EuroCloud AUSTRIA

LEITFADEN

CLOUD COMPUTING

CLOUD & DATENSCHUTZ

DER CLOUD PRIVACY CHECK (CPC)

ÖSTERREICH
DEUTSCHLAND
SCHWEIZ



Impressum

EuroCloud Austria
Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Wien

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at

Copyright: EuroCloud Austria Verein zur Förderung von Cloud Computing. 2015

Inhaltsverzeichnis

1. Einleitung 6

1.1 Jetzt wird es ernst 6
1.2 Wir machen es uns schwer 6
1.3 Wie geht es einfacher? 7

2. Datenschutz und Cloud Computing 8

2.1 Generelles zum Datenschutz 8
2.2 Datenschutzrechtliche Bedenken gegenüber Cloud-Services 8
2.3 Zwei Kernregeln des Datenschutzrechts 10

3. Cloud Privacy Check (CPC) 10

3.1 Der CPC löst ein Wahrnehmungsproblem 10
3.2 Terminologie des CPC 11
3.3 Was beantwortet der CPC? Was beantwortet der CPC nicht? 12
3.4 Grundüberlegung zum CPC 12
3.5 Die vier Schritte des CPC 14

4. Rechtliche Erläuterungen zu den einzelnen Schritten des CPC 14

4.1 Die Toolbox 14
4.2 Das Vier-Schritte-Modell 16

5. Besonderheiten der nationalen Datenschutzrechte 20

5.1 Anwendung des nationalen Datenschutzrechts 20
5.2 Österreich – Besonderheiten im Datenschutz für Cloud Computing 21
5.3 Deutschland – Besonderheiten im Datenschutz für Cloud Computing 23
5.4 Schweiz – Besonderheiten im Datenschutz für Cloud Computing 25

6. Ausblick: Entwurf einer EU-DSGVO (EU-DSGVO-E) 27

7. Fazit 28

8. Glossar Cloud Computing 29

9. Rechtlicher Hinweis 30

10. Autoren 31

Vorwort



Dr. Tobias Höllwarth
Vorstand EuroCloud Austria

Bis vor kurzem gehörte es fast schon zum guten Ton, das Thema Cloud Computing zu ignorieren oder vollständig zu blockieren. Diese Frühphase der Entwicklung eines Teilbereichs der digitalen Revolution, die wir gerade erleben, kann als überwunden gelten. Niemand kann heutzutage noch behaupten, dass Cloud Computing nicht einen wesentlichen Aspekt des IT-Sourcings in den kommenden Jahren darstellen wird.

Und damit wird schlagartig deutlich, welch umfassendes Know-how in vielen Wissensbereichen – nicht nur in der Technik – erforderlich ist, will man Cloud-Services ernsthaft, verantwortungsbewusst, wirtschaftlich und rechtlich kompatibel zum lokal gültigen Rechtsrahmen einsetzen.

Das Thema Datenschutz taucht unweigerlich gleich zu Beginn auf, denn mit dem Einsatz von Cloud-Services werden Daten – und eben auch personenbezogene Daten – an andere zur Bearbeitung übergeben. Leider machen es uns in Europa nicht nur die unterschiedlichen Sprachen schwer: Beim Datenschutz werden Cloud-Service-Anbietern und -Nutzern noch einmal extra große Hürden in den Weg gelegt. Hier leiden alle unter einem untragbaren und massiven Wettbewerbsnachteil im Vergleich etwa zu den USA.

Dieser untragbare Zustand muss möglichst rasch auf EU-Ebene und auf Länderebene bereinigt werden. Leider wird dies noch etwas dauern, und bis dahin soll der vorliegende Leitfaden, der den Cloud Privacy Check (CPC) beschreibt, eine erhebliche Vereinfachung für die meisten Betroffenen darstellen. Er ersetzt nicht juristische Fachexpertise, aber er strukturiert und vereinfacht ein komplexes Thema ohne Verlust von wesentlichen Informationen.

Dieser Leitfaden wurde im Rahmen des Trust-in-Cloud-Projektes erstellt und ist das Ergebnis einer mehrmonatigen Entwicklungsarbeit des CPC-Teams, dem mein besonderer Dank gilt: Dr. Clemens Thiele (Österreich), Dr. Jens Eckhardt (Deutschland) und Dr. Christian Laux (Schweiz).

Wien, November 2015

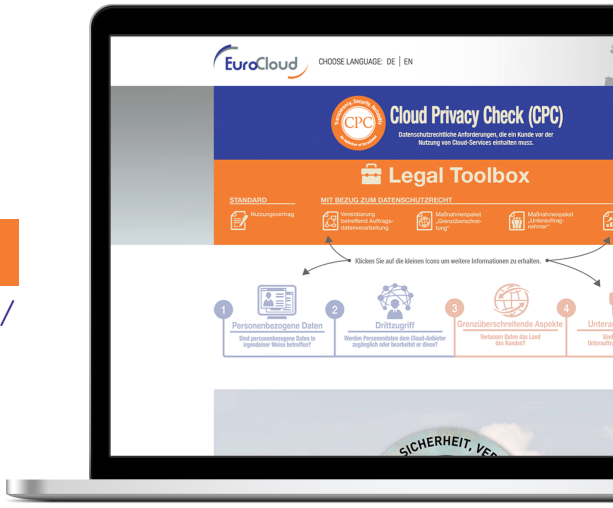
Dr. Tobias Höllwarth

Vorstand EuroCloud Austria

Transparency, Security, Reliability
CPC
An Initiative of EuroCloud

CPC ONLINE TOOL

http://www.cloudprivacycheck.eu/de/



1 Einleitung

1.1 Jetzt wird es ernst

Wer das erste Mal personenbezogene Daten in einen Cloud-Service überträgt, weiß, dass dies ein kritischer Moment ist.

Kritisch deshalb, weil die Abhängigkeit von einem extern zugekauften Service bzw. dessen Betreiber damit schlagartig deutlich wird. Kritisch auch deshalb, weil die Integration eines Cloud-Services in eine bestehende Unternehmens-IT ein komplexes Outsourcing-Unterfangen ist und dabei die eigenen, aber auch die providerseitigen Schwächen, Know-how-Lücken und Inkompatibilitäten zu Tage treten können. Und kritisch, weil die Übertragung von personenbezogenen Daten an einen Dritten (einen Auftragnehmer), manchmals sogar in ein anderes Land, ein Vorgang ist, der im Regelfall strengen juristischen Rahmenbedingungen unterliegt. Mit anderen Worten: Macht man dabei einen groben Fehler, kann das neben einem hohen Reputationsschaden auch ernste kommerzielle und juristische Konsequenzen haben.

Cloud-Sourcing ist ein komplexes Outsourcing-Unterfangen, das zusätzlich durch juristische Vorgaben reglementiert wird. In Europa gibt es für Anbieter und Nutzer von Cloud-Services nicht nur sprachliche Erschwernisse zu bewältigen. Die Eigenheiten im Bereich des Datenschutzes in jedem der EU-Mitgliedsländer tragen maßgeblich dazu bei, dass der Einkauf und Verkauf von Cloud-Services nur mit großer Mühe grenzüberschreitend erfolgen kann. Diese Mühe lässt sich ökonomisch quantifizieren, denn die Kosten einer Kaufanbahnung sowie der Evaluierung und des Einkaufs von Services kann man letztlich messen.

1.2 Wir machen es uns schwer

Die juristische Komplexität der aktuellen europäischen Datenschutzregu-larien zu verstehen, stellt für sich schon eine Herausforderung für einen IT-Techniker, Einkäufer oder Businessnutzer dar. In Kombination mit den kleinen, aber relevanten Unterschiedlichkeiten in den EU-Mitgliedsländern wird es ohne juristische Begleitung selbst in der Einstiegsphase eine fast unbewältigbare Aufgabe.

Fazit: Wir machen es uns hier in der EU schwerer als notwendig. Es besteht dabei auch ein allgemeines Einvernehmen, dass dieser Wettbewerbsnachteil rasch behoben werden muss – und dies wird wohl auch durch die Europäische Datenschutzdirektive teilweise geschehen. Aber lassen Sie uns gleich zu Beginn allzu optimistische Illusionen auflösen. Die Gültigkeit der Direktive selbst, aber noch viel mehr das Entfernen von Landesspezifika wird wohl erst mit einigen Übergangsfristen vollständig abgeschlossen sein.

1.3 Wie geht es einfacher?

Bis dahin muss es eine Abhilfe geben. Dieser Leitfaden und der Cloud Privacy Check (CPC) sollen eine solche Abhilfe darstellen. Dabei gibt es drei methodische Ansätze:

Der Cloud Privacy Check (CPC) bedient sich dreier methodischer Ansätze: Vereinfachung, Strukturierung, Separierung.

1. Vereinfachung

Vereinfachung einer komplexen Materie ohne inhaltliche Verluste: Das Ziel des CPC ist es, auf einer einzigen A4-Seite das Thema Datenschutz und Cloud zu 90 Prozent abzubilden und damit für 90 Prozent aller Personen, die sich damit befassen müssen, eine verständliche und tragfähige Informationsbasis zu liefern. Keine Sorge: Juristen werden weiter benötigt.

2. Strukturierung

Strukturierung einer Vielzahl von Fragen in einzelne Themenblöcke, die schrittweise abgearbeitet werden können – vom einfachen zum kompliziertesten Fall. Und dabei jeweils die Zuordnung von juristischen Werkzeugen, die dazu erforderlich sind und die dann im Detail von Juristen zu erstellen bzw. zu beurteilen sind.

3. Separierung

Separierung des Allgemeingültigen vom Speziellen: Das ist wohl die entscheidendste Hilfe zur Bewältigung einer komplexen, grenzüberschreitenden Herausforderung. Wenn man erkenntlich macht, was in allen Ländern gleich ist, muss sich der Nutzer nur mehr mit den Unterschiedlichkeiten beschäftigen, wenn diese für ihn von Bedeutung sind. Es muss also möglich sein, ganz rasch und einfach die Informationen zu erhalten, die ein anderes Land betreffen, ohne sich wiederum mit jenen Aspekten beschäftigen zu müssen, die ohnehin gleich wie „zu Hause“ sind.

Dieser Leitfaden folgt ähnlichen Prinzipien wie der CPC selbst. Er startet mit einer grundsätzlichen und leicht verständlichen Einführung in das Thema und erklärt in einem weiteren Schritt die Anwendung des CPC. Eine Beschreibung der Legal Tools, die es einzusetzen gilt, darf natürlich ebenso wenig fehlen wie letztlich die Darstellung von landesspezifischen Besonderheiten, die in diesem Leitfaden auf die DACH-Region beschränkt ist.

2 Datenschutz und Cloud Computing

2.1 Generelles zum Datenschutz

Als Datenschutzrecht bezeichnet man im Allgemeinen die Normen einer Rechtsordnung zum Schutz von Personendaten. Der Schutz von Personendaten bezweckt, dass die Persönlichkeit der betroffenen Person geschützt wird. Den Menschen ist in der Informationsgesellschaft das Grundrecht auf Privatsphäre zu sichern. Der zentrale Rahmen des Datenschutzrechts in Ländern der Europäischen Union und des Europäi-schen Wirtschaftsraums ist die Datenschutzrichtlinie.[1]

Schutz von Personendaten bezweckt den Schutz von Personen. Schutz von Daten ist kein Selbstzweck.

Schutz von Personendaten bezweckt den Schutz von Personen. Es sind also nicht die Daten, die als Selbstzweck geschützt werden sollen.

Zum Schutz der Privatsphäre gewährt das Datenschutzrecht vor allem ein Recht auf Geheimhaltung personenbezogener Daten, soweit ein schutzwürdiges Interesse daran besteht.[2] Dieses Recht kann insbesondere mit Zustimmung des Betroffenen oder zur Wahrung überwiegender berechtigter Interessen eines anderen eingeschränkt werden. Daneben treten weitere Ansprüche der betroffenen Person (namentlich die Rechte auf Auskunft, Richtigstellung und Löschung).

Das Datenschutzrecht ist von einem Regel-Ausnahme-Prinzip geprägt. Wer Personendaten Dritter bearbeitet, bedarf dazu eines Rechtfertigungsgrunds.

Das Datenschutzrecht ist von einem Regel-Ausnahme-Prinzip geprägt. Wer Personendaten Dritter bearbeitet, bedarf dazu eines Rechtfertigungsgrunds.

Regeln des Datenschutzrechts kommen ungeachtet vertraglicher Regeln zur Anwendung. Datenschutzrechtliche Regelungen gelten für jede Art von Datenverarbeitung, online ebenso wie offline.[3]

2.2 Datenschutzrechtliche Bedenken gegenüber Cloud-Services

„Cloud“ ist der Sammelbegriff für serverbasierte Angebote zur Verarbeitung von Daten.

Cloud-Services haben ein hohes Potenzial zur Effizienzsteigerung im Wirtschaftsleben. Aus datenschutzrechtlicher Sicht werden jedoch die beiden folgenden Aspekte als kritisch bezeichnet:

1 L 95/46/EG. Mitgliedstaaten müssen die Datenschutzrichtlinie in nationales Recht überführen. Künftig soll die Datenschutzrichtlinie (und mit ihr die nationalen Ausführungsgesetze) durch eine einheitliche Datenschutz-Grundverordnung (DSVO) ersetzt werden.

2 rt. 1 Abs. 1 RL 95/46/EG.

3 Der Europäische Gerichtshof (EuGH) hat dies bereits im Jahr 2003 in der Rechtssache Lindqvist festgestell EuGH 6.11.2003, C-101/01.

Risiko durch Beizug eines Dritten: Mit dem Cloud-Service-Provider (CSP) wird ein Dritter in die Verarbeitung der personenbezogenen Daten durch den Cloud-Service-Customer (CSC) einbezogen. Aus Sicht der zu schützenden betroffenen Person stellt dies eine Erhöhung des Risikos dar, dass mehr Personen möglicherweise auf die bearbeiteten Personendaten zugreifen können.

Kontrollverlust: Erhöht sich die Anzahl der zugriffsberechtigten Personen, steigt die Herausforderung, diese auf datenschutzkonformes Handeln zu verpflichten bzw. die Einhaltung der datenschutzrechtlichen Pflichten zu kontrollieren. Als Kontrollverlust bezeichnet man den Umstand, dass die betroffene Person die zugriffsberechtigten Dritten oft nicht kennt oder keine Möglichkeit hat, diese zu kontrollieren.

Der Datenschutz scheint im Zusammenhang mit der Nutzung von Cloud-Services für den Cloud-Nutzer große Hürden mit sich zu bringen.

Der Datenschutz scheint im Zusammenhang mit der Nutzung von Cloud-Services für den Cloud-Nutzer große Hürden mit sich zu bringen.

Den Bedenken kann Folgendes entgegengehalten werden:

Zum Risiko wegen Beizugs eines Dritten: Dieses Risiko ist nur vermeintlich neu. Die arbeitsteilige und digitale Welt war bereits vor dem Angebot von Cloud-Services durch die Einbeziehung von Dritten bei der Verarbeitung personenbezogener Daten geprägt. Das Datenschutzrecht stellt mit der sogenannten Auftragsdatenverarbeitung auch ein geeignetes Instrument zur Beherrschung dieser Situation zur Verfügung. Richtig aufgesetzte Cloud-Services können sogar einen höheren Schutz gegen den unbefugten Zugriff auf Personendaten bieten als traditionelle Outsourcing-Infrastrukturen.

Zum befürchteten Kontrollverlust: Diese Befürchtung mag durch das Bild der „Wolke" befeuert worden sein. Tatsächlich ist es so, dass die Erbringung von Cloud-Services zum einen häufig unter Einbeziehung von Subunternehmern und zum anderen auch landesgrenzenüberschreitend angeboten wird. Allerdings ist auch dies dem Datenschutzrecht nicht fremd und in der Praxis bereits lange Zeit üblich. Die Besonderheit von Cloud-Services mag darin bestehen, dass solche Konstrukte nun „massentauglich" gemacht werden. An der datenschutzrechtlichen Beherrschbarkeit dieser Konstellation ändert sich hingegen nichts. Das Datenschutzrecht sieht für die Einbindung von Subunternehmern das Instrument der Auftragsdatenverarbeitung vor. Für die grenzüberschreitende Datenverarbeitung stellen die Datenschutzgesetze spezielle Anforderungen auf.

Cloud-Services lassen sich datenschutzkonform erfassen.

Im Ergebnis ist festzuhalten, dass das Datenschutzrecht imstande ist, Cloud-Services datenschutzkonform zu erfassen. Der Grund für die Befürchtungen, die den Cloud-Services entgegengebracht werden, ist wohl zweifacher Natur: (1) Es treffen verschiedene datenschutzrechtliche Anforderungen zusammen; (2) die Komplexität des Sachverhalts ist gesteigert.

2.3 Zwei Kernregeln des Datenschutzrechts

Das Datenschutzrecht stellt zwei Regeln auf, die insbesondere für Cloud-Services zentral sind:

Auf Verantwortung des Cloud-Service-Customers (CSC): Der CSC bleibt bei der Nutzung von Cloud-Services für die Einhaltung des Datenschutzrechts im Rahmen der verwendeten Cloud-Services verantwortlich. Es findet keine Delegation der Verantwortung auf den Cloud-Service-Provider (CSP) statt. Es sind – vereinfacht gesagt – dieselben Grundsätze zu beachten, wie wenn der CSC die Daten auf seinen eigenen Systemen ohne Einschaltung eines CSP bearbeiten würde.

CSP als Auftragsdatenverarbeiter: Der Cloud-Service-Provider (CSP) wird datenschutzrechtlich als sogenannter Auftragsdatenverarbeiter tätig. Die Stellung als Auftragsdatenverarbeiter ist die vorzugswürdige datenschutzrechtliche Einbindung des CSP. Der CSP bleibt eine rechtlich eigenständige Stelle, die allerdings personenbezogene Daten im Auftrag des Cloud-Service-Customers (CSC) als des für die Verarbeitung Verantwortlichen verarbeitet.

3 Cloud Privacy Check (CPC)

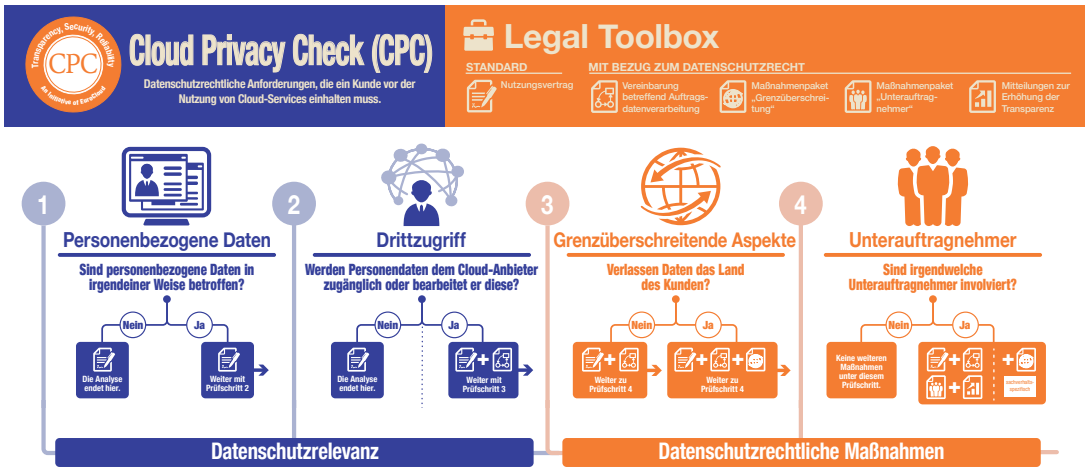
3.1 Der CPC löst ein Wahrnehmungsproblem

Die Erfahrung zeigt, dass sich die datenschutzrechtliche Analyse streckenweise zu kompliziert präsentiert. Dies fördert Rechtsunsicherheit eher, als dass solche reduziert wird.

Dem wirkt der Cloud Privacy Check (CPC) entgegen:

SYSTEMATIK: Der CPC verdeutlicht zunächst, dass die grundlegenden Fragestellungen systematisch angegangen werden können. Nach verschiedenen Datenschutzrechtsordnungen stellen sich dieselben Grundsatzfragen. Diese Grundsatzfragen hebt der CPC deutlich hervor.

TOOLBOX: Darüber hinaus zeigt der CPC auch, dass sich diese Grundsatzfragen mit den zutreffenden datenschutzrechtlichen Instrumenten (CPC Toolbox) datenschutzkonform beantworten lassen.



Der Cloud Privacy Check verdeutlicht die grundsätzliche Fragestellung und verweist auf die richtigen datenschutzrechtlichen Instrumente.

3.2 Terminologie des CPC

Ein häufiges Problem bei der datenschutzrechtlichen Einordnung von Cloud-Services ist die nicht einheitliche Terminologie. Das Datenschutzrecht hat Cloud Computing nicht antizipiert, weswegen die datenschutzrechtlichen Begrifflichkeiten erst noch für Cloud Computing „übersetzt" werden müssen.

Zur Aufhebung dieser Begriffsverwirrung definiert der CPC die Begrifflichkeiten der Cloud-Branche eindeutig wie folgt:

Cloud-Service-Customer (CSC): Der Kunde eines Cloud-Services wird als Cloud-Service-Customer (CSC) bezeichnet. Er steht im Mittelpunkt der wirtschaftlichen Betrachtung.

Cloud-Service-Provider (CSP): Das ist der Dienstleister, der den Cloud-Service dem CSC bereitstellt.

Cloud-Data-Subject (CDS): Die betroffene Person, die als CDS bezeichnet wird, steht im Mittelpunkt der datenschutzrechtlichen Betrachtung. Der CSC lagert Daten des CDS in die Cloud aus. Erst deswegen stellen sich die datenschutzrechtlichen Fragen (Risikoerhöhung und Kontrollverlust).[4] Das CDS soll trotz Auslagerung von Daten in die Cloud durch das Datenschutzrecht geschützt werden.

4 Siehe oben, Punkt 2.2

Personenbezogene Daten: Daten sind nur dann datenschutzrechtlich relevant, wenn sie einen Bezug zum CDS aufweisen. Erst dann liegen personenbezogene Daten vor. Der Bezug zum CDS muss derart klar sein, dass die betroffene Person (CDS) bestimmbar ist. Eine solche Bestimmbarkeit ist gegeben, wenn nähere Informationen ohne unangemessene Anstrengungen beschafft werden können und damit die Identifizierung der betroffenen Person (CDS) möglich wird. Es genügt also, wenn der CSP durch weitere Nachforschungen herausfinden kann, wer die betroffene Person (CDS) ist, damit die datenschutzrechtlichen Regeln zur Anwendung gelangen.[5]

3.3 Was beantwortet der CPC? Was beantwortet der CPC nicht?

Der CSC darf Daten des CDS auch außerhalb der Cloud nur rechtmäßig bearbeiten. Allfällige Bearbeitungsschranken hat bereits der CSC einzuhalten. Diese Bearbeitungsschranken muss der CSC dem CSP weitergeben. Mit dieser auch unabhängig von Cloud-Services bestehenden datenschutzrechtlichen Betrachtung befasst sich der CPC nicht.

Der CSC muss zusätzlich die beiden zuvor[6] dargestellten Kernregeln des Datenschutzrechts einhalten. Er muss in Bezug auf das CDS den datenschutzrechtlichen Schutz mit Blick auf die Besonderheit der Nutzung des Cloud-Services sicherstellen. Diese Fragestellungen sind die cloudspezifischen Datenschutzfragen. Mit diesen befasst sich der CPC.

3.4 Grundüberlegung zum CPC

Kriterium #1: Personendaten: Der CPC kommt zum Tragen, wenn Personendaten eines CDS bearbeitet werden.

Kriterium #2: Beizug eines Dritten: Der CPC trägt dem Umstand Rechnung, dass Cloud-Services durch externe Dienstleister erbracht werden.

Kriterium #3: Auslandsbezug: Externe Dienstleister erbringen ihre Leistungen oft im bzw. aus dem Ausland heraus.

Kriterium #4: Subunternehmer: Externe Dienstleister bedienen sich wiederum weiterer Dienstleister zur Erbringung des Cloud-Services. Diese weiteren Dienstleister erbringen unter Umständen ihre Teilleistung wiederum in bzw. aus weiteren Ländern heraus.

5 Siehe außerdem die Ausführungen unter Punkt 4.2

6 Siehe oben, Punkt 2.3

In jeder Datenschutzrechtsordnung in der EU, im EWR und auch in der Schweiz sowie der Türkei ergeben sich bei der datenschutzrechtlichen Bewertung von Cloud-Services also vier grundlegende Fragestellungen.

In jeder Datenschutzrechtsordnung in der EU, im EWR und auch in der Schweiz sowie der Türkei ergeben sich bei der datenschutzrechtlichen Bewertung von Cloud-Services vier grundlegende Fragestellungen.

Praxisbeispiel: Es ist nicht ungewöhnlich, dass ein inländischer CSP die für den Cloud-Service erforderliche Data-Center-Leistung durch eine ausländische Gesellschaft erbringen lässt. Die Softwarepflege und/oder Softwareentwicklung sowie den Support lässt sie von weiteren ausländischen Gesellschaften erbringen (Stichwort: „off-shoring" und „follow-the-sun"). Merke: Obwohl der CSP ein inländisches Unternehmen ist, liegt ein Sachverhalt mit Auslandsbezug vor.

Praxisbeispiel: Wenn der CSP ein ausländisches Unternehmen ist und sich die im vorstehenden Praxisbeispiel genannte Kette daran anschließt, ist der Auslandsbezug offensichtlich.

Jede der vier genannten grundlegenden Fragestellungen (siehe oben: Kriterium #1 bis #4) markiert aus datenschutzrechtlicher Sicht eine Weichenstellung. Je nach Beantwortung dieser weichenstellenden Fragen fordert das Datenschutzrecht bestimmte Maßnahmen zur Wahrung des Datenschutzes.

Die Bewertung von Cloud-Services lässt sich auf vier grundlegende Fragestellungen herunterbrechen. Cloud-Services können datenschutzkonform genutzt werden, wenn zu jeder dieser grundlegenden Fragestellungen die verlangten Maßnahmen entsprechend der Bewertung der Frage ergriffen werden.

Der Cloud Privacy Check (CPC) bildet diese vier grundlegenden Fragestellungen in vier Schritten ab und zeigt die Antworten auf. Der Cloud Privacy Check (CPC) verdeutlicht damit Folgendes:

Die Bewertung von Cloud-Services lässt sich auf vier grundlegende Fragestellungen herunterbrechen. Es ist eine übersichtliche Bewertung von Cloud-Services in vier Schritten möglich.

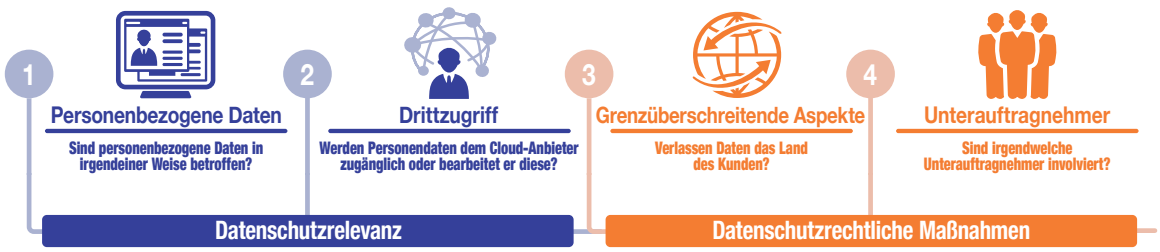
Cloud-Services können datenschutzkonform genutzt werden, wenn zu jeder dieser grundlegenden Fragestellungen die verlangten Maßnahmen entsprechend der Bewertung der Frage ergriffen werden.

3.5 Die vier Schritte des CPC

Kriterium #1 (Personenbezug) und Kriterium #2 (Drittzugriff) adressieren gemeinsam die Frage, ob die Nutzung des Cloud-Services datenschutzrechtlich relevant ist. Zusammengenommen markieren die beiden den Umschlagspunkt der datenschutzrechtlichen Analyse. Diese beiden Kriterien fragt der CPC in den Schritten 1 und 2 ab.

Die Schritte 3 und 4 des CPC adressieren die datenschutzrechtlichen Maßnahmen für Gestaltungsformen, die für Cloud-Services typisch sind.

So entsteht der vierstufige Prozess, den der CPC vorsieht. Die einzelnen Schritte werden unter Punkt 4.2 im Einzelnen dargestellt.



4 Rechtliche Erläuterungen zu den einzelnen Schritten des CPC

Jeder der vier Schritte des CPC beinhaltet datenschutzrelevante Fragestellungen und Aspekte zur datenschutzkonformen Gestaltung der Nutzung von Cloud-Services.

4.1 Die Toolbox

Die einzelnen nachstehend dargestellten Maßnahmenpakete werden jeweils im Kontext der jeweiligen Schritte und unter Punkt 4.2 näher betrachtet Eine Cloud-Lösung wird aus datenschutzrechtlicher Sicht dann rechtmäßig eingesetzt, wenn die richtigen Instrumente dafür verwendet werden.



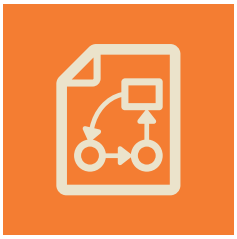
1. Cloud-Nutzungsvertrag



Ein Nutzungsvertrag in Bezug auf den Cloud-Service ist Standard. In diesem werden zivilrechtlich die Leistungspflichten des CSC und des CSP geregelt. Der Kern der geregelten Pflicht des CSC ist die Zahlung des Entgelts. Der Kern der Pflicht des CSP ist die Bereitstellung des Cloud-Services. Ob und welche weiteren Regelungen enthalten sind, obliegt den Bedürfnissen der Parteien (z. B. Regelungen zum Zahlungsverzug, zur Sperre, zum Service Level, zur Verfügbarkeit, zur Performance etc.).

Neben dem immer erforderlichen Cloud-Nutzungsvertrag gibt es vier Instrumente, die sich in der sogenannten „CPC Legal Toolbox“ wiederfinden:

2. Vertrag betreffend Auftragsdatenverarbeitung



Die Vereinbarung über die Auftragsdatenverarbeitung ist ein Vertrag, für den das jeweils nationale Recht inhaltliche Vorgaben vorsieht.[7] Werden diese Anforderungen berücksichtigt, handelt es sich dabei um eine datenschutzrechtlich privilegierte Einbindung eines Dienstleisters.

Daher handelt es sich um eine vorzugswürdige Ausgestaltung der Ein-bindung von Auftragnehmern.

3. Maßnahmen bei Grenzüberschreitung



Das Maßnahmenpaket „Grenzüberschreitung“ umfasst Leitlinien zur da-tenschutzkonformen Ausgestaltung der grenzüberschreitenden Daten-verarbeitung. Es bestehen Unterschiede, je nachdem, in welches Land die Daten übertragen werden.[8]

7 Siehe hierzu die Darstellung der Besonderheiten der nationalen Rechtsordnungen (Punkt 5).
8 Nationale Besonderheiten werden wiederum unter (Punkt 5). dargestellt.



4. Maßnahmen zur Einbindung von Subunternehmern

Das Maßnahmenpaket „Unterauftragnehmer“ umfasst Leitlinien zur Ein-bindung von Subunternehmern durch den Cloud-Service-Provider. Hierfür ergeben sich sowohl aus der Vereinbarung über die Auftragsdatenverarbeitung (siehe Punkt 4.1.2) und eine eventuelle weitere grenzüberschreitende Datenverarbeitung (siehe Punkt 4.1.3) besondere Anforderungen.[9]



5. Mitteilungen an den Kunden zur Erhöhung der Transparenz

Gerade bei der Einbindung von Subunternehmern entsteht eine Trans-parenzpflicht des CSP gegenüber dem CSC. Diesem Umstand trägt das Tool „Mitteilung zur Erhöhung der Transparenz“ Rechnung.[10]

4.2 Das Vier-Schritte-Modell

1. Schritt #1: Personenbezogene Daten

Das Datenschutzrecht ist nur zu beachten, wenn personenbezogene Daten erhoben oder verwendet werden. Es stellt sich damit für die Nutzung eines Cloud-Services die folgende zentrale Frage:

Werden (überhaupt) personenbezogene Daten in der Cloud genutzt?

Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“) sind personenbezogene Daten.

Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

9 Die Anforderungen der einzelnen Rechtsordnungen werden auch hierfür unter (Punkt 5). dargestellt.tellt.

10 DieUnter (Punkt 5). werden Details zu Informationsumfang und Informationstiefe beschrieben.

Beispiele von Personendaten:

- IP-Adressen (wie sie von Servern im Rahmen von http-Abrufen gesammelt werden)
- Daten über einen Mobiltelefonvertrag oder über Stromrechnungen (Informationen, die zum Ausdruck bringen, womit der Nutzer belastet werden wird)



Manchmal ist es schwer zu bestimmen, ob personenbezogene Daten vorliegen.

Anonymisierte Information fällt nicht in den Anwendungsbereich der Datenschutzgesetze. Forscher konnten jedoch nachweisen, dass gewisse anonymisierte Daten deanonymisiert werden könnten, wenn man nur genügend Know-how dafür besitzt und den notwendigen Aufwand betreibt. Das Risiko der Deanonymisierung ist jedenfalls gestiegen. In Kürze: Je stärker ein Datensatz geeignet ist, deanonymisiert zu werden, desto mehr muss man im Rahmen einer Analyse davon ausgehen, dass es sich bei einem Datensatz tatsächlich um eine personenbezogene Angabe handelt.

Ist die Antwort auf die Frage, ob personenbezogene Daten betroffen sind, NEIN, dann sind keine datenschutzrechtlichen Instrumente erforderlich. Es bleibt dann beim Nutzungsvertrag zwischen Cloud- Anbieter und Cloud-Kunden.

Ist die Antwort JA, muss die zweite Prüfung des Cloud Privacy Checks durchgeführt werden.

Zu beachten ist, dass im Detail in den nationalen Datenschutzgesetzen Abweichungen bestehen können, insbesondere zu folgenden Aspekten:

- Sind nur Menschen (natürliche Personen) oder auch juristische Personen durch den Datenschutz geschützt?
- Wann ist von einer Bestimmbarkeit auszugehen bzw. wie hoch sind die Anforderungen an eine Anonymisierung?



2. Schritt #2: Drittzugriff

Die datenschutzrechtliche Anforderung, einen Dritten datenschutzkonform einzubinden, stellt sich nur, wenn der Dritte Zugriff auf personenbezogene Daten hat.

Welche Art von Zugriff erforderlich ist, ist in den nationalen Datenschutzbestimmungen teilweise unterschiedlich ausgeprägt.

Der CPC verdeutlicht, wann ein solcher datenschutzrechtlicher Zugriff tendenziell verneint werden kann.

Dabei ist die technische Ausgestaltung der Dienstleistung entscheidend. Es lässt sich ein sogenannter Umschlagspunkt definieren.

Wird der Umschlagspunkt nicht überschritten, kann der CPC beendet werden und es bleibt beim Nutzungsvertrag.

Wird der Umschlagspunkt jedoch überschritten, muss als erstes datenschutzrechtliches Instrument ein Vertrag betreffend Auftragsdatenverarbeitung zum Einsatz kommen – zusätzlich zum Nutzungsvertrag.

Ist die Antwort auf die Frage, ob Dritte Zugriff auf personenbezogene Daten haben, JA, dann muss nach der zweiten Prüfung nun die dritte Prüfung ausgeführt werden.



3. Schritt #3: Grenzüberschreitende Aspekte

Werden die personenbezogenen Daten im Rahmen des Cloud-Services außerhalb des Heimatlandes des CSC verarbeitet, stellt dies aus datenschutzrechtlicher Sicht eine neue Dimension des Umgangs mit personenbezogenen Daten dar.

Die Regeln zur Umsetzung des Maßnahmenpakets Grenzüberschreitung sind von Land zu Land verschieden. Aggregiert lässt sich die Rechtslage wie folgt darstellen:

(1) Wenn der Cloud-Dienstleister (CSP) keinen Bezug zu einer Rechtsordnung außerhalb der EU bzw. des EWR hat, dann sind keine zusätzlichen Maßnahmen erforderlich. Im vorliegenden Kontext heißt „kein Bezug“, dass der CSP weder Geschäftssitz noch IT-Infrastruktur außerhalb des EU/EWR-Raums hat und auch nicht von außerhalb des EU/EWR-Raums auf Daten des Kunden zugreift.

(2) Wenn der CSP in einem Land außerhalb des EU/EWR-Raums tätig ist, dieses Land aber als eines mit gleichwertigem Schutzniveau anerkannt ist (z. B. Kanada, Israel, Schweiz, Uruguay), dann sind keine zusätzlichen Maßnahmen zu ergreifen.

Wenn der CSP nicht in die Kategorie (1) oder (2) fällt, sind weitere Maßnahmen nötig: Vorgehen nach den EU-Standardvertragsklauseln oder Genehmigung.

Der EuGH hat mit Urteil vom 06.10.2015 die sogenannten Safe-Harbor-Principles in der Fassung der Entscheidung der EU-Kommission 2000/520/EG vom 26.07.2000 für unwirksam erklärt. Diese Safe-Harbor-Principles sind damit keine Rechtsgrundlage mehr für einen Datentransfer. Es müssen daher andere Maßnahmen ergriffen werden. Auf den ersten Blick bieten sich der EU-Standardvertrag oder Binding Corporate Rules an.[11]

Ist die Antwort auf die Frage nach der Grenzüberschreitung NEIN (also: kein Auslandsbezug), dann kommt kein weiteres datenschutzrechtliches Instrument zum Einsatz und man kann direkt zur vierten Prüfung übergehen.

Ist die Antwort JA (also: Auslandsbezug gegeben), dann ist das Maßnahmenpaket „Grenzüberschreitung“ zu aktivieren. Danach kann die vierte Prüfung durchgeführt werden.

4. Schritt #4: Unterauftragnehmer



Sind irgendwelche Unterauftragnehmer involviert?

Das Maßnahmenpaket „Unterauftragnehmer“ kann sich an den Cloud-Kunden sowie an den Unterauftragnehmer richten:

(1) Maßnahmen zwischen dem Cloud-Service-Provider (CSP) und dem Cloud-Kunden:

a) Vereinbarung betreffend Auftragsdatenverarbeitung

b) Die Maßnahmen gemäß Prüfstufe 3 sind erforderlich, wenn der Unterauf-tragnehmer einen relevanten Bezug zum Ausland hat.

c) Der Kunde muss angemessen über den Beizug von Unterauftragnehmern informiert sein.

(2) Maßnahmen, die im Verhältnis zwischen dem Cloud-Service-Provider (CSP) und dem Unterauftragnehmer greifen: Der CSP muss seine Pflichten aus der Auftragsdatenverarbeitung an den Unterauftragnehmer weitergeben.

11 So die Stellungnahme der Art. 29-Datenschutzgruppe vom 16. Oktober 2015: „In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, EU-data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used.“

(3) Maßnahmen, die im Verhältnis zwischen dem Cloud-Kunden und dem Unterauftragnehmer greifen: Eine im Direktverhältnis vereinbarte Vereinbarung betreffend Auftragsdatenverarbeitung kann die Compliance verbessern.

Der Auslandsbezug kann die Analyse betreffend Unterauftragnehmer beeinflussen:

(1) Die Umsetzung des Maßnahmenpakets unter Prüfschritt 3 soll geprüft werden.

(2) Die Weiterleitung von Daten kann unter den EU-Standardvertragsklauseln mit Subprozessorklausel geregelt werden (in Österreich erfordert dies eine Genehmigung von der Aufsichtsbehörde; in Deutschland ist keine Genehmigung erforderlich; in der Schweiz reicht eine bloße Meldung aus).

Für die EU-Standardverträge ist zu beachten, dass sie nicht zwischen Vertragspartnern angewendet werden können, die beide ihren Sitz in der EU / im EWR haben. Sie müssen vom Auftraggeber in der EU direkt mit dem Unternehmen im Drittstaat abgeschlossen werden.

5 Besonderheiten der nationalen Datenschutzrechte

Der CPC zeigt die vier grundlegenden datenschutzrechtlichen Fragestellungen zur Nutzung von Cloud-Services durch den CSP und zum Schutz des CDS auf. Der rechtliche Werkzeugkasten (Legal Toolbox, dazu Punkt 4.1) hält die Antworten zur datenschutzkonformen Gestaltung der Cloud-Nutzung aus Kundensicht (Sicht des CSC) bereit.

Im Rahmen der Antworten des CPC können sich bei einer Detailbetrachtung nationale Besonderheiten ergeben. Hierüber wird nachfolgend in der gebotenen Kürze ein Überblick gegeben.

Die Länderteile sind entsprechend dem 4-Schritte-Schema gegliedert.

5.1 Anwendung des nationalen Datenschutzrechts

Das anwendbare Recht bestimmt sich jeweils ausgehend vom Territorialitätsprinzip, denn jeder Staat kann nur für sein Staatsgebiet die Rechtslage bestimmen. Für die EU-Mitgliedstaaten ist diese Bewertung im Datenschutzrecht durch eine EU-Richtlinie überlagert. Die Bestimmung knüpft an die betroffene Person (CDS) an. Für die Bestimmung des anwendbaren Datenschutzrechts kommt es also nicht auf die Beziehung zwischen CSP und CSC an, sondern auf die Beziehung

des CSC zum CDS.

Hiervon ausgehend ergibt sich für die Anwendung des Datenschutzrechts – vereinfacht gesagt – folgende Aufteilung:

- Hat der CSC seinen Sitz in demselben Land wie das CDS, dann gilt das Recht dieses Landes.
- Hat der CSC seinen Sitz in einem EU-/EWR-Mitgliedsstaat und das CDS seinen Sitz in einem EU-Mitgliedsstaat, dann gilt das Datenschutzrecht am Sitz des CSC.
- Hat der CSC seinen Sitz außerhalb der EU / des EWR und das CDS seinen Sitz in einem EU-Mitgliedsstaat, dann gilt das Datenschutzrecht am Sitz des CDS.

Im Folgenden wird zur Vereinfachung der Begrifflichkeiten jeweils von „DSG" gesprochen, wenn das nationale Datenschutzgesetz bezeichnet wird. Statt vom deutschen Bundesdatenschutzgesetz oder „BDSG" ist also vom DSG-DE die Rede (bzw. für Österreich vom DSG-AT, für die Schweiz vom DSG-CH).

Es geht ja nur um DE, AT und CH, also gibts kein etc.

5.2 Österreich – Besonderheiten im Datenschutz für Cloud Computing

1. Allgemeine Bemerkung

Eingangs ist festzuhalten, dass derzeit in Österreich weder eine Empfehlung noch eine ausdrückliche, gefestigte Rechtsprechung zum Datenschutz bei Cloud Computing besteht. Der Cloud Privacy Check (CPC) gibt allerdings einen Best-Practice-Standard nach dem DSG-AT wieder. Die rechtssichere Umsetzung von Datenschutzprojekten im Bereich des Cloud Computings hat sich daher (auch) in Österreich an den durch den Cloud Privacy Check (CPC) vorgegebenen vier Prüfungen zu orientieren:

2. Personenbezogene Daten

Das DSG-AT schützt auch juristische Personen in Bezug auf die sie beschreibende Information.

Für die Frage, ob in pseudonymisierten Daten oder verschlüsselten Daten ein Personenbezug erkennbar bleibt, kommt es auf den Horizont des Empfängers an.

3. Einbindung von Dritten

Ein Dienstleister, der vom CSC als beigezogener Dritter beauftragt wird, gilt nicht als Dritter im Sinne des DSG-AT. Die Privilegierung durch Auftragsdatenverarbeitung gilt nur in Bezug auf Dienstleister, die ihren Sitz in der EU oder im EWR (oder in einem als gleichwertig anerkannten Drittland) haben. Das Gesetz verlangt ausdrücklich, dass das Datengeheimnis auf Mitarbeitende des CSP überbunden wird.

Eine Pflicht zur namentlichen Nennung des beigezogenen Dienstleisters an das CDS besteht nach DSG-AT nicht. Auf Anfrage muss der CSC dem CDS aber den Namen des beigezogenen Dienstleisters bekanntgeben. Auf Anfrage muss der CSC dem CDS auch den Ort der Datenverarbeitung bekanntgeben.

Es besteht eine gesetzliche Herausgabe- und physische Löschungsverpflichtung des CSP für die im Auftrag des CSC verarbeiteten Daten nach Beendigung des Auftragsdatenverhältnisses. Ein bestimmtes Datenformat für die Herausgabe ist allerdings gesetzlich nicht vorgesehen.

4. Grenzüberschreitender Datentransfer

Im Cross-Border-Transfer über IT-Schengen hinaus ist der CSP unabhängig vom CSC befugt, eine Genehmigung bei der österreichischen Datenschutzbehörde (DSB-AT) zu beantragen, wenn er einen bestimmten weiteren Subdienstleister aus dem Ausland heranziehen will.

5. Einbindung von Subunternehmern

Der CSP darf Subdienstleister nur mit Billigung des CSC einsetzen. Dies bedingt, dass der CSP den CSC vor dem Beizug von Subdienstleistern informiert haben muss. Auf Anfrage muss der CSC dem CDS den Namen von beigezogenen Subunternehmern bekanntgeben. Der CSC hat ein Vetorecht gegen den Beizug von Subdienstleistern.

5.3 Deutschland – Besonderheiten im Datenschutz für Cloud Computing

1. Allgemeine Bemerkung

Das deutsche Datenschutzrecht weist Besonderheiten auf, die im Rahmen eines Überblicks nachfolgend angesprochen werden. Eine vertiefte Darstellung enthält der „Leitfaden Cloud Computing: Recht, Datenschutz & Compliance“ des EuroCloud Deutschland_eco e.V.[12]

Die datenschutzrechtliche Bewertung wird in Deutschland durch eine Orientierungshilfe der deutschen Datenschutzaufsichtsbehörden erleichtert: „Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises“, Version 2.0, Stand 09.10.2014[13]. Diese wird nachfolgend als „Orientierungshilfe“ abgekürzt.

Die Orientierungshilfe ist nicht gesetzesgleich, sondern gibt die Bewertung der Datenschutzaufsichtsbehörden wieder. Eine Befreiung von eigenen datenschutzrechtlichen Prüfungen ist damit nicht verbunden. Ein Gericht ist weder im positiven noch im negativen Sinn hieran gebunden.

2. Personenbezogene Daten

Das DSG-DE schützt nur natürliche Personen in Bezug auf die sie beschreibende Information. Juristische Personen sind grundsätzlich nicht geschützt. Eine Ausnahme enthalten die Datenschutzbestimmungen des deutschen Telekommunikationsgesetzes (TKG). Die Datenschutz-bestimmungen des TKG gelten auch für juristische Personen, soweit es um Verkehrsdaten geht.

Das Datenschutzrecht ist auch auf pseudonymisierte Daten anwendbar. Allein auf anonymisierte Daten findet das Datenschutzrecht nicht mehr Anwendung. Die deutschen Datenschutzaufsichtsbehörden haben den Standpunkt eingenommen, dass das Datenschutzrecht auch dann bei der Nutzung eines Cloud-Services zu beachten ist, wenn die in die Cloud ausgelagerten Daten, so verschlüsselt sind, dass der CSP sie nicht der jeweiligen Person zuordnen kann. Dieser Ansatz ist aufgrund seiner Begrün-dung jedoch umstritten.

Für sogenannte besondere personenbezogene Daten gilt eine Spezial-regelung. Nach dieser scheidet eine Verarbeitung solcher Daten in der Cloud außerhalb einer Auftragsdatenverarbeitung in der EU bzw. des EWR aus (zulässig selbstverständlich bei Vorliegen einer Einwilligung des CDS).

12 http://www.eurocloud.de/2010/news/datensicherheit/eurocloud-leitfaden-recht-datenschutz-compliance.html

13 Quelle: https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf; Stand des Aufrufs der Quelle: 7.09.2015

Solche besondere personenbezogene Daten sind Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

3. Einbindung von Dritten

Ein Dienstleister, der vom CSC als Auftragsdatenverarbeiter im Sinne des DSG-DE beauftragt wird, gilt nicht als Dritter im Sinne des DSG-DE. Das DSG-DE setzt für die Privilegierungswirkung jedoch – vereinfacht – die folgenden Eckpunkte voraus:

- Sorgfältige Auswahl des CSP durch den CSC
- Regelmäßige Prüfung des CSP durch den CSC in Bezug auf IT-Sicherheit
- Weisungsgebundenheit des CSP gegenüber dem CSC
- Vertrag über die Auftragsdatenverarbeitung nach den Vorgaben des DSG-DE
- Schriftform des Vertrags über die Auftragsdatenverarbeitung

Für alle Länder, die nicht zur EU oder zum EWR gehören, gilt die Privilegierung nicht. Dabei bleibt es selbst dann, wenn für diese Länder durch die EU-Kommission ein angemessenes Datenschutzniveau anerkannt worden ist. Das hat folgende praktische Konsequenz für die Zulässigkeitsbewertung der Einbeziehung eines Dritten:

- Innerhalb der EU / des EWR: Eine inhaltlich und formell korrekt aufgesetzte Vereinbarung über die Auftragsdatenverarbeitung macht den Einbezug des Dritten zulässig.

- Außerhalb der EU / des EWR: Die datenschutzrechtliche Zulässigkeit ist anhand einer Interessenabwägung zu bewerten. Die Existenz der formell und inhaltlich korrekt zustande gekommenen Vereinbarung über die Auftragsdatenverarbeitung wirkt sich positiv auf die Interessenabwägung und damit auf die Zulässigkeit der Einbeziehung des Dritten aus.

Bei grenzüberschreitendem Datentransfer sind weitere Anforderungen zu beachten (hierzu nachfolgend Ziffer 4).

Jedenfalls auf Nachfrage muss der CSC dem CDS den Namen des Dienstleisters und auch den Ort der Datenverarbeitung bekanntgeben.

Es ist durch den CSC gegenüber dem CSP vertraglich die Herausgabe- oder physische Löschungsverpflichtung des CSP für die im Auftrag des CSC verarbeiteten Daten nach Beendigung des Auftragsdatenverhältnisses zu regeln.

4. Grenzüberschreitender Datentransfer

Bei Nutzung eines Cloud-Services in einem Drittstaat bzw. einem Zugriff auf personenbezogene Daten aus einem Drittstaat sind weitere Maßnahmen zum Schutz der personenbezogenen Daten zu ergreifen. Dies sind die Instrumente (z. B. EU-Standardvertrag, durch die Aufsichtsbehörden genehmigter Individualvertrag), die auch in den anderen EU-Mitgliedsstaaten vorgesehen sind. Als deutsche Besonderheit kommen zwei Aspekte hinzu:

Bei der Verwendung von EU-Standardverträgen besteht keine Anzeigepflicht und kein Genehmigungserfordernis. Nur individuell gestaltete Verträge müssen den Aufsichtsbehörden zur Genehmigung vorgelegt werden, damit sie datenschutzrechtlich rechtfertigende Wirkung haben. Für Binding Corporate Rules bestehen Sonderregelungen.

Nach Ansicht der deutschen Datenschutzaufsichtsbehörden in der Orientierungshilfe müssen in jedem Fall ergänzend zu den vorstehenden Gestaltungen Vereinbarungen nach den inhaltlichen Maßgaben der Vereinbarung über die Auftragsdatenverarbeitung getroffen werden.

5. Einbindung von Subunternehmern

Der Subunternehmer muss in jedem Fall vertraglich durch den CSP eingebunden werden und gegenüber dem CSC transparent gemacht werden. Der CSC muss auch eine Möglichkeit haben, die Einbindung von weiteren Subunternehmern zu „steuern“; er muss zumindest die Möglichkeit haben, der Einbeziehung von Subunternehmern zu widersprechen. Hierzu müssen ihm die Subunternehmer so rechtzeitig benannt werden, dass er deren Einbindung effektiv widersprechen kann. Die Vereinbarung muss auch dem CSC die Rechte gegenüber dem Subunternehmer einräumen, die der CSC gegenüber dem CSP hat.

5.4 Schweiz – Besonderheiten im Datenschutz für Cloud Computing

1. Allgemeine Bemerkungen

Das DSG-CH beansprucht Geltung für jede Transaktion, die sich auf betroffene Personen auswirkt, die ihren Wohnsitz, Sitz oder Aufenthaltsort in der Schweiz haben. Massgeblich ist somit die Perspektive der betroffenen Person.

2. Personenbezogene Daten

Das DSG-CH schützt auch juristische Personen in Bezug auf die sie beschreibende Information. Das DSG-CH kennt die Kategorie der Persönlichkeitsprofile. Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Persönlichkeitsprofile sind den besonders schützenswerten Informationen (sensiblen Personendaten) gleichgestellt.

Die Schweizer Datenschutzbehörde (DSB-CH) behandelt pseudonymisierte Daten als Personendaten. Die Rechtsfolgen richten sich nach einem „risikobasierten Ansatz". Die DSB-CH hat sich gegen die Beurteilung allein aus Empfängersicht ausgesprochen.

3. Einbindung von Dritten

Die Privilegierung durch Auftragsdatenverarbeitung gilt nicht nur in Bezug auf Dienstleister, die ihren Sitz in der EU oder im EWR (oder in einem als gleichwertig anerkannten Drittland) haben, sondern generell.

4. Grenzüberschreitender Datentransfer

Grenzüberschreitender Datentransfer, der über genehmigte Muster-vertragsklauseln oder über Binding Corporate Rules gerechtfertigt wird, ist zu melden.

5. Einbindung von Subunternehmern

Es gibt keine ausdrückliche Pflicht, beigezogene Subunternehmer namentlich zu nennen. Allerdings kann sich eine solche Pflicht im Einzelfall aus den Umständen ergeben (Angemessenheitsprüfung).

6 Ausblick: Entwurf einer EU-DSGVO (EU-DSGVO-E)

Am 25.01.2012 hat die EU-Kommission einen ersten Entwurf für eine Europäische Datenschutz-Grundverordnung (EU-DS-GVO-E) vorgelegt.

Im Gegensatz zu den bisherigen unionsrechtlichen Datenschutzregelungen, die in Form von Richtlinien erlassen wurden, wählt die Kommission nun die Rechtsform der Verordnung. Im Unterschied zu einer Richtlinie, die gem. Art. 288 Abs. 3 AEUV immer einen nationalen Transformationsakt zur Umsetzung in das nationale Recht benötigt, gilt eine Verordnung gem. Artikel 288 Abs. 2 AEUV ohne einen entsprechenden Transformationsakt unmittelbar verbindlich in allen Mitgliedstaaten.

Im September 2015 befindet sich die EU-DSGVO noch im Gesetzgebungsverfahren, sodass die Inhalte noch nicht abschließend feststehen. Ein Inkrafttreten der EU-DSGVO ist seitens der EU für 2016 angestrebt.

Die EU-DSGVO wird in den EU-Mitgliedstaaten unmittelbar geltendes Recht. Sie hat Vorrang vor allen kollidierenden nationalen Datenschutzbestimmungen, sofern sie nicht selbst Ausnahmen festlegt. Derzeit ist vorgesehen, dass die EU-DSGVO erst zwei Jahre nach ihrem Inkrafttreten anzuwenden ist. Es entsteht also eine Art Übergangszeit.

Was bedeutet die EU-DSGVO für den CPC? Es wird sich voraussichtlich nichts am CPC ändern. Denn: Auch nach der EU-DSGVO sind weiterhin die vier grundlegenden Fragen zu stellen. Den Hintergrund bildet jedoch nicht mehr das jeweilige nationale Recht, sondern für die EU-Mitgliedsstaaten die EU-DSGVO:

Für die Anwendbarkeit der EU-DSGVO wird die Betroffenheit personenbezogener Daten entscheidend sein.

Für die EU-DSGVO wird es darum gehen, ob und wie ein CSP auf diese Daten zugreift. Auch die Auftragsdatenverarbeitung und deren Anforderungen werden in der EU-DSGVO geregelt werden.

Die EU-DSGVO wird ebenfalls die Frage nach der grenzüberschreitenden Datenübermittlung stellen. Sie wird – wie auch bisher im nationalen Recht – an die Übermittlung innerhalb der EU und des EWR weniger hohe Anforderungen stellen als an die Übermittlung in Drittstaaten.

Auch die Einbindung von Subunternehmern muss entsprechend den Vorgaben aus der Auftragsdatenverarbeitung des CSP ausgestaltet und ein eventueller weiterer Auslandstransfer berücksichtigt werden.

Zusammenfassend: Der CPC wird auch unter der EU-DSGVO die richtigen Fragen stellen und

damit als Hilfsmittel zur Veranschaulichung Geltung behalten.

Was kann die EU-DSGVO für Cloud-Services bedeuten?

Vereinheitlichung der datenschutzrechtlichen Vorgaben und damit Wegfall von nationalen Sonderbestimmungen z. B. bei der Bewertung, was personenbezogene Daten sind oder wie eine Übermittlung in Drittstaaten zu gestalten ist.

Die EU-DSGVO wird allerdings auch die Abstimmung von datenschutzrechtlichen Positionen erschweren. Denn die weiterhin national zuständigen Aufsichtsbehörden müssen sich – vereinfacht gesagt – bei grenzüberschreitend relevanten Fragen mit den anderen Aufsichtsbehörden der EU-Mitgliedsstaaten abstimmen. Dies wird sicherlich ein zeitintensiver Vorgang.

7 Fazit

Der jetzige Zustand mit national unterschiedlich aufgesetzten Regulierungen ist unzumutbar.

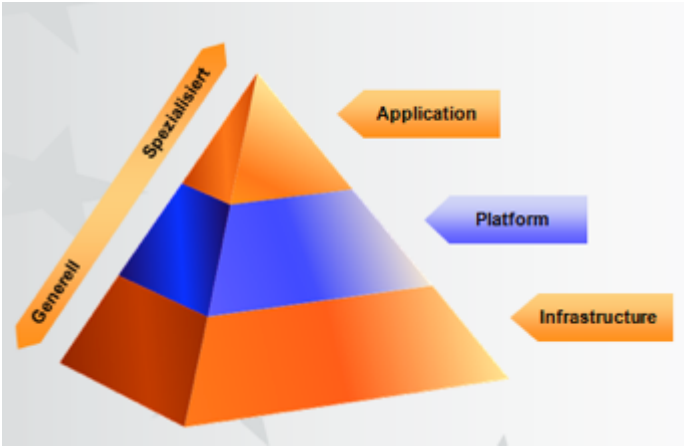
Der CPC schafft zwar Klarheit und eine inhaltliche Übersicht über die Vielzahl bestehender nationaler Regelungen.

Europäische Wettbewerbsfähigkeit, Digitaler Binnenmark und Vertrauensvolle Nutzung neuer IT Services ist nur möglich, wenn es in Europa eine einzige einheitlich gültige Regelung zum Datenschutz gibt. Wie man vorgehen könnte, zeigt der CPC.

8 Glossar Cloud Computing

„**Cloud Computing** ist ein Modell, das on-demand und online den Zugriff auf einen gemeinsamen Pool konfigurierbarer Computing-Ressourcen wie Netzwerke, Server, Speichersysteme, Anwendungen und Dienste ermöglicht. Diese können passgenau, schnell, kostengünstig und mit minimalem Verwaltungs-aufwand bereitgestellt und abgerufen werden." (Definition: NIST; National Institute of Standards and Technology, USA)

Als Grundansatz für die Darstellung der verschiedenen Elemente des Cloud Computings wird oftmals das **SPI-Modell** herangezogen, welches die drei Serviceebenen — Infrastruktur, Plattform und Software — darstellt:



Hierbei werden die Ebenen aufeinander aufbauend dargestellt, wobei die jeweils unteren Ebenen auch unabhängig von der darüber liegenden Ebene genutzt werden können.

Public Cloud: IT-Dienstleistungen werden von einem Cloud-Anbieter bereitgestellt und können von jedem über das Internet genutzt werden.

Private Cloud: IT-Dienstleistungen werden aus den eigenen Rechenzentren bezogen. Alle Dienste und die Infrastruktur unterstehen einer Institution. Die Cloud kann durchaus von Dritten betrieben werden. Auf die Dienste wird entweder über das Intranet oder über VPN (Virtual Private Network) zugegriffen.

Hybride Cloud: ist eine Mischform bestehend aus einer Public Cloud und einer Private Cloud.

Föderierte Cloud: Hybride Cloud mit spezieller Sicherheitstechnik durch vertrauenswürdige Service-Anbieter im Bereich der Identifikation und Verschlüsselung.

IaaS: Infrastructure as a Service: Bereitstellung von Rechen- und Speicherkapazitäten als Service.

PaaS: Platform as a Service: Bereitstellung von „Middleware" als Service.

SaaS: Software as a Service: Bereitstellung von Applikationen als Service.

XaaS: X as a Service: Bereitstellung von zusätzlichen Funktionen wie Geschäftsprozesse, Netzwerke, Kommunikation und weitere als Service.

9 Rechtlicher Hinweis

Allgemeines

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung spezieller rechtlicher Aspekte im Zusammenhang mit Cloud Computing, stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls voraussetzt.

Inhalt des Leitfadens

Der Herausgeber/die Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereitgestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen den Herausgeber/die Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

Verweise und Links

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z. B. „Links"), die außerhalb des Verantwor-tungsbereichs des Herausgebers/der Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem der Herausgeber/die Autoren von den Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Der Herausgeber/die Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben der Herausgeber/die Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wurden. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotenen Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht derjenige, der über Links auf die jeweilige Veröffentlichung lediglich verweist.

Urheberrecht

Die in diesem Leitfaden dargestellten Inhalte wie Texte, Graphiken oder Bilder sind nach dem österreichischen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

Vergütung

Dieser Leitfaden wird den Adressaten/Empfängern kostenlos zur Verfügung gestellt.

10 Autoren

Die Autoren dieses Leitfadens sind:



Dr. Tobias Höllwarth
EuroCloud Europe
tobias.hoellwarth@eurocloud.org



Dr. Christian Laux
Switzerland
christian.laux@lauxlawyers.ch



Dr. Clemens Thiele
Austria
anwalt.thiele@eurolawyer.at



Dr. Jens Eckhardt
Germany
eckhardt@juconomy.de

EuroCloud AUSTRIA

EUROCLOUD AUSTRIA

VEREIN ZUR FÖRDERUNG
VON CLOUD COMPUTING

MUSEUMSTRASSE 5/14
1070 WIEN, AUSTRIA

E-MAIL: INFO@EUROCLOUD.AT
WEB: HTTP://WWW.EUROCLOUD.AT