



Bundesminister für EU,
Kunst, Kultur und Medien

bundeskanzleramt.gv.at

Mag. Gernot Blümel, MBA
Bundesminister für EU, Kunst, Kultur und Medien

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: BKA-353.120/0030-IV/10/2019

Wien, am 30. April 2019

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Gamon, MSc (WU), Kolleginnen und Kollegen haben am 1. März 2019 unter der Nr. **3009/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Einsatz von Cloud Computing im öffentlichen Sektor“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 und 3:

- *In welcher Form werden Cloud Computing und Cloud Services in Ihrem Ministerium genutzt?*
 - a) *Welche Vertragspartner sind dabei involviert?*
 - b) *Welche Prozesse und Infrastrukturen sind davon betroffen?*
 - c) *Welche Formen von Cloud Computing verwendet Ihr Ministerium?*
- *Welche Cloud Services bezieht Ihr Ministerium?*

Im Bereich der Fachservices werden interne Services der Bundesrechenzentrum GmbH als Dienstleister herangezogen (Private Cloud).

Das Bundeskanzleramt setzt im Bereich des Eventmanagements seit 2015 das Produkt „iventcloud“ der Firma Liland ein (Public Cloud).

Zu den Fragen 2 und 9:

- *Welche Sicherheitsstandards herrschen in Ihrem Ministerium bezüglich des Einsatzes von Cloud Computing?*
 - a) *Ist die Nutzung in der Sicherheitsbelehrung Ihres Hauses für die Mitarbeiter_innen geregelt?*
 - b) *Wenn ja, wie?*
 - c) *Wenn nein, warum nicht?*
- *Welche Sicherheitsrisiken sieht Ihr Ministerium in Bezug auf die Verwendung von Cloud Computing und Cloud Services in der öffentlichen Verwaltung von Österreich?*
 - a) *Mit welchen Maßnahmen begegnen Sie diesen?*

Im allgemeinem Geschäftsbetrieb erfolgt bei der Nutzung von Cloud-Lösungen in der Regel eine explizite Freischaltung, bei manchen Services ist dies jedoch nicht notwendig (z. B. Office 365, OneDrive). Es gibt keine allgemein gültige Regelung für die Nutzung von Cloud-Lösungen, da jeder Einsatzfall individuell analysiert, bewertet und entschieden wird, um sichere Rahmenbedingungen zu gewährleisten.

Im Bereich der Fachservices ist die Bundesrechenzentrum GmbH als Dienstleister nach den Normen ISO 27001, ISO 27002, ISO 27017 und ISO 20000 zertifiziert.

Die Sicherheitsvorgaben sind für die Mitarbeiterinnen und Mitarbeiter verpflichtend. Es handelt sich vor allem um Informationssicherheitsanalyseberichte, welche die Grundlage für das Sicherheitskonzept sowohl im Bundeskanzleramt als auch in der Bundesrechenzentrum GmbH sind.

Zu Frage 4:

- *Werden seitens Ihres Ressorts Daten auf Cloud Computing Infrastrukturen privater Anbieter ausgelagert?*
 - a) *Wenn ja, welche und wo sind diese gespeichert?*
 - b) *Wer hat Zugriff auf diese Daten?*
 - c) *Welche Sicherheitsstandards gelten hierbei?*
 - d) *Welche Vertragspartner sind hierbei involviert?*

Auf Diensthändies werden die speziell für den dienstlichen Gebrauch vorgesehenen Apps und Datenbanken laufend sicherheitstechnisch auf dem letzten Stand gehalten. In Bezug auf Eventmanagement und Fachservices wird auf die Beantwortung der Fragen 1 und 3 verwiesen.

Zu Frage 5:

- *Welche datenschutzrechtlichen Probleme sehen Sie konkret in Bezug auf die Nutzung von Cloud Computing im öffentlichen Sektor?*

Ich darf auf die Beantwortung der gleichlautenden parlamentarischen Anfrage Nr. 3011/J vom 1. März 2019 durch den Herrn Bundesminister für Verfassung, Reformen, Deregulierung und Justiz verwiesen.

Zu den Fragen 6 und 7:

- *Welche Maßnahmen plant Ihr Ministerium im Bereich Cloud Computing? Ist es seitens Ihres Ministeriums der verstärkte Einsatz von Cloud Computing geplant?*
- *Welche Strategie verfolgt ihr Ministerium zu Cloud Computing?*

Derzeit ist kein verstärkter Einsatz von Cloud-Computing geplant. Die Technologie von Cloud-Computing und die damit verbundenen Chancen und Risiken werden laufend und eingehend geprüft.

Nach heutigem Stand sind allfällige Risiken dabei durch folgende Maßnahmen zu minimieren:

- Informationssicherheits-Risikoanalysen, unter anderem nach anerkannten und standardisierten bzw. best practise-Richtlinien (z. B. Star Audit Trusted Services),
- Feststellen des Schutzbedarfes,
- Risikobewertung gemäß DSGVO, wenn personsbezogene Daten verarbeitet werden,
- Hinzuziehen von Sicherheitsexpertinnen und -experten und CISO (Chief Information Security Officer),
- Hinzuziehen von Cloud-Expertinnen und -Experten.

Zu Frage 8:

- *Wie sieht Ihre Zusammenarbeit mit anderen Ministerien in Bezug auf Cloud Computing aus?*

Die Ministerien vernetzen sich insbesondere über die Chief Digital Officer-Task Force. Die Chief Digital Officer-Task Force soll eine abgestimmte und proaktive Herangehensweise an das Thema Digitalisierung verfolgen, da die erfolgreiche Positionierung Österreichs als Vorreiter der Digitalisierung eine dynamische und abgestimmte Vorgehensweise unter Berücksichtigung der Sicherheitsbedürfnisse innerhalb der Bundesverwaltung erfordert. Dem Regierungsprogramm folgend wurde in jedem Ressort die Rolle eines Ressort-Chief Digital Officers besetzt. Im Bundesministerium für Digitalisierung und Wirtschaftsstandort ist zur

Leitung der „CDO-Task Force“ die Rolle eines Bundes-Chief Digital Officer besetzt. Das IT-Trendthema Cloud-Computing wird auch in diesem Gremium behandelt und entsprechende Strategien entwickelt.

Ebenso ist das Gremium IKT-Bund ein interministerielles Forum, das die Frau Bundesministerin für Digitalisierung und Wirtschaftsstandort in allgemeinen Angelegenheiten der Informations- und Kommunikationstechnologie und zur Besorgung ressortübergreifender IKT-Koordinationsaufgaben wie der Festlegung von IKT-Standards berät. Daher werden in diesem Rahmen die Grundlagen erarbeitet, um Cloud-Computing zu nutzen bzw. in eigenen Rechenzentren zu implementieren.

Mag. Gernot Blümel, MBA

