Neuerungen im europäischen Datenschutzrecht für Unternehmen

herausgegeben von

Christoph Grabenwarter
Ferdinand Graf
Mercedes Ritschl

mit Beiträgen von

Jens Eckhardt
Sabine Gölles
Christoph Grabenwarter
Ferdinand Graf
Manfred Hartl
Tobias Höllwarth
Bernhard Koch
Marija Križanac
Gerhard Kunnert
Christian Laux
Judith Leschanz
Clemens Thiele

Wien 2017
MANZ'sche Verlags- und Universitätsbuchhandlung

Zitiervorschlag: *[Autor]* in *Grabenwarter/Graf/Ritschl* (Hrsg), Neuerungen im europäischen Datenschutzrecht für Unternehmen (2017) [Seite]

ISBN 978-3-214-01239-7

Telefon: (01) 531 61-0
E-Mail: verlag@manz.at
www. manz.at
Datenkonvertierung und Satzherstellung: Druckerei Robitschek, 1050 Wien
Druck: Prime Rate Kft., Budapest

Cloud & Datenschutz

Der Cloud Privacy Check (CPC)

Jens Eckhardt, Düsseldorf/Tobias Höllwarth, Wien
Christian Laux, Zürich/Clemens Thiele, Salzburg

Übersicht:

I. Einleitung

Cloud-Computing ist zum fixen Bestandteil der IT-Sourcing-Strategie vieler Unternehmen geworden.

IT-, Legal- und Procurement-Verantwortliche in diesen Unternehmen müssen sich damit dem Umstand stellen, dass umfassendes Know-how in vielen Wissensbereichen – nicht nur in der Technik – erforderlich ist, wenn Cloud-Services verantwortungsbewusst, wirtschaftlich und rechtlich kompatibel zum lokal gültigen Rechtsrahmen eingesetzt werden sollen.

Bei strategisch geplanter Einführung und Nutzung von Cloud-Services ist unweigerlich zu Beginn das Thema Datenschutz einzubeziehen. Denn mit dem Einsatz von Cloud-Services werden Daten – und eben auch personenbezogene Daten – an andere zur Bearbeitung übergeben.

Mit der am 25. Mai 2018 in allen EU-Ländern verbindlich geltenden Europäischen Datenschutz-Grundverordnung (DSGVO) werden auf fundamentale und moderne Weise technische, ökonomische und juristische Rahmenbedingungen gelten. Die EU setzt damit ein deutliches und weltweit erkennbares Signal, wie eine Gesellschaft auf rasant voranschreitende technische Möglichkeiten und deren Konsequenzen für die Menschen reagieren kann. Die Herausforderungen für Anbieter wie Nutzer moderner IT-Services sind nicht zu unterschätzen. Sich rechtzeitig darauf vorzubereiten ist ein „Muss".

Der Cloud Privacy Check (CPC) ist ein Baustein im Rahmen des Streams „Cloud Know-how", den EuroCloud Europa setzt, um ein komplex wirkendes Thema für Betroffene einfach darzustellen und eine geeignete und praktikable Handlungsweise aufzuzeigen. Der CPC ersetzt nicht juristische Fachexpertise, aber er strukturiert und vereinfacht ein komplexes Thema ohne Verlust von wesentlichen Informationen.

Der CPC ordnet damit die Fragestellungen, die Cloud-Nutzer stellen und Cloud-Provider beantworten müssen, um den Datenschutz bei der Nutzung von Cloud-Services transparent und nachvollziehbar zu machen – eine ebenfalls grundsätzliche Forderung der Datenschutz-Grundverordnung (Art 5 DSGVO).

Der Cloud Privacy Check wurde durch die Autoren entwickelt und im Rahmen des Europäischen CPC-Netzwerks, eines Verbunds von Rechtsanwälten, überprüft und ist damit das Ergebnis der Zusammenarbeit von Anwaltskanzleien aus rund 30 Ländern. Die hier beschriebenen Informationen, also der CPC und die Länderreports, sind auch auf der CPC-Website abrufbar: cloud-privacycheck.eu.

A. 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 nicht zuletzt auch deshalb kritisch, weil die Übertragung von personenbezogenen Daten an einen Dritten (einen Auftragnehmer), unter Umständen sogar in ein anderes Land, ein Vorgang ist, der grundsätzlich strengen juristischen Rahmenbedingungen unterliegt.

Mit anderen Worten: Wird bei diesem Outsourcing ein grober Fehler gemacht, kann das neben einem hohen Reputationsschaden auch ernste kommerzielle und juristische Konsequenzen haben. Nicht zu übersehen ist auch, dass der Bußgeldrahmen der DSGVO für ein nicht datenschutzkonformes Outsourcing mit einem Bußgeldrahmen bis 20 Millionen Euro oder 4 Prozent des weltweiten Vorjahresumsatzes des Unternehmens, je nachdem was höher ist, sanktioniert ist.

B. Wir machen es uns schwer

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

Mit dem Anwendungsbeginn der DSGVO am 25. 5. 2018 wird zwar der Datenschutzrechtsrahmen in der EU vereinheitlicht, sodass die nationalen Besonderheiten zurücktreten. Dafür tritt eine neue Unsicherheit auf: die Anwendung der DSGVO im Rahmen der Nutzung von Cloud-Services. Denn die DSGVO setzt einen neuen Rechtsrahmen, der nicht mehr in der jeweiligen nationalen „Rechtstradition" angewendet werden kann, sondern zu einer EU-weit einheitlichen Anwendung der Regelungen der DSGVO zwingt. Es entstehen damit Unsicherheiten, wie die neuen und zugleich recht komplexen Vorgaben der DSGVO im konkreten Anwendungsfall anzuwenden sind. Gerade in der Übergangszeit nach Anwendungsbeginn bis zu einer gefestigten Auslegung und Anwendung der Vorgaben der DSGVO bedarf es wieder Leitlinien, die der CPC bietet.

Fazit: Das Datenschutzrecht ist und bleibt ein komplexes Thema. Obgleich die DSGVO eine unionsweite Vereinheitlichung des Rechtsrahmens bringt, schafft sie auch neue Unklarheiten und Unsicherheiten. Der CPC ist – und bleibt gerade auch unter der DSGVO – ein Kompass, welche Fragen der Cloud-Nutzer sich stellen muss und der Cloud-Provider beantworten muss, um sich datenschutzrechtlich bei der Nutzung von Cloud-Services zu orientieren.

C. Die Methodik des CPC

Der CPC stellt aufgrund seiner länderübergreifenden Erstellung bereits heute eine Abhilfe gegen die Unklarheiten dar und wird es auch unter der Geltung der DSGVO ab dem 25. 5.2018 sein. Denn die durch den CPC herausgearbeiteten Kernfragen basieren auf den Eckpunkten der DS-RL 95/46/EG, die sich auch in der DSGVO fortsetzen. Die DSGVO löst die DS-RL 95/46/EG ab.

Die DSGVO geht aber noch weiter als die RL 95/46/EG. Denn die DSGVO gilt als EU-Verordnung – anders als eine EU-Richtlinie – in jedem EU-Mitgliedstaat unmittelbar. Das bedeutet konkret, dass die Regelungen der DSGVO in jedem EU-Mitgliedstaat anzuwenden sind. Es bedarf für die Umsetzung der Grundsätze der DSGVO keines nationalen Umsetzungsgesetzes. Gleichzeitig bedeutet das auch, dass nationale Gesetze grundsätzlich nicht mehr anwendbar sind.

Dieser Leitfaden soll gemeinsam mit dem Cloud Privacy Check (CPC) und den Länderreports eine solche Abhilfe darstellen, indem er sich dreier methodischer Ansätze bedient:

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 die grundsätzlichen Fragen aller Cloud-

Nutzer und Cloud-Provider eine verständliche und tragfähige Informationsbasis zu liefern. Eine individuelle rechtliche Beratung wird dadurch nicht ersetzt, aber die Bewertung auf einem gemeinsamen Nenner für Cloud-Nutzer und Cloud-Provider sowie für Datenschutzaufsichtsbehörden und Betroffene strukturiert.

Strukturierung

Der CPC bietet eine 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.

Separierung

Separierung des Allgemeingültigen vom Speziellen. Das ist wohl die entscheidendste Hilfe zur Bewältigung einer komplexen, grenzüberschreitenden Herausforderung. Es muss also möglich sein, ganz rasch und einfach die Informationen zu erhalten, die einheitlich 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.

II. Datenschutz und Cloud-Computing

A. 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 Europäischen Wirtschaftsraums ist die DS-RL 95/46/EG. In einigen Ländern (zB Österreich und außer der EU/EWR bspw Schweiz) sind durch das jeweilige nationale Datenschutzrecht auch die Daten juristischer Personen durch das Datenschutzrecht geschützt. Die DSGVO sieht nur den Schutz der Daten von natürlichen Personen vor.

Entscheidend für die Bewertung im Unternehmen ist die Ausrichtung des Datenschutzes: Der Schutz von Personendaten – also der Datenschutz – bezweckt den Schutz von Personen. Es sind also nicht die Daten, die als Selbstzweck geschützt werden sollen. Diese Unterscheidung zeigt sich häufig bei technischen Schutzkonzepten, die am Schutz von Daten zum Schutz der Funktionsfähigkeit des Unternehmens ausgerichtet ist, während das Datenschutzrecht technisch-organisatorischen Schutz der Daten mit dem Ziel des Schutzes der Person fordert. Die konkreten Maßnahmen können sich überschneiden, das Schutzziel unterscheidet sich aber (vgl Art 32, 35 DSGVO).

Zum **Schutz der Privatsphäre** gewährt das Datenschutzrecht vor allem ein Recht auf **Vertraulichkeit personenbezogener Daten,** soweit ein schutzwürdiges Interesse daran besteht.[1] 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 sowie mit der DSGVO der Datenportabilität).

Das Datenschutzrecht ist von einem Regel-Ausnahme-Prinzip geprägt. Wer Personendaten Dritter bearbeitet, bedarf dazu eines Rechtfertigungsgrundes. Das gilt bereits heute im nationalen Datenschutzrecht und wird durch Art 6 der DSGVO fortgeschrieben.

Regeln des Datenschutzrechts kommen ungeachtet vertraglicher Regeln zur Anwendung. Datenschutzrechtliche Regelungen gelten für jede Art von Datenverarbeitung, online ebenso wie offline.[2]

B. 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:

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 es 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.

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

[1] Art 1 Abs 1 DS-RL.

[2] Der EuGH hat dies bereits im Jahr 2003 in der Rs *Lindqvist* festgestellt: EuGH 6. 11. 2003, C-101/01.

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.

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.

C. Zwei Kernregeln des Datenschutzrechts

Das Datenschutzrecht stellt zwei zentrale 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, als würde der CSC die Daten auf seinen eigenen Systemen ohne Einschaltung eines CSP bearbeiten.

CSP als Auftragsverarbeiter[3]: Der Cloud-Service-Provider (CSP) wird datenschutzrechtlich als sogenannter Auftragsverarbeiter 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.

III. Cloud Privacy Check (CPC)

A. 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.

[3] Die DSGVO verwendet den Begriff Auftragsverarbeiter, weshalb dieser auch in diesem Beitrag verwendet 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 und vor allem auch nach der DSGVO 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" oder „Der rechtliche Werkzeugkasten") datenschutzkonform beantworten lassen.

Figure III-1

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

B. 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, weshalb 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.

Der Cloud-Service-Provider (CSP)

Der CSP 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.

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]

C. 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 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 cloud-spezifischen Datenschutzfragen. Mit diesen befasst sich der CPC.

D. Grundüberlegung zum CPC

Kriterium 1. Personenbezogene Daten (vgl Art 4 Nr. 1 DSGVO): Der CPC kommt zum Tragen, wenn personenbezogene Daten eines CDS bearbeitet werden. Denn nur dann ist der Anwendungsbereich des Datenschutzrechts eröffnet (vgl Art 2 Abs 1 DSGVO).

Kriterium 2. Beizug eines Dritten: Das zweite Kriterium trägt dem Umstand Rechnung, dass Cloud-Services durch externe Dienstleister erbracht werden. Denn der Zugriff eines Dritten auf die durch den CSC verarbeiteten personenbezogenen Daten bedarf einer datenschutzrechtlichen Rechtfertigung.

[4] Siehe oben Abschnitt II.B.

[5] Siehe außerdem die Ausführungen in Abschnitt IV.B.

Kriterium 3. Auslandsbezug: Externe Dienstleister erbringen ihre Leistungen oft im bzw. aus dem Ausland heraus. Für eine grenzüberschreitende Datenverarbeitung stellen sich zusätzliche Zulässigkeitsfragen neben dem Kriterium 2 (vgl Art 44 ff DSGVO).

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. Hierfür stellen sich dann die beiden vorgenannten Fragen (vgl Art 28 Abs 2 und Abs 4 DSGVO).

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

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

E. 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 vier Schritte werden unter Abschnitt IV.B im Einzelnen dargestellt.

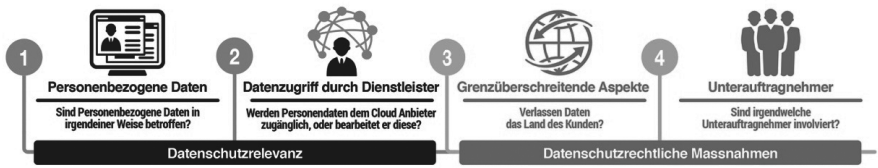

Figure III-2

IV. Rechtliche Erläuterungen zu den einzelnen CPC-Schritten

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

A. Die Toolbox

Die einzelnen nachstehend dargestellten Maßnahmenpakete werden jeweils im Kontext der jeweiligen Schritte und unter Abschnitt V näher betrachtet.

Figure IV-1

Eine Cloud-Lösung wird aus datenschutzrechtlicher Sicht dann rechtmäßig eingesetzt, wenn die richtigen Instrumente dafür verwendet werden.

Cloud-Nutzungsvertrag

Figure IV-2

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 (zB 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:

Vertrag betreffend die Auftragsverarbeitung

Figure IV-3

Die Vereinbarung über die Auftragsdatenverarbeitung ist ein Vertrag, für den das jeweils nationale Recht sowie ab dem 25. 5. 2018 die DSGVO einheitlich für die EU-Mitgliedstaaten inhaltliche Vorgaben vorsieht[6]. Werden diese Anforderungen berücksichtigt, handelt es sich dabei um eine datenschutzrechtlich privilegierte Einbindung eines Dienstleisters.

Daher handelt es sich um eine vorzugswürdige Ausgestaltung der Einbindung von Auftragnehmern.

Maßnahmen bei Grenzüberschreitung

Figure IV-4

Das Maßnahmenpaket „Grenzüberschreitung" umfasst Leitlinien zur datenschutzkonformen Ausgestaltung der grenzüberschreitenden Datenverarbeitung. Es bestehen Unterschiede, je nachdem, in welches Land die Daten übertragen werden.[7]

Maßnahmen zur Einbindung von Subunternehmern

Figure IV-5

Das Maßnahmenpaket „Unterauftragnehmer" umfasst Leitlinien zur Einbindung von Subunternehmern durch den Cloud-Service-Provider. Hierfür

[6] Siehe hierzu die Darstellung der Besonderheiten der nationalen Rechtsordnungen (Abschnitt V).

[7] Nationale Besonderheiten werden wiederum unter Abschnitt V dargestellt.

ergeben sich sowohl aus der Vereinbarung über die Auftragsdatenverarbeitung und eine eventuelle weitere grenzüberschreitende Datenverarbeitung besondere Anforderungen.[8]

Mitteilungen an den Kunden zur Erhöhung der Transparenz

Figure IV-6

Gerade bei der Einbindung von Subunternehmern entsteht eine Transparenzpflicht des CSP gegenüber dem CSC. Diesem Umstand trägt das Tool „Mitteilung zur Erhöhung der Transparenz" Rechnung. Art 20 DSGVO sichert jedem CDS das Recht auf Datenübertragbarkeit zu. Unter der DSGVO ergeben sich insgesamt deutlich mehr Anforderungen an die Transparenz, welche durch den CSC zu beachten sind.[9]

B. Das Vier-Schritte-Modell

Schritt 1: Personenbezogene Daten

Figure IV-7

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?

Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die di-

[8] Die Anforderungen der einzelnen Rechtsordnungen werden auch hierfür unter Abschnitt V dargestellt.

[9] Unter Abschnitt V werden Details zu Informationsumfang und Informationstiefe beschrieben.

rekt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann" (Art 4 Z 1 DSGVO).

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.

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 wird)

Manchmal ist es schwer zu bestimmen, ob personenbezogene Daten vorliegen. Mit dieser Frage hat sich der EuGH in der Rs *Breyer*[10] aufgrund der Vorlage des deutschen Bundesgerichtshofs befasst[11].

Anonymisierte Informationen fallen nicht in den Anwendungsbereich der Datenschutzgesetze (vgl ErwGr 26 DSGVO). 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 NEIN – dh sind die Daten nicht personenbezogen –, sind keine datenschutzrechtlichen Instrumente erforderlich. Es bleibt dann beim Nutzungsvertrag zwischen Cloud-Anbieter und Cloud-Kunden.

Ist die Antwort JA – dh liegt ein Personenbezug vor –, muss die zweite Prüfung des Cloud Privacy Checks durchgeführt werden.

Zu beachten ist, dass nationale Unterschiede bestehen können, ob neben den durch die DSGVO geschützten natürlichen Personen auch juristische Personen durch das Datenschutzrecht geschützt werden. Obgleich die DSGVO als EU-Verordnung in allen EU-Mitgliedstaaten unmittelbar gilt, ist es nicht offensichtlich ausgeschlossen, dass nationale Gesetzgeber auch juristischen Personen den gleichen Schutz durch nationales Recht gewähren.

[10] EuGH 19. 10. 2016, C-582/14, *Breyer/Deutschland*.

[11] Ausführlich hierzu *Eckhardt*, ZIIR 2017/1, 6 ff.

Schritt 2: Drittzugriff

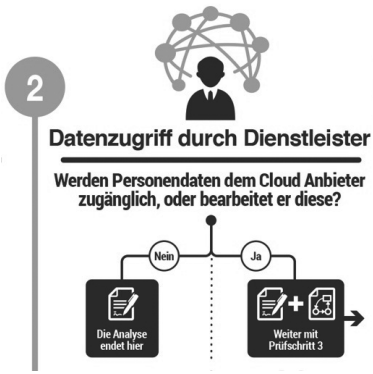

Figure IV-8

Die datenschutzrechtliche Anforderung, einen Dritten datenschutzkonform einzubinden, stellt sich nur, wenn der Dritte (gemeint ist der CSP) Zugriff auf personenbezogene Daten hat. Welche Art von Zugriff erforderlich ist, ist für die ab dem 25. 5. 2018 anzuwendende DSGVO derzeit noch nicht abschließend geklärt.

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 also JA, dann muss nach der zweiten Prüfung nun die dritte Prüfung ausgeführt werden.

Schritt 3: Grenzüberschreitende Aspekte

Figure IV-9

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" waren bislang von Land zu Land verschieden. Neu ist die Rechtslage mit der DSGVO in der EU vereinheitlicht. Aggregiert lässt sich die Rechtslage aus der europäischen Warte wie folgt darstellen:

(1) Wenn der Cloud-Dienstleister (CSP) keinen Bezug zu einer Rechtsordnung außerhalb der EU/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 (zB 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; Art 46 DSGVO nennt weitere Rechtfertigungsgründe.

Der EuGH hat mit Urteil vom 6. 10. 2015 die sogenannten Safe-Harbor-Principles in der Fassung der Entscheidung der EU-Kommission 2000/520/EG vom 26. 7. 2000 für unwirksam erklärt. Diese Safe-Harbor-Principles sind damit keine Rechtsgrundlage mehr für einen Datentransfer. Die EU und die USA haben sich auf das Nachfolgeabkommen EU-US Privacy Shield verständigt, das dem Safe-Harbor-Principle vergleichbar ist, aber mit mehr Schutz für die betroffenen EU-Bürger verbunden sein soll. Daneben bieten sich andere Maßnahmen an (insbesondere EU-Standardvertrag oder Processor Binding Corporate Rules).[12]

Für den CPC bedeutet dies Folgendes:

Ist die Antwort 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.

[12] So die Stellungnahme der Artikel-29-Datenschutzgruppe vom 16. 10. 2015: „In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgement on other transfer tools. *During this period, EU-data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used.*"

Schritt 4: Unterauftragnehmer

Figure IV-10

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 (CSC):

a) Vereinbarung betreffend Auftragsdatenverarbeitung

b) Die Maßnahmen gemäß Prüfstufe 3 sind erforderlich, wenn der Unterauftragnehmer 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.

(3) Maßnahmen, die im Verhältnis zwischen dem Cloud-Kunden (CSC) und dem Unterauftragnehmer greifen: Eine im Direktverhältnis geschlossene 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. Das Verfahren ist unter der DSGVO neu vereinheitlicht worden. Bislang galt diesbezüglich Folgendes:

In Österreich erforderte dies eine Genehmigung von der Aufsichtsbehörde; in Deutschland war eine Genehmigung erforderlich; in der Schweiz reichte 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.

V. 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 Abschnitt IV.A) hält die Antworten zur datenschutzkonformen Gestaltung der Cloud-Nutzung aus Kundensicht (Sicht des CSC) bereit.

Die am 25. 5. 2016 in Kraft getretene und ab dem 25. 5. 2018 anzuwendende Datenschutz-Grundverordnung (DSGVO) vereinheitlicht den Datenschutz-Rechtsrahmen in der EU. Für die durch den CPC angesprochenen Aspekte gibt es damit in den EU-Mitgliedstaaten praktisch keine nationalen Unterschiede mehr.

Nationale Besonderheiten ergeben sich nur noch dort, wo die DSGVO hierfür Raum lässt. Über die Rechtslage bis zum 25. 5. 2018 kann man sich in den sogenannten „Country Reports" des CPC leicht einen Überblick verschaffen.

VI. 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 Verwaltungsaufwand bereitgestellt und abgerufen werden." *(Definition: NIST; National Institute of Standards and Technology, USA)*

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 Serviceanbieter 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.

CSC: Cloud-Service-Customer (Kunde)

CSP: Cloud-Service-Provider (Anbieter)

CDS: Cloud-Data-Subject oder betroffene Person