und des Notfallkonzeptes.
- Wer ist der betriebliche Datenschutzbeauftragte und welche Funktion hat er im Unternehmen?
- Welche TOM nach § 9 BDSG hat das Unternehmen ergriffen? Gibt es Dokumentationen und Zertifikate?
- Welche Kontrollrechte hat ein Vertragspartner vor Ort?

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?

Rechtsanwalt Thomas Feil
Fachanwalt für Informationstechnologierecht
und Arbeitsrecht
Datenschutzschutzbeauftragter TÜV - Geschäftsführer

Döhrbruch 62 · 30559 Hannover

Tel 0511 / 473906-0
Fax 0511 / 473906-7

feil@recht-freundlich.de