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.