Beschluss des Rates der IT-Beauftragten der Ressorts vom 29. Juli 2015

Kriterien für die Nutzung von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung

1. Der IT-Rat hat mit Beschluss Nr. 2014/3 vom 12. Februar 2014 das BMI gebeten, einen Kriterienkatalog zum Einsatz von Cloud-Technologien in der Bundesverwaltung zu erarbeiten, der Mindestanforderungen statuiert in Bezug auf IT-Sicherheit, Datenschutz und zu Fragen von Interoperabilität und Standards, die Cloud-Dienste der IT-Wirtschaft erfüllen müssen, um durch die Bundesverwaltung in Anspruch genommen werden zu können.

2. Es ist zu beobachten, dass Softwarehersteller ihre Produkte zunehmend als Komplettdienstleistung – sogenannte Cloud-Dienste – anbieten, die auch den IT-Betrieb umfasst. Dort, wo Cloud-Angebote und Kauf-Software gemeinsam angeboten werden oder in Konkurrenz zueinander stehen, werden die Cloud-Angebote und der Fremdbetrieb gegenüber dem Kauf und dem Eigenbetrieb vom Cloud-Anbieter häufig als wirtschaftlich deutlich attraktiver dargestellt.

3. Die Bundesregierung hat es mit der Digitalen Agenda zu den Grundsätzen ihrer Digitalpolitik gemacht, die Autonomie und Handlungsfähigkeit der IT des Staates zu erhalten und insbesondere die technologische Souveränität für die IT des Staates zu stärken.

4. Der Einsatz von Cloud-Diensten der IT-Wirtschaft durch die Bundesverwaltung sollte daher erst nach sorgfältiger Abwägung von Risiken unter anderem für die IT-Sicherheit, der wirtschaftlichen und praktischen Folgen und der entsprechenden Mehrwerte erfolgen.

Vor diesem Hintergrund fasst der IT-Rat im Umlaufverfahren folgenden

Beschluss Nr. 2015/5

1. Cloud-Dienste im Sinne dieses Beschlusses sind Software-as-a-Service-, Platform-as-a-Service- und Infrastructure-as-a-Service-Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.

2. Vor Inanspruchnahme und Beschaffung von Cloud-Diensten der IT-Wirtschaft ist zu prüfen, ob vergleichbare und anforderungsgerechte Leistungen durch die Bundesverwaltung selbst oder im Auftrag der Bundesverwaltung durch Dritte bereitgestellt werden. Dies schließt bundeseigene Inhouse-Gesellschaften mit ein. Sofern dies der Fall ist, ist die Nutzung dieser Leistungen zu bevorzugen.

3. Die Einrichtungen des Bundes werden ihre Planungen, Bedarfsbeschreibungen und Vergaben zur etwaigen Verwendung von Cloud-Diensten der IT-Wirtschaft nach folgenden Grundsätzen ausrichten:

   a. Von den Einrichtungen des Bundes gehaltene schützenswerte Informationen (z. B. Betriebs- und Geschäftsgeheimnisse, sensible Daten über IT-Infrastrukturen des Bundes) müssen ausschließlich in Deutschland verarbeitet werden. Cloud-Anbieter müssen eine Vertraulichkeitsvereinbarung abschließen, nach der diese Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Zugriffsmöglichkeiten gelangen dürfen, die sich außerhalb der Bundesrepublik Deutschland gegen Cloud-Anbieter richten können.

   b. Werden von einem Cloud-Anbieter Daten in Deutschland verarbeitet, die Privat- oder Dienstgeheimnisse gemäß §§ 203 und 353b StGB enthalten, ist darüber hinaus durch geeignete technische und organisatorische Regelungen sicherzustellen, dass diese Daten nicht unbefugt Dritten offenbart werden. Unbefugt ist eine Offenbarung insbesondere, wenn durch sie gegen gesetzliche

Anforderungen des Datenschutzrechts sowie der §§ 203 und 353b StGB verstoßen wird. Die IT-Unterstützung für die Verarbeitung von Verschlusssachen (im Allgemeinen nur bis VS-NfD zulässig) unterliegt zudem den Regelungen der Verschlusssachenanweisung (VSA). Bei der Verarbeitung personenbezogener Daten sind §11 BDSG (Auftragsdatenverarbeitung) sowie die entsprechenden Nachweispflichten des Cloud-Anbieters zur Einhaltung des technischen und organisatorischen Datenschutzes zu beachten.

c. Soweit Cloud-Lösungen in Anspruch genommen werden, ist zur Vermeidung von „Lock-in-Effekten“ und wirtschaftlich ausnutzbaren Abhängigkeiten in möglichst hohem Maße Cloud-Lösungen auf Basis offener Standards der Vorzug zu geben, um die Möglichkeit eines Austauschs von Anbietern in wettbewerblicher Vergabe nicht zu erschweren oder zu verhindern. Insbesondere haben Planungen und die Ausrichtung eines Bedarfs auch zu berücksichtigen, dass besonders für den Fall von

   - Schlechtleistung, Unzuverlässigkeit oder Insolvenz eines Cloud-Anbieters,
   - Austausch von Subunternehmern, zu Gunsten solcher, die nicht die bei Vergabe geforderte Zuverlässigkeit und Vertrauenswürdigkeit haben,
   - Eingliederung des Cloud-Anbieters in ein anderes Unternehmen oder einen anderen Konzern oder sonstige Fälle des Wechsels des wirtschaftlichen Eigentums an ihm, wenn infolge dessen die geforderte Zuverlässigkeit und Vertrauenswürdigkeit nicht mehr besteht oder nicht mehr in der bei Vertragsschluss geforderten Weise belegt ist,
   - Kündigung des Vertragsverhältnisses aus wichtigem Grund oder regulärem Ende einer Vertragslaufzeit

   stets mehrere Anbieter am Markt zur Verfügung stehen, die die Aufgaben des ursprünglich beauftragten Anbieters übernehmen können.

d. Bei den Planungen zur Inanspruchnahme von Cloud-Diensten sind in Wirtschaftlichkeitsbetrachtungen auch angemessene Bewertungen mit Kostenschätzungen und Annahmen zu Risiken hinsichtlich der Wirtschaftlichkeit, Zuverlässigkeit und Sicherheit zu treffen. Hierzu zählen neben den Betriebskosten des Cloud-Dienstes insbesondere:

- weitere Kosten auf Seiten des Cloud-Anwenders, hier vor allem
  - Schulung der Mitarbeiter und Administratoren,
  - Vorhalten von IT-Know-how zum Cloud-Dienst,
  - Verwalten und Überwachung des Cloud-Dienstes,
- Migrationskosten zum Cloud-Dienst,
- Aufwände für Migrationsszenarien, die ein gegebenenfalls notwendiger Anbieterwechsel gemäß Ziffer 3 c. erzeugen könnte oder die Kosten einer gegebenenfalls notwendigen Wiederaufnahme des Eigenbetriebs durch die Wiederbereitstellung von Personal und Sachmitteln („Insourcing“).

e. Vertragsverhältnisse zu Cloud-Diensten ohne angemessene Preissicherung werden nicht eingegangen.

f. Zur Absicherung der Verfügbarkeit als Teil der IT-Sicherheit erfolgt eine Beauftragung von Cloud-Diensten nur unter vertraglicher Vereinbarung von deutschem Recht und Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren. Es ist zu gewährleisten, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtschutz keine Zeitverluste eintreten, zum Beispiel durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten, so dass die jeweilige Behörde handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann. In Bezug auf den Betrieb der Cloud-Dienste werden zur Absicherung der Verfügbarkeit außerdem keine kurzfristigen einseitigen Kündigungsrechte oder Zurückbehaltungsrechte an den Leistungen zu Lasten des Auftraggebers akzeptiert.

g. Soweit im Zusammenhang mit der Nutzung von Cloud-Diensten Software zu erwerben ist (zum Beispiel auch zum Fremdbetrieb), ist einem Erwerb dauerhafter Nutzungsrechte (Kauf) grundsätzlich der Vorzug zu geben gegenüber zeitlich befristeten Nutzungsrechten (Miete) oder solchen Nutzungsrechten, zu denen sich der Anbieter kurzfristig einseitig ausübbare Kündigungs- oder Widerrufsmöglichkeiten vorbehält.

h. Vor jeder Beschaffung sind eine Risikoanalyse zur Nutzung des beabsichtigen Cloud-Dienstes anzufertigen, in denen die unter Ziffer 3 c. und 3 d. genannten Gesichtspunkte berücksichtigt werden, daraus angemessene Maßnahmen abzuleiten und diese Maßnahmen als Anforderung in der Bedarfsbeschreibung als Grundlage der dem Vertrag zu Grunde liegenden Leistungsbeschreibung zu formulieren. Die Risikoanalyse muss die aktuellen Sicherheitsempfehlungen des BSI berücksichtigen. Die Risikoanalyse und die darin getroffenen Entscheidungen werden nachvollziehbar dokumentiert. Vor einer Beauftragung sollte jeder Bieter darlegen, welche Sicherheitsmaßnahmen getroffen werden, um die jeweiligen Sicherheitsanforderungen umzusetzen. Eine Beauftragung kann nur erfolgen, wenn die Umsetzung dieser Sicherheitsanforderungen sowie angemessene Kontrollmöglichkeiten vertraglich zugesichert werden.

i. Der Cloud-Anbieter hat eine ausreichende Informationssicherheit nachzuweisen. Dies kann durch ein Zertifikat „ISO 27001 auf der Basis von IT-Grundschutz“ oder durch zukünftige, gleichwertige BSI-Verfahren geschehen. Die Anerkennung anderer Zertifizierungen bzw. Sicherheitsnachweise ist im Einzelfall zu prüfen. In Betracht kommen jedoch nur Nachweise der Informationssicherheit, die von einer vertrauenswürdigen und unabhängigen Stelle ausgestellt werden und deren Prüfanforderungen sowie das Evaluationsschema zur Begutachtung offen liegen.

   Die Verpflichtung zur Erfüllung von Sicherheitsvorgaben muss vom Cloud-Anbieter auch an etwaige Subunternehmer weitergegeben und von diesen vertraglich übernommen und erfüllt werden. Der Cloud-Anbieter muss (gegebenenfalls unter einer Vertraulichkeitsvereinbarung) dem Auftraggeber Einblick in die zum Erlangen des Zertifikats erstellten Audit-Reports gewähren.

   Für einen hohen Schutzbedarf richten sich die Maßnahmen der Informationssicherheit nach einer eingehenden Risikoanalyse, wie sie gemäß ISO 27001 auf der Basis von IT-Grundschutz gefordert wird sowie nach den gemäß der Einschätzung des Bedarfsträgers zusätzlich erforderlichen Maßnahmen. Insbesondere kann die Beschaffungsstelle auf Grundlage der Risikoanalyse gemäß Ziffer 3h), auch auf Veranlassung des Bedarfsträgers, im Einzelfall den Nachweis strengerer Anforderungen verlangen.

j. Cloud-Anbieter müssen ein Notfall-Management nachweisen, vorzugsweise basierend auf dem BSI-Standard 100-4 oder der Norm ISO 22301.

Abweichungen von diesen Grundsätzen müssen sich auf besonders begründete Ausnahmen beschränken.

4. Die Grundsätze in Ziffer 3 dieses Beschlusses gelten für die IT-Unterstützung und Aufgabenerfüllung im Inland. Aufgrund der besonderen Anforderungen sind für die Informationstechnik des Auswärtigen Amts, des Bundesministeriums für Verteidigung sowie des Bundesnachrichtendienstes und anderer, im Auftrag der Bundesregierung im Ausland tätigen Behörden Abweichungen möglich.

5. Komponenten, die bereits in Maßnahmen des Programms „Gemeinsame IT des Bundes“ entwickelt werden und anforderungsgerecht sind, werden von den Einrichtungen des Bundes nicht unabhängig davon als Cloud-Lösungen entwickelt oder erstbeschafft. Für die Fortführung alternativer Cloud-Lösungen dürfen Mittel nur veranschlagt werden, soweit dies wirtschaftlich ist.

6. Weitergehende gesetzliche Regelungen, zum Beispiel zum Umgang mit personenbezogenen Daten, oder spezielle Regelungen zum Geheimschutz (zum Beispiel VSA) bleiben von diesem Beschluss unberührt.

7. Der Beschluss wird veröffentlicht.