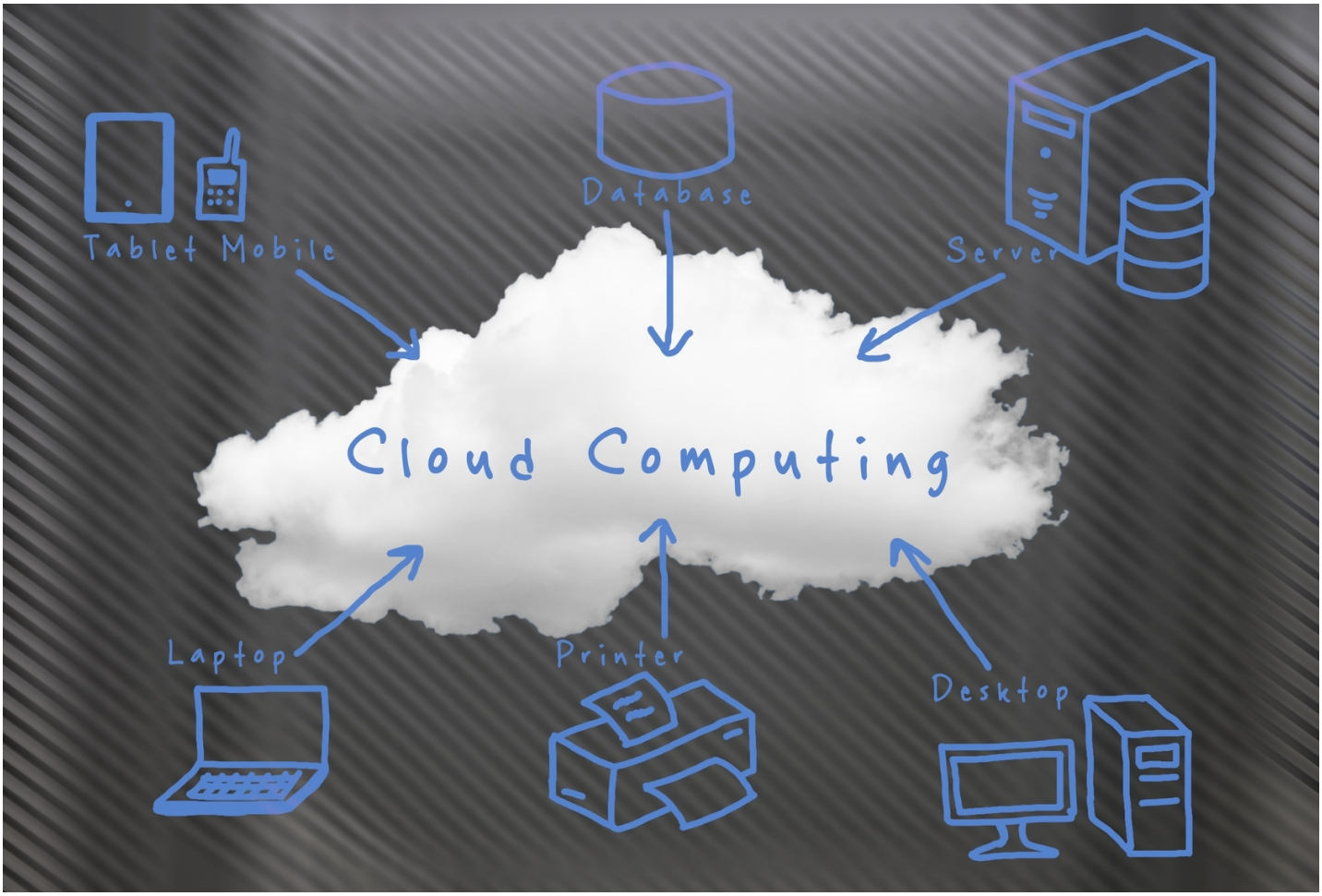
Eine paradoxe Wolke vernebelt die Realitäten des Datenschutzrechts

Cloud-Computing

Wenn man der Werbung glaubt, dann leben wir in einer schönen neuen Welt ohne Grenzen. Persönliche Daten sind hilfreich und nützlich, sie schwirren um die Welt, um uns in eine Wolke des Glücks einzuhüllen: Die Cloud. Das Problem: Dieser Glaube und die Realität liegen gar nicht mal so weit auseinander.

Dr. Kai Stumper
Rechtsanwalt

Stand: 28.11.2014



Was versteht man eigentlich unter Cloud-Computing?

Cloud-Computing könnte man übersetzen mit „Rechnen in Wolke“. Man meint damit das grenzüberschreitende, dynamische Speichern und Verarbeiten von Daten auf wechselnden Servern rund um die Welt.

Weltumspannendes Cloud-Computing: Nach deutschem Recht fast unmöglich

Was im Bereich Cloud-Computing und Datenschutz tatsächlich weit auseinander klafft, sind die wirtschaftlich erstrebte und die rechtlich gebotene Realität. Die „Cloud“, also das grenzüberschreitende, dynamische Speichern und Verarbeiten von Daten auf wechselnden Servern rund um die Welt, ist längst Realität. Es ist eine kostengünstige, effiziente und praktische Realität.

Sie lässt sich sogar rechtlich sauber abbilden. Allerdings liegt da auch die Quelle des oben genannten Problems: wer das versucht, unternimmt gleichzeitig die Quadratur des Kreises. Denn der Aufwand für eine rechtlich saubere Abbildung von Cloud-Computing-Datenflüssen ist umso höher, je weiter sie zunächst Deutschland und dann den EU-Raum verlassen sollen.

Er ist am Ende so hoch, dass jeglicher Effizienzgewinn in sich zusammensinkt. Man kann also durchaus sagen, dass wirtschaftlich attraktive Cloud-Lösungen und rechtlich saubere Cloud-Lösungen sich tendenziell gegenseitig ausschließen, je internationaler sie sein sollen.

In der Cloud: Wo ist das Datum zu welcher Zeit?

Der Grund für dieses scheinbare Paradox liegt im Grundkonzept des Datenschutzrechts, dass nun mal bis heute von einem raumgebundenen Konzept ausgeht. Das bedeutet, die Zulässigkeit des Umgangs mit Daten fragt auch immer danach, ob das Datum seinen physikalischen Aufenthaltsort verändert. Geschieht das, so muss juristisch gesehen im selben Augenblick auch geprüft werden ob, und unter welchen Voraussetzungen dies überhaupt erlaubt sein könnte.

Bezugspunkt dafür ist die „verantwortliche Stelle“. Da dies in der Regel die Unternehmen selbst sind, ist jede Übertragung von Daten zwischen zwei Unternehmen ein datenschutzrechtlich relevanter und sensibler Vorgang.

Für personenbezogene Daten von Arbeitnehmern bedeutet das:

- sie dürfen nicht einfach an andere Unternehmen weitergeleitet werden
- auch nicht innerhalb desselben Konzerns
- wenn nicht besondere und mitunter sehr komplexe Erlaubnisse hierfür gefunden werden können
- und dies alles gilt umso intensiver und umso komplexer, sobald nationale Grenzen überschritten werden
- und zwar erst Recht, wenn es sich um Grenzen zu Staaten außerhalb der EU handelt.

Thema Datenschutzrecht: Die Wolke ist kein rechtsfreier Raum

Vor diesem Hintergrund können Cloud-Lösungen noch diesseits der oben genannten Paradox-Grenze halbwegs ökonomisch sinnvoll existieren, wenn sie sich auf den innerdeutschen oder den EU-Raum beschränken. Spätestens danach öffnet sich das Paradoxon.

Solange daher das Grundkonzept des Datenschutzrechts nicht verändert wird, solange werden Cloud-Lösungen unter diesem Mangel leiden und solange wird es Aufgabe eines Betriebsrates sein, sehr genau hinzuschauen, wenn das Unternehmen Arbeitnehmerdaten in Cloud-Modellen verarbeiten möchte. Die Vermutung der Rechtswidrigkeit liegt hier sehr nahe.

Denn Cloud-Lösungen schweben nicht etwa wolkenartig in einem rechtsfreien Kosmos. Ganz im Gegenteil. Das Datenschutzrecht gilt selbstverständlich. Und nur weil jemand es günstiger, angenehmer, leichter, gewinnträchtiger oder sonst wie vorteilhafter findet, Dinge zu tun, die unzulässig sind, werden sie dadurch nicht zulässig.

Und es gibt auch kein spezielles „Cloud-Datenschutzrecht“, zumindest nicht im Bereich des Arbeitsrechts. Probleme im Umgang mit Cloud-Konzepten sind also mit ganz herkömmlichem, altbekanntem Datenschutz-Handwerk zu lösen.

Am Recht auf Informationelle Selbstbestimmung hängt kein Preisschild.

Und wenn dann das Ergebnis dieser Lösungen in vielen Fällen so aussieht, dass die gewünschten Konzepte unzulässig sind, dann ist das auch vom Arbeitgeber zu akzeptieren. Es gibt keinen Rechtssatz, wonach das Grundrecht auf informationelle Selbstbestimmung irgendeinen Kaufpreis hat. Selbstverständlich findet eine Grundrechtsabwägung statt und auch der Arbeitgeber hat ein Recht am Gewerbebetrieb und seinem Eigentum. Aber diese Abwägung fällt sehr oft zugunsten des Datenschutzes aus und nicht umgekehrt.

Wenn also bereits mit dem vorhandenen Instrumentarium auch das Thema Cloud in den Griff zu bekommen ist, dann müsste hier eigentlich nichts weiter erwähnt werden. Cloud-Konzepte sind daran zu messen und sie sind häufig unzulässig.

Meistens geht es um Auftragsdatenverarbeitung

Übersehen wird dabei auch oft, dass im Verhältnis zwischen Cloud-Anwender und Cloud-Anbieter, also dem Servicedienstleister, der das Cloud-Hosting betreibt, in der Praxis meistens eine Situation vorliegt, die datenschutzrechtlich der Beziehung zwischen Auftraggeber und Auftragnehmer entspricht.

Damit wird bereits deutlich, dass ein Cloud-Anwender an sämtliche Vorgaben des §§ 11 BDSG gebunden ist. Dazu gehört auch die Klärung der Frage

- ob und unter welchen Bedingungen der Cloud-Anbieter Unterauftragsverhältnisse eingehen darf und
- wie bei Verstößen gegen das Datenschutzrecht, insbesondere durch Unterauftragnehmer, ggf. durch Vertragsstrafe-Regelungen, der Schaden begrenzt werden kann.

Der Cloud-Anwender muss also mit seinem Cloud-Anbieter vertragliche Vereinbarungen treffen, die, wie oben schon gesagt, tendenziell die gewünschten Vorteile der Cloud wieder aufheben.

Sobald ein Auslandsbezug ins Spiel kommt, muss der Cloud-Anwender als Auftragsdatenverarbeiter vorher (!) wissen, wo sich seine Daten jeweils aufhalten werden. Er benötigt folglich einen Cloud-Anbieter, der ihm vor der Verarbeitung und zu jedem Zeitpunkt während der Verarbeitung sagen kann, wo sich seine Daten geographisch aufhalten. Wie gesagt: das scheint paradox.

Bei sensiblen Daten hört der Spaß ganz auf

Gänzlich unmöglich ist ein Datentransfer ins Ausland bei sensiblen Daten gem. § 3 IX i.V.m. 28 VI BDSG, es sei denn, der Betroffene hätte ausdrücklich eingewilligt.

Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Eine Einwilligung im internationalen Kontext außerhalb der EU müsste im Übrigen ausdrücklich beinhalten, dass das Datenschutzniveau am Zielort geringer ist, als am Quellort, um dem Einwilligenden eine informierte und damit wirksame Einwilligung unterstellen zu dürfen.

Kontakt zur Redaktion
Haben Sie Fragen oder Anregungen? Wenden Sie sich gerne direkt an unsere Redaktion. Wir freuen uns über konstruktives Feedback!
redaktion-dbr@ifb.de