IT-Planungsrat

Digitale Zukunft gestalten

Vorgehensweisen und Kriterien zur Inanspruchnahme und Beschaffung von Cloud-Diensten der IT-Wirtschaft

Beschluss des IT-Planungsrats

vom

13. Oktober 2016

Stand: 30. August 2016

I Vorbemerkungen

i. Im Zuge der technischen Verfügbarkeit von Cloud-Technologien, der zunehmenden Standardisierung von Prozessen in der öffentlichen Verwaltung und den gestiegenen Anforderungen an die Kosteneffizienz von IT-Dienstleistungen fordert die öffentliche Verwaltung die Bereitstellung von Cloud-Dienstleistungen.

ii. Die Nutzung von Cloud Diensten ist strategischer Natur. Der Einsatz von Cloud-Diensten durch die öffentliche Verwaltung erfordert die Prüfung der Schutzbedürftigkeit der Daten und Anwendungen sowie die sorgfältige Abwägung von Risiken unter anderem für die IT¬-Sicherheit, der wirtschaftlichen und praktischen Folgen sowie die entsprechenden Mehrwerte.

iii. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Cloud Computing wie folgt: „Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.“ Auf dieser Basis sind die Empfehlungen des BSI und des Arbeitskreises der Datenschützer in die nachfolgenden Kriterien eingeflossen.

iv. Vor diesem Hintergrund legt der IT-PLR folgende Kriterien zur Nutzung von Cloud-Diensten fest, die auch dazu dienen sollen, Angebote unterschiedlicher Cloud-Dienstleister miteinander hinsichtlich Wirtschaftlichkeit, Leistung und Schutzbedarf besser vergleichen zu können:

II Vorgehensweisen und Kriterien

1. Vor Inanspruchnahme und Beschaffung von Cloud-Diensten der IT-Wirtschaft ist zu prüfen, ob vergleichbare und anforderungsgerechte Leistungen bereits durch die Einrichtungen der öffentlichen Verwaltung selbst oder im Auftrag dieser durch Dritte bereitgestellt werden. Dies schließt bundes- und landeseigene sowie kommunale Inhouse-Gesellschaften mit ein. Die Nutzung dieser Cloud-Dienste ist der Beschaffung neuer Cloud-Dienste vorzuziehen soweit dies wirtschaftlich sinnvoll und rechtlich zulässig ist.

2. Die Einrichtungen der öffentlichen Verwaltung werden ihre Planungen, Bedarfsbeschreibungen und Vergaben sowie die Nutzung von Cloud-Diensten nach folgenden Grundsätzen ausrichten:
    a. Von den Einrichtungen der öffentlichen Verwaltung gehaltene schützenswerte Informationen (z. B. Informationen aus Verfahren mit hohem oder sehr hohem Schutzbedarf, Betriebs- und Geschäftsgeheimnisse sowie sensible Daten über IT-Infrastrukturen) dürfen ausschließlich in Deutschland gespeichert und verarbeitet werden. Cloud-Anbieter sollen ein dafür geeignetes Betriebsmodell vorweisen. Sie 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 gespeichert und/oder verarbeitet, die Privat- oder Dienstgeheimnisse gemäß §§ 203 und 353b StGB enthalten, ist darüber hinaus durch geeignete technische und organisatorische Regelungen in einem Sicherheitskonzept 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 des Bundes oder der Länder). Bei der Verarbeitung personenbezogener Daten sind die gesetzlichen Vorgaben zum Datenschutz sowie die entsprechenden Nachweispflichten des Cloud-Anbieters zur Einhaltung des technischen und organisatorischen Datenschutzes zu beachten.
    c. Zur Vermeidung von „Lock-in-Effekten“, wirtschaftlich ausnutzbaren Abhängigkeiten und um den Austausch von Anbietern in wettbewerblicher Vergabe zu ermöglichen, sind in möglichst hohem Maße Cloud-Lösungen auf Basis offener Standards der Vorzug zu geben. Die Planungen zur Nutzung von Cloud-Diensten haben zu berücksichtigen, dass stets mehrere Anbieter am Markt zur Verfügung stehen, die die Aufgaben des ursprünglich beauftragten Anbieters übernehmen können. Das gilt besonders für folgende Fälle:
        - 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.

d. Bei den Planungen zur Inanspruchnahme von Cloud-Diensten der IT-Wirtschaft sind in Wirtschaftlichkeitsbetrachtungen auch angemessene Bewertungen mit Kostenschätzungen und Annahmen zu Risiken hinsichtlich der Wirtschaftlichkeit, Zuverlässigkeit und Sicherheit zu treffen. Hierzu zählen neben den Kosten für die Nutzung 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 2 c. erzeugen könnte oder die Kosten einer gegebenenfalls notwendigen Wiederaufnahme des Eigenbetriebs durch die Wiederbereitstellung von Personal und Sachmitteln („Insourcing“).

e. Zur Absicherung der Verfügbarkeit als Teil der IT-Sicherheit erfolgt eine Beauftragung von Cloud-Diensten nur unter vertraglicher Vereinbarung von deutschem Recht und Gerichtsstand sowie ohne obligatorisch vorab zu betreibende Schlichtungsverfahren. Es ist zu gewährleisten, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz 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 die Nutzung der Cloud-Dienste werden zur Absicherung der Verfügbarkeit außerdem keine kurzfristigen einseitigen Kündigungsrechte oder Zurückbehaltungsrechte an den Leistungen zu Lasten des Auftraggebers akzeptiert.

f. Soweit im Zusammenhang mit der Nutzung von Cloud-Diensten Software zu erwerben ist (zum Beispiel auch zum Fremdbetrieb) sind kurzfristig einseitig ausübbare Kündigungs- oder Widerrufsmöglichkeiten seitens des Anbieters auszuschließen

g. Vor jeder Beschaffung ist der Schutzbedarf der gespeicherten bzw. verarbeiteten Daten festzustellen. Auf Basis dieser Schutzbedarfsfeststellung ist eine

Risikoanalyse zur Nutzung des beabsichtigen Cloud-Dienstes anzufertigen, in der die unter Ziffer 2 c. und 2 d. genannten Gesichtspunkte berücksichtigt werden. Eine Beauftragung kann nur erfolgen, wenn die Umsetzung der Sicherheitsanforderungen sowie angemessene Kontrollmöglichkeiten dargelegt und vertraglich zugesichert werden (vgl. auch Ziffer 5).

h. Der Cloud-Anbieter hat für die Bereitstellung der relevanten Dienste (inklusive der dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten) eine ausreichende Informationssicherheit durch ein gültiges Zertifikat „ISO 27001 auf der Basis von IT-Grundschutz“ oder durch ein gleichwertiges BSI-Verfahren bzw. vom BSI anerkanntes Verfahren nachzuweisen. Der Cloud-Anbieter muss einen Ansprechpartner für Informationssicherheit, Datenschutz und Geheimschutz benennen, der vom Auftraggeber direkt erreicht werden kann.

   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. Der Cloud-Anbieter hat die an der Cloud-Dienstleistung beteiligten Subunternehmer dem Auftraggeber zu offenbaren.

   Für einen hohen Schutzbedarf richten sich die Maßnahmen der Informationssicherheit nach einer eingehenden Risikoanalyse, wie sie gemäß BSI-Standard 100-2 i.V.m. 100-3 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.

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

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

3. Die Grundsätze in Ziffer 2 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 oder der Landesregierungen im Ausland tätigen Behörden Abweichungen möglich.

4. Weitergehende gesetzliche Regelungen, zum Beispiel zum Umgang mit personenbezogenen Daten, oder spezielle Regelungen zum Geheimschutz (zum Beispiel VSA) bleiben von diesem Beschluss unberührt. Zudem bleibt es den Mitgliedern des IT-Planungsrats unbenommen, weitergehende Anforderungen an die Nutzung von Cloud-Diensten festzulegen.
5. Bei der Inanspruchnahme von Cloud-Dienstleistungen und Cloud Service Providern sind die „Handlungsempfehlungen für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud“ und/oder der „Anforderungskatalog Cloud Computing - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“ des BSI zu verwenden.