Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Erläuterungen zu Cloud Computing

Immer mehr Unternehmen und Behörden/Institutionen lagern ihre bisher typischerweise intern erledigten Datenverarbeitungen an externe Unternehmen aus («Outsourcing») und setzen dafür auf «Cloud Computing». Die Anwendungen (und Daten) befinden sich nicht mehr im eigenen Netzwerk, sondern in der Cloud. Der Zugang zu Daten, Services und Infrastruktur, die in der Cloud zur Verfügung gestellt werden, erfolgt mittels Fernzugriff (remote access).

Cloud Computing (deutsch: «rechnen in der Wolke») ist ein Begriff aus der Informationstechnik (IT). Er bedeutet, vereinfacht gesagt, dass Software, Speicherkapazitäten oder Rechnerleistung über ein Netzwerk, zum Beispiel das Internet, oder innerhalb eines Virtual Private Network (VPN) bedarfsorientiert bezogen, d.h. gemietet werden. Die IT-Landschaft (z.B. Rechenzentrum, Datenspeicher, Mail- oder Kollaborationssoftware, Entwicklungsumgebungen oder Spezialsoftware wie Customer Relationship Management [CRM]) steht nicht mehr im Eigentum des Unternehmens oder der Behörde und wird nicht mehr von diesen selbst betrieben, sondern von einem oder mehreren Cloud-Service-Anbietern als Dienstleistung (Service) gemietet.

Die verschiedenen Varianten von Cloud Computing unterscheiden sich in Bezug auf Organisationsform und Servicemodell.

Organisationsformen

Es wird zwischen Private, Public, Hybrid und Community Cloud unterschieden.

In einer Public Cloud wird die Infrastruktur vollständig durch den Cloud Anbieter bewirtschaftet und bestimmt. Der Cloud-Nutzer hat diesbezüglich nichts zu sagen und kann beispielsweise keinen Einfluss auf die Serverstandorte nehmen. Anders dagegen die Private Cloud: Sie wird durch ein Unternehmen selbst oder durch einen externen Dritte betrieben und ist immer nur auf das jeweilige Unternehmen ausgerichtet. Eine solche Lösung ist viel sicherer, jedoch auch kostspieliger. Werden eine Public und eine Private Cloud gleichzeitig und parallel genutzt, spricht man von einer Hybrid Cloud. Eine Community Cloud schliesslich ermöglicht es verschiedenen Organisationen, dieselbe Infrastruktur gemeinsam zu nutzen.

Servicemodelle

Es gibt drei Typen von Servicemodellen: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) sowie Software as a Service (SaaS).

IaaS betrifft die Beherbergung: Der Cloud-Anbieter stellt in der Cloud einen Server zur Verfügung, auf dem die Cloud-Nutzer ihre Daten oder Anwendungen abspeichern können. Verantwortlich für das Funktionieren des Netzes, dessen Zugang, der Hardware etc. ist allein der Cloud-Anbieter. **PaaS** beschlägt die Bearbeitung von Daten: Der Cloud-Anbieter entwickelt eine Anwendung und stellt diese den Nutzern in der Cloud zur Verfügung. Die Bewirtschaftung der Daten mittels dieser Anwendung erfolgt jedoch durch den Nutzer selber. Bei **SaaS** ist der Cloud-Nutzer nur noch Konsument in der Cloud. Er bewirtschaftet nichts mehr selber, weder die Anwendungen noch die Daten. Ihm wird einzig in der Cloud eine Funktionalität zur Verfügung gestellt, um dort Daten bearbeiten zu können.

Die **Hauptgründe** für den Einsatz von Cloud-Computing-Systemen sind geringere Kosten für IT-Infrastruktur und Software, Software Updates on Demand, höhere Rechenleistung, dynamischer Speicherplatz (der gemietete Speicherplatz in der Cloud wächst oder schrumpft mit den Daten, die dort abgelegt werden), Mobilität, schnelle und einfache Verfügbarkeit, Skalierbarkeit und in einigen Fällen auch verbesserte und erhöhte Sicherheit.

Risiken bei der Nutzung von Cloud Computing

Die Auslagerung von Daten ist immer mit Risiken verbunden. Auf das Cloud Computing treffen insbesondere die folgenden zu:

- **Kontrollverlust über die Daten:** Wegen der weltweiten Vernetzung und der Virtualität ist der Standort der Daten oft nicht erkennbar. Dies trifft im besonderen Mass für die Public Clouds zu. Der Cloud-Nutzer als verantwortlicher Dateninhaber weiss damit nicht, wo genau seine Daten in der Cloud gespeichert und verarbeitet werden. Er weiss oft auch nicht, ob Subunternehmer involviert sind und ob diese für einen angemessenen Datenschutz sorgen. Der Cloud-Nutzer kann somit seine datenschutzrechtlichen Pflichten hinsichtlich Gewährleistung der Datensicherheit, Gewährung des Auskunftsrechts oder Berichtigung und Löschung der Daten nicht (mehr) oder nur ungenügend wahrnehmen.

- **Fehlende oder mangelnde Abgrenzung/Isolierung der verschiedenen Datenverarbeitungen:** Dem Konzept von Cloud Computing ist inhärent, dass verschiedene Nutzer, die in keiner Beziehung zu einander stehen, ihre Daten in derselben Cloud und durch dasselbe System verarbeiten lassen (sog. *Multi-Tenant-Architektur*). Damit erhöht sich das Risiko, durch Attacken auf einen der Nutzer in Mitleidenschaft gezogen zu werden. Die eigenen Daten könnten also wegen Hackerangriffen oder Distributed Denial of Services Attacken (DDoS) nicht mehr verfügbar sein oder selbst «mitgehackt» werden. Es ist deshalb eminent wichtig, dass die Datenbearbeitungen der verschiedenen Cloud-Nutzer strikt voneinander getrennt werden und es nicht zu einer Vermischung der Daten kommt.

- **Compliance Risiken:** In der Cloud kann es vorkommen, dass Teile eines Datensatzes in verschiedenen weltweit verstreuten Rechenzentren liegen. Daraus ergeben sich Probleme nicht nur in Bezug auf die Gewährleistung von Datenschutz und Datensicherheit, sondern auch in Bezug auf die Einhaltung von anderen gesetzlichen Pflichten (Aufbewahrungs- oder Beweispflicht, Einhaltung von Geheimhaltungspflichten, etc.). Unternehmen und Behörden, die solche Dienste in Anspruch nehmen, sind sich oft zu wenig bewusst, dass die primäre Pflicht zur Einhaltung der Datenschutzregeln zunächst einmal bei ihnen selbst liegt und nicht beim Anbieter, der die Daten auf einem Cloud-Server speichert oder in der Cloud bearbeitet.

- **Zugriff von ausländischen Behörden auf die Daten:** In vielen Fällen werden die Daten für die Bearbeitung in der Cloud ins Ausland bekannt gegeben. Dabei werden die Daten oftmals auch in Ländern gespeichert oder bearbeitet, die über keinen (ausreichenden) Datenschutz verfügen. Cloud-Service-Anbieter sind aber auch gegenüber ausländischen Behörden und Gerichten verpflichtet, gegebenenfalls Zugriff auf Daten in der Cloud zu gewähren; dies gilt selbst dann, wenn die Daten nicht im Land der Behörde bearbeitet oder gespeichert werden.

- **Lock-in Effekte:** Ein weiteres Risiko ist die Abhängigkeit vom Cloud-Service-Anbieter und fehlende Portabilität und Interoperabilität. Das heisst, die Daten können wegen nicht vorhandener standardisierter Technologien und Schnittstellen nicht (mehr) oder nur mit grossem finanziellen und/oder technischem Aufwand ins eigene IT-System zurückgeführt oder zu einem anderen Cloud-Anbieter migriert werden.

Die nachfolgenden Risiken bestehen immer, unabhängig davon, ob die Datenbearbeitung in einer Cloud stattfindet oder nicht.

- **Datenverlust:** Daten können durch Diebstahl, Löschung, fehlerhafte Überschreibung oder sonstige Veränderung verloren gehen. Wenn keine entsprechenden Back-up-Systeme für die Originaldaten vorhanden sind, stellt dies ein enormes rechtliches Risiko dar und kann für ein Unternehmen möglicherweise existenzbedrohlich werden. Beispielsweise dann, wenn besonderes technisches Know-how, andere Geschäftsgeheimnisse (wie z.B. Kundenlisten oder Kalkulationsgrundlagen) oder die Finanzbuchhaltung betroffen sind. Zur Verhinderung von Datenverlusten müssen also entsprechende Sicherheitssysteme implementiert werden; solche Daten sollten nur zurückhaltend in die Cloud ausgelagert werden.

- **System- und Netzwerkausfälle sowie Nichtverfügbarkeit angemieteter Ressourcen und Services** können dazu führen, dass Daten verloren gehen oder unberechtigten Personen zugänglich werden und dass damit die Vertraulichkeit, Sicherheit und Integrität der Daten nicht mehr gewährleistet ist. Überdies können solche Ausfälle den Geschäftsbetrieb eines Unternehmens oder der Behörde massiv beeinträchtigen und nebst finanziellen Verlusten auch gravierende Reputationsschäden nach sich ziehen.

- **Missbrauch der Daten durch böswillig agierende Insiders oder Mitarbeitende**: Bei einem Outsourcing legt der Service-Anbieter unter Umständen nicht offen, wie die Zugriffsberechtigungen (physisch und virtuell) seiner Mitarbeitenden geregelt sind und wie diese diesbezüglich überwacht werden. Auch die Vertraulichkeitserklärungen sind für den Nutzer oft nicht einsehbar. Im Bereich Cloud Computing muss diesem Problem umso mehr Aufmerksamkeit gewidmet werden, wenn es um eine Public Cloud geht

Datenschutzrechtliche Anforderungen bei der Nutzung von Cloud-Computing-Diensten

1. Werden bei der Nutzung von Cloud Computing personenbezogene Daten bearbeitet, so liegt aus datenschutzrechtlicher Sicht normalerweise eine Datenbearbeitung durch Dritte im Sinne von Art. 10a DSG vor. Demnach kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten (hier: Cloud-Service-Anbieter) übertragen werden, **wenn die Daten nur so bearbeitet werden, wie der Auftraggeber (**hier: **Cloud-Nutzer) selbst es tun dürfte, und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.** Der Cloud-Service-Anbieter muss also verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt in gleichem Masse für allfällige Subunternehmer, die vom Anbieter beigezogen werden. Die Umsetzung dieses Erfordernisses bereitet in der Praxis jedoch Schwierigkeiten, da bei den Cloud-Computing-Anwendungen die Unterauftragsverhältnisse des Cloud-Service-Anbieters für den Cloud-Nutzer oft nicht transparent sind.

2. Weiter muss sich der Cloud-Nutzer vergewissern, dass der Cloud-Service-Anbieter als Dritter die Datensicherheit im Sinne von Art. 7 DSG und Art. 8 ff. bzw. 20 ff. VDSG gewährleistet. Das heisst, die Personendaten müssen durch angemessene **technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden**. Es muss für **Vertraulichkeit, Verfügbarkeit und Integrität der Daten** gesorgt sein. Der Cloud-Service-Anbieter muss die Daten gegen folgende Risiken schützen: unbefugte oder zufällige Vernichtung oder zufälligen Verlust; technische Fehler; Fälschung; Diebstahl oder widerrechtliche Verwendung; unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. Diese Massnahmen sind periodisch vor Ort zu überprüfen. Wie die Datenschutzanforderungen im Einzelnen umzusetzen sind, hängt vom Unternehmen bzw. der Behörde, von der Art der Daten, aber auch von der Organisation und des Zuschnitts der Cloud-Lösung (bspw. Private oder Public; IaaS, PaaS oder SaaS) ab. Als Grundregel gilt: Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) die Daten sind, umso eher ist von einer Auslagerung der Daten in die Cloud, insbesondere eine ausländische Cloud, abzusehen, und desto strikter und umfassender müssen die (Datenschutz-) Sicherheitsvorkehrungen und deren Kontrolle sein.

3. Die Nutzung von Cloud Computing bedingt in vielen Fällen eine **Datenbekanntgabe ins Ausland**, da die Verarbeitung oftmals auf weltweit verstreuten Servern stattfindet. Häufig werden dazu auch Subunternehmer beigezogen. Sehr oft geht es dabei um Länder, die ein tieferes Datenschutzniveau als die Schweiz aufweisen, so dass mit der Übermittlung dorthin die Gefahr einhergeht, dass mit diesen Daten Bearbeitungen durchgeführt werden, die in der Schweiz nicht erlaubt wären. Aus diesen Gründen dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen **angemessenen Schutz** gewährleistet (Art. 6 Abs. 1 DSG). Unter diesen Umständen können Personendaten nur ins Ausland bekannt gegeben werden, wenn eine der in Art. 6 Abs. 2 DSG aufgeführten Bedingungen erfüllt ist. In vielen Fällen wird der Cloud-Nutzer daher nicht umhin kommen, mit dem Cloud-Service-Anbieter (unter Einbezug allfälliger Subunternehmer) vertragliche Datenschutzgarantien abzuschliessen. Dabei besteht die praktische Schwierigkeit, dass alle Teilnehmer in der Cloud, auf deren Rechner personenbezogene Daten bearbeitet werden, vertraglich eingebunden werden müssen. Es ist zu bedenken, dass grundsätzlich derjenige, welcher Personendaten ins Ausland übermittelt, nachweisen muss, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.

4. Schliesslich ist der Cloud-Nutzer auch dafür verantwortlich, dass das Auskunftsrecht nach Art. 8 DSG und das Recht auf Löschung und Berichtigung nach Art. 5 DSG jederzeit gewährleistet sind und entsprechend den datenschutzrechtlichen Vorgaben umgesetzt werden. Die Einhaltung dieser Erfordernisse kann mit

erheblichen Schwierigkeiten verbunden sein, da mit der Nutzung von Cloud-Anwendungen wie erwähnt oftmals ein Kontrollverlust über die Daten einhergeht und der Cloud-Nutzer nicht (mehr) weiss, wo welche Daten bearbeitet werden. Er kann sich von diesen gesetzlichen Pflichten jedoch nicht befreien.

Schlussfolgerung

Die sorgfältige Auswahl (inkl. Risikobeurteilung), Instruktion und Überwachung des Service-Anbieters sind zentrale Elemente bei einer Datenbearbeitung in der Cloud. Der Cloud-Nutzer bleibt als Auftraggeber letztlich gegenüber den betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften und haftet bei allfälligen Verletzungen. Deshalb sollte er sich gut überlegen, welche Anwendungen und Daten er am eigenen Standort behalten will und welche in die Cloud wandern sollen. Zu diesem Zweck muss er im Vorfeld eine sorgfältige Prüfung des Cloud-Service-Anbieters und eine umfassende Risikoeinschätzung in organisatorischer, rechtlicher und technischer Hinsicht vornehmen. Bei der Auswahl der in Frage kommenden Cloud-Variante (Private Clouds, unternehmenseigene Public Clouds oder Hybrid Clouds) ist frühzeitig eine gründliche Analyse gerade auch der datenschutzrechtlichen Anforderungen vorzunehmen. Auf diese Weise kann von Beginn an eine datenschutzkonforme Gestaltung der Cloud gewährleistet werden. Besonderes Augenmerk sollte auf die Bearbeitung mit personenbezogenen Daten gelegt werden, was alle Schritte von der Speicherung über die Weiterverarbeitung bis hin zur Löschung mit einschliesst. Falls aufgrund der Risikoeinschätzung bezüglich der Verarbeitung von Personendaten in der Cloud Zweifel bestehen, ist von einer Auslagerung der Daten abzusehen.

Weiterführende Links:

- **ANSSI** L'Agence nationale de la sécurité des systèmes d'information, « Maîtriser les risques de l'infogérance », Décembre 2010, abrufbar unter : http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf(1)
- **BITKOM** Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., «Cloud Computing - Evolution in der Technik, Revolution im Business - BITKOM-Leitfaden», Oktober 2009, abrufbar unter: http://www.bitkom.org/de/themen/36129_61111.aspx(2) oder
- **BSI** Bundesamt für die Sicherheit in der Informationstechnik, «Sicherheitsempfehlungen für Cloud Computing Anbieter - Mindestsicherheitsanforderungen in der Informationssicherheit», Mai 2011, abrufbar unter: https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html(3)
- **CSA** Cloud Security Alliance, «Security Guidance for Critical Areas of Focus in Cloud Computing V2.1», December 2009, abrufbar unter : https://cloudsecurityalliance.org/csaguide.pdf(4)
- **ENISA** European Network and Information Security Agency, «Benefits, risks and recommendations for information security», November 2009, abrufbar unter: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment(5)
- **ENISA** European Network and Information Security Agency, «Security & Resilience in Governmental Clouds», January 2011, abrufbar unter: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds(6)
- **Fraunhofer Institut**, «Cloud-Computing für die öffentliche Verwaltung - ISPRAT-Studie», November 2010, abrufbar unter: http://www.cloud.fraunhofer.de/de/publikationen/isprat_cloud.html(7)

Zurück zur Übersicht Cloud Computing

Alle Links dieser Seite(n)

1. http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf
2. http://www.bitkom.org/de/themen/36129_61111.aspx
3. https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html
4. https://cloudsecurityalliance.org/csaguide.pdf
5. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-

assessment
6. http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
7. http://www.cloud.fraunhofer.de/de/publikationen/isprat_cloud.html

---

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) - 2014
http://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de