

Cloud Computing & DSGVO

Datenschutz und Datensicherheit - Update 2018

14. März 2018

Cloud Computing & DSGVO

- ◆ DSGVO – wesentliche Regelungen
- ◆ Trusted Cloud – Ansatz zur Standardisierung
 - ◆ Schutzklassen und Schutzbedarf
 - ◆ Datenschutz-Zertifizierung für Cloud-Dienste
- ◆ Data Trustee – Ein Modell zur Trennung der Verantwortung
- ◆ DSGVO als Chance – Gibt es eine Alternative?

Cloud Computing & DSGVO

- ◆ **DSGVO – wesentliche Regelungen**
- ◆ Trusted Cloud – Ansatz zur Standardisierung
 - ◆ Schutzklassen und Schutzbedarf
 - ◆ Datenschutz-Zertifizierung für Cloud-Dienste
- ◆ Data Trustee – Ein Modell zur Trennung der Verantwortung
- ◆ DSGVO als Chance – Gibt es eine Alternative?

Cloud Computing & DSGVO

KAPITEL IV - VERANTWORTLICHER UND AUFTRAGSVERARBEITER

ABSCHNITT 1 ALLGEMEINE PFLICHTEN

ABSCHNITT 2 SICHERHEIT PERSONEN- BEZOGENER DATEN

Artikel 24
Verantwortung des für die Verarbeitung Verantwortlichen

Artikel 25
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Artikel 26
Gemeinsam für die Verarbeitung Verantwortliche

Artikel 27
Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern

Artikel 28
Auftragsverarbeiter

Artikel 29
Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Artikel 30
Verzeichnis von Verarbeitungstätigkeiten

Artikel 31
Zusammenarbeit mit der Aufsichtsbehörde

Artikel 32
Sicherheit der Verarbeitung

Artikel 33
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Artikel 34
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Cloud Computing & DSGVO

- ◆ DSGVO – wesentliche Regelungen
- ◆ **Trusted Cloud – Ansatz zur Standardisierung**
 - ◆ Schutzklassen und Schutzbedarf
 - ◆ Datenschutz-Zertifizierung für Cloud-Dienste
- ◆ Data Trustee – Ein Modell zur Trennung der Verantwortung
- ◆ DSGVO als Chance – Gibt es eine Alternative?

Cloud Computing & DSGVO

Trusted Cloud – Ansatz zur Standardisierung

- ◆ Technologieprogramm Trusted Cloud (2010 -2015)
- ◆ Schirmherrschaft:
Bundesministerium für Wirtschaft und Energie (BMWi)
- ◆ Prüfstandard für die Datenschutz-Zertifizierung nach dem Bundesdatenschutzgesetz (BDSG)
- ◆ 2015 - Kompetenznetzwerk Trusted Cloud e. V.

Cloud Computing & DSGVO

◆ DSGVO Erwägungsgrund 100

Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass **Zertifizierungsverfahren sowie Datenschutzsiegel** und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

Cloud Computing & DSGVO

- ◆ Die Nutzung von Cloud Computing bedeutet für den Cloud-Nutzer keine Aufhebung der datenschutzrechtlichen Verantwortlichkeit und keine Delegation der datenschutzrechtlichen Verantwortlichkeit auf den Cloud-Anbieter. **Der Cloud-Nutzer bleibt datenschutzrechtlich in der Verantwortung** – insbesondere auch für die datenschutzrechtliche Zulässigkeit der Nutzung eines Cloud-Dienstes.

Cloud-Nutzer = Auftraggeber = Verantwortlicher

Cloud Computing & DSGVO

Schutzklassenkonzept (Trusted Cloud)

- ◆ Das Schutzklassenkonzept unterscheidet die Schutzbedarfsklassen 0, 1, 2, 3 und 3+.
- ◆ Eine Schutzbedarfsklasse "0" zeigt das Fehlen eines datenschutzrechtlichen Schutzbedarfs an, etwa bei nicht-personenbezogenen Daten.
- ◆ Eine Schutzklasse "3+" gilt für Daten, die nicht zur Verarbeitung durch Cloud-Dienste geeignet sind.

0

1

2

3

3+

Cloud Computing & DSGVO

Schutzbedarf in der Cloud

- ◆ Pilotprojekt "Datenschutz-Zertifizierung für Cloud-Dienste"
 - ◆ Phase 1: Schaffung eines Prüfstandards für den Datenschutz
 - ◆ Phase 2: Erste Zertifizierungen nach TCDP
- ◆ Trusted Cloud Datenschutz-Profil für Cloud-Dienste
<https://tcdp.de/index.php/hintergrund/pilotprojekt>

Cloud Computing & DSGVO

- ◆ DSGVO – wesentliche Regelungen
- ◆ Trusted Cloud – Ansatz zur Standardisierung
 - ◆ Schutzklassen und Schutzbedarf
 - ◆ Datenschutz-Zertifizierung für Cloud-Dienste
- ◆ **Data Trustee – Ein Modell zur Trennung der Verantwortung**
- ◆ DSGVO als Chance – Gibt es eine Alternative?

Cloud Computing & DSGVO



Cloud-
Anbieter

Daten-
Treuhandler

Cloud Computing & DSGVO

Cloud-Anbieter

Kein grundsätzlicher Zugriff auf Kundendaten

Keine technische Möglichkeit, auf Kundendaten ohne Zustimmung des Datentreuhänders oder des Kunden gemäß den Zugangskontrollrichtlinien zuzugreifen

Kein physischer Zugang zu Rechenzentren, in denen Kundendaten gespeichert sind (ohne Begleitung durch den deutschen Datentreuhänder)

Datentreuhänders

Kontrolliert jeglichen physischen und logischen Zugriff auf Kundendaten (mit Ausnahme eines Zugriffs durch die Kunden oder deren Endbenutzer).

Führt Aufgaben, die Zugriff auf Server mit Kundendaten erfordern, selbst durch oder beaufsichtigt die Ausführung.

Überwacht und prüft jeden im Einzelfall gewährten Zugriff durch Microsoft und beendet den Zugriff, wenn das Problem gelöst ist.

Deutsche Cloud mit Datentreuhänder

Rechtsgarantie durch den Datentreuhänder

Jeder Kunde hat das Commitment des Datentreuhänders, dass dieser den Zugriff auf die Kundendaten nur wie vom Kunden angewiesen oder durch deutsches Recht erfordert gewährt.

Kundendaten in der Microsoft Cloud Deutschland werden vor „Herausgabeverlangen ausländischer Behörden“ oder richterlichen Anordnungen zusätzlich durch ein Datentreuhändermodell geschützt.

Schutz durch den Datentreuhänder

Ein deutsches Unternehmen mit Sitz in Deutschland, agiert als Datentreuhänder im Auftrag des Kunden und muss jede einzelne Datenherausgabe an Dritte freigeben.

Es darf keine Daten (Kundendaten oder Daten über den Kunden) für kommerzielle Zwecke nutzen.

Der Datentreuhänder verpflichtet sich vertraglich direkt gegenüber dem Kunden, dass Kundendaten nicht gegenüber Drittparteien offengelegt werden, es sei denn, der Kunde verlangt es oder deutsches Recht erfordert es.

Cloud Computing & DSGVO

- ◆ DSGVO – wesentliche Regelungen
- ◆ Trusted Cloud – Ansatz zur Standardisierung
 - ◆ Schutzklassen und Schutzbedarf
 - ◆ Datenschutz-Zertifizierung für Cloud-Dienste
- ◆ Data Trustee – Ein Modell zur Trennung der Verantwortung
- ◆ **DSGVO als Chance – Gibt es eine Alternative?**

Cloud Computing & DSGVO

Verantwortlicher - Auftragsverarbeiter - Empfänger - Dritter

Datenverarbeitung im Auftrag

Artikel 24 – Verantwortlicher
Artikel 28 – Auftragsverarbeiter
Artikel 29 – Verarbeitung unter der
Aufsicht des Verantwortlichen
oder des Auftragsverarbeiter



Gemeinsame Verantwortung

Artikel 26 – Gemeinsam für die
Verarbeitung
Verantwortliche

Cloud Computing & DSGVO

Artikel 26 - Gemeinsam für die Verarbeitung Verantwortliche

- (1) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.
- (2) Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.
- (3) Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Cloud Computing & DSGVO

Gemeinsame Verantwortung

- ◆ Vertragliche Festlegung insbesondere zur Transparenz
 - ◆ Rechte der Betroffenen
 - ◆ Informationspflichten
 - ◆ Klare Aufgaben und Verantwortlichkeit
- ◆ Veröffentlichung der Funktionen und Verantwortung
- ◆ Zusammenarbeit gegenüber den Betroffenen

Cloud Computing & DSGVO

Gemeinsame Verantwortung

- ◆ Beispiel Konzern:
 - ◆ Vertrieb und Marketing
 - ◆ Produktion
 - ◆ Zentrale Finanzprozesse
 - ◆ Zentrale IT
- ◆ Beispiel IoT-Service:
 - ◆ Vertrieb und Kundenbetreuung
 - ◆ Produkt-, Softwareentwicklung und Betrieb
 - ◆ Cloud Computing

Was es sonst noch gibt ...

- ◆ Artikel 29 Gruppe (EU) http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
- ◆ Trusted Cloud (KNTC, BMWI) <https://trusted-cloud.de>
- ◆ Standards (Trusted Cloud) <https://trusted-cloud.de/de/standards>
- ◆ Eine Cloud mit deutscher Datentreuhand <https://www.microsoft.com/de-de/cloud/deutsche-cloud>
- ◆ Podcast DaZ <https://auszauberer.de/>
- ◆ Podcast Datenschutz Guru <https://www.datenschutz-guru.de/>
- ◆ Podcast-Suche Datenschutz (FYVD) <https://fyvd.de/search/datenschutz/>
- ◆ Schutzklassenkonzept für die Datenschutz-Zertifizierung nach TCDP
<https://tcdp.de/data/pdf/Schutzklassenkonzept-fuer-die-Datenschutz-Zertifizierung-nach-TCDP-Version-1-o.pdf>