FAQ zum Bericht rechtlicher Rahmen für die Nutzung von Public Cloud-Diensten in der Bundesverwaltung

Inhaltsverzeichnis

1 Einleitung

Der Bericht «rechtlicher Rahmen für die Nutzung von Public-Cloud Diensten in der Bundesverwaltung» der Bundeskanzlei gibt einen Überblick über die wichtigsten rechtlichen Fragestellungen, die sich in der Bundesverwaltung im Zusammenhang mit der Auslagerung von Daten in eine (ausländische) Cloud ergeben. Ergänzend wurden die vorliegenden FAQ für die Bundesverwaltung erarbeitet. Die FAQ nehmen wichtige praxisrelevante Fragestellungen zum Thema Auslagerung von Daten in eine Cloud auf und beantworten diese. Dabei sollen die FAQ regelmässig überprüft und angepasst werden, so dass sie dem aktuellen Stand der Erkenntnisse entsprechen. Die Fragen sind thematisch geordnet. Die Verweise referenzieren den eingangs erwähnten Bericht.[1]

2 Allgemeine Fragen

2.1 Änderung Auslagerung Cloud gegenüber On-Premises

Frage: Was ändert sich bei der Auslagerung von Daten in eine Cloud im Gegensatz zu einer Haltung On-Premises? Oder anders: Was ist der Unterschied zwischen der Bearbeitung von Daten in der Cloud und der Bearbeitung On-Premises?

Antwort: Abgesehen von der Tatsache, dass die zuständige Verwaltungseinheit bei der Auslagerung von Daten und Anwendungen in eine Cloud nicht mehr selbst die physische Kontrolle über die IT-Mittel hat, tragen insbesondere drei Faktoren zur rechtlichen, aber auch zur technischen Komplexität von Cloud-Sourcing-Lösungen bei, die sie von einer Haltung On-Premises unterscheiden und welche bei der Risikobeurteilung zu berücksichtigen sind:

- Auslandbezug: Aus heutiger Sicht werden insbesondere Public-Cloud-Dienstleistungen von grossen Anbietern (sog. «Hyperscalern») potenziell vollumfänglich oder teilweise im Ausland erbracht (Server-Standorte, Supportzugriffe). Damit muss eine tendenziell abnehmende Kontrolle über das rechtliche Umfeld (z.B. Frage der Angemessenheit der Datenschutzgesetzgebung im Zielland, Risiko von Behördenzugriffen) mit vertraglichen, technischen und organisatorischen Massnahmen kompensiert werden.
- Beizug von Unterauftragnehmern: Für die Auftragserfüllung ziehen Cloud-Service-Anbieter (auch bei Private-Cloud-Lösungen) in der Regel weitere Dritte bei, die gewisse Aufgaben erfüllen. Diese Unterauftragnehmer erfüllen ihre Aufgaben zudem in manchen Fällen von (weiteren) Drittländern aus.
- Abhängigkeiten von Dritten: Cloud-Sourcing-Lösungen können zu erheblichen Abhängigkeiten von einzelnen Dienstleistern führen, insbesondere was die Verfügbarkeit der Leistungen betrifft.

Welche Restrisiken im Vergleich zu einer Bearbeitung in bundeseigenen Rechenzentren (On-Premises) – innerhalb der Grenzen des anwendbaren Rechts – akzeptiert werden können, ist ein von der Verwaltungseinheit zu fällender Führungsentscheid, der von den Projektverantwortlichen einzuholen ist. Der Entscheid ist ausgehend von der Art der auszulagernden Daten gestützt auf eine Analyse des Rechtsrahmens und einer Risikoanalyse zu treffen. Die Risikoanalyse muss die im konkreten Anwendungsfall bestehenden Risikofaktoren und die Massnahmen zu deren Mitigation berücksichtigen. In Bezug auf den Informationsschutz ist der Cloud-Einsatz in der Bundesverwaltung für GEHEIME Informationen jedoch per se untersagt.

Verweis: Teil 1 (Ziff. 3.1 – 3.2 und Anhänge C bis E), Teil 2 (Ziff. 1.4 – 1.7 und 4).

2.2 Amtsgeheimnis

Frage: Was ändert sich mit dem revidierten Art. 320 StGB (Fassung vom 1.1.2023)?

Antwort: Mit dem revidierten Artikel 320 Ziffer 1 StGB unterstehen Cloud-Service-Anbieter dem Amtsgeheimnis, wenn Sie Daten der Verwaltung bearbeiten. Neben der Verletzung möglicher technischer Massnahmen oder vertraglicher Verpflichtungen wird der Cloud-Service-Anbieter

[1] Cloud (admin.ch).

also ebenfalls strafbar, wenn er durch das Amtsgeheimnis geschützte Informationen offenbart. Die Auslagerung der Datenhaltung in die Cloud für sich alleine stellt keine Verletzung des Amtsgeheimnisses dar.

Verweis: Teil 2 (Ziff. 2).

2.3 Vertragliche Massnahmen

Frage: Welche vertraglichen Massnahmen können dabei helfen, die allgemeinen Risiken einer Auslagerung von Daten zu minimieren? Warum sind solche vertraglichen Massnahmen erforderlich?

Antwort: Neben den technischen und organisatorischen Massnahmen ermöglichen auch vertragliche Massnahmen eine Risikomitigation. Vertragliche Massnahmen können in folgenden Bereichen sinnvoll sein:

- **Compliance-Risiken**: insb. Regelung der Pflichten des Cloud-Service-Anbieters und dessen Unterauftragnehmer, Regelung über den Beizug von Unterauftragnehmern, Kontrollbefugnisse des Auftraggebers, Informationspflichten des Anbieters bei sicherheitsrelevanten Vorkommnissen, Gewährleistung eines angemessenen Datenschutzniveaus und, dass Daten nur in einem bestimmten ausländischen Staat bearbeitet werden dürfen, Verpflichtung des Anbieters, sich an das einschlägige schweizerische Recht zu halten und die Schweiz als Gerichtsstand zu akzeptieren, Regelung des Verfahrens bei Zugangsantrag durch ausländische Behörden, Regelung der Verteidigung bei Angriffen, Ausschluss von einseitigen Vertragsänderungen, Kündigungsrechte bei Vertragsänderungen, Angemessene Haftung für Vertragsverletzungen.
- **Business-Continuity-Risiken**: insb. Regelung bei Serviceänderungen durch den Anbieter, Exit-Option bei Änderung der Konditionen vorsehen, Datenexport und Migration regeln, Regelung des Wiederherstellungsverfahrens, Konventionalstrafen für besonders kritische Arten von unvorhergesehenen Serviceunterbrechungen, klare Regelung der Befugnisse von Administratoren, Sicherheitsverfahren und -kontrollen für die Mitarbeitenden des Anbieters regeln.
- **Politische Risiken**: insb. Vereinbarung von Bearbeitungsstandorten, die rechtlich und politisch stabil sind, Vereinbarung von Exit-Klauseln.
- **Technische Risiken**: insb. Prüfberichte des Anbieters, welche die Datensicherheit dokumentieren, Verpflichtung des Anbieters zur Meldung von schwerwiegenden Cyberangriffen, Verpflichtung des Anbieters zur Einhaltung von ISO-Standards, Zugang der verantwortlichen Bundesstelle zu Audit-Ergebnissen, Vertragliche Zusicherungen betr. Detektion von Schwachstellen und entsprechende frühzeitige Kommunikation durch den Anbieter, Vorgaben betr. Personensicherheit beim Anbieter.

Vertragliche Massnahmen sind zusätzlich wichtig, um eine mit dem Schweizer Recht vereinbare Datenbearbeitung in der Cloud zu gewährleisten. Sie sind insbesondere wesentlich und datenschutzrechtlich absolut notwendig in Ausnahmefällen einer Datenbearbeitung in einem Staat, der nicht über eine angemessene Datenschutzgesetzgebung verfügt.

Verweis: Teil 1 (Ziff. 3), Teil 2 (Ziff. 1.3 – 1.7), Anhang C.

2.4 Datenschutz

Frage: Gibt es generelle Empfehlungen und Vorgaben bezüglich des Datenschutzes aus rechtlicher Sicht?

Antwort: Soweit für die Bearbeitung die nötigen Rechtsgrundlagen bestehen und die Sorgfaltspflicht bei der Wahl des Cloud-Service-Anbieters beachtet wird, sind keine besonderen rechtlichen Vorkehrungen erforderlich. Die Bearbeitung von Personendaten mittels Public-Cloud-Diensten stellt indessen nach Auffassung des EDÖB eine Bearbeitung mit besonderem Risiko dar, die eine Datenschutzfolgenabschätzung nötig macht. Weiter leiten sich aus dem Datenschutzgesetz insbesondere Anforderungen zur Gewährleistung der Datensicherheit ab.

Neben dem rechtlichen Rahmen spielen für eine umfassende Einschätzung der Zulässigkeit der Datenbearbeitung durch Public Cloud-Anbieter auch die Risikobeurteilung aus geschäftlicher

Sicht sowie interne Richtlinien und Vorgaben eine Rolle. Die Vorgabe Si001 der Bundesverwaltung zum IKT-Grundschutz ist zentral: Sie legt nämlich die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Für jedes Informatikschutzobjekt gilt als Minimum der IT-Grundschutz.

In diesem Prozess stellt die Schutzbedarfsanalyse (Schuban; Vorgabe P041) den Ausgangspunkt dar. Sie dient insb. dazu, zu analysieren, ob die auszulagernden Daten grundsätzlich zugänglich sind oder ob sie aufgrund spezifischer Rechtsgrundlagen besonderen Anforderungen an die Vertraulichkeit unterliegen. Weiter ist zu beurteilen, ob dabei Personendaten bearbeitet werden und mithin eine Datenschutz-Folgenabschätzung vorzunehmen ist. Diese analysiert insbesondere die Risiken, definiert die Massnahmen und beschreibt deren Umsetzung. Dabei ist auch zu prüfen, ob die Public Cloud-Anbieter gemäss den Rechtsordnungen ihrer Herkunftsländern Daten an die jeweiligen Regierungen herausgeben müssen und welche Datenhaltungs-Regionen sie anbieten.

Darauf gestützt ist festzulegen, welche angemessenen Schutzmassnahmen, insb. technische und organisatorische Massnahmen des Daten- und Informationsschutzes (vgl. z.B. Art. 11 VDTI in diesem Bezug), zu treffen sind.

Ergibt die Schuban einen erhöhten Schutzbedarf, so ist zusätzlich zur Dokumentation der Umsetzung des IT-Grundschutzes ein ISDS-Konzept mit Risikoanalyse zu erstellen (Vorgabe P042). Es legt die nötigen Angaben zur Erhaltung und Verbesserung der Informationssicherheit und des Datenschutzes fest und fasst beide Aspekte im Projekt zusammen.

Verweis: Art. 8 DSG; Art. 14b ff CyRV, Teil 2 (Ziff. 2.2.2), Vorgabe Si001 (IT-Grundschutz in der Bundesverwaltung), Vorgabe P041 (Schutzbedarfsanalyse), Vorgabe P042 (Informationssicherheits- und Datenschutzkonzept), SB020 - Cloud-Strategie der Bundesverwaltung .

2.5 Arten von auszulagernden Daten

Frage: Welche Arten von Daten fallen unter das DSG, das ISG oder unter das Amtsgeheimnis?

Antwort: Der Fokus dieser Rechtsgrundlagen ist unterschiedlich:

Das DSG zielt darauf ab, die informationelle Selbstbestimmung der Einzelnen zu gewährleisten.

Das ISG hingegen befasst sich mit dem Schutz von Informationen unabhängig davon, ob es sich um Personendaten handelt. Die Klassifizierung in Bezug auf die Interessen der Eidgenossenschaft ist hier massgebend.

Das Amtsgeheimnis greift im Kontext der Offenbarung einer bestimmten Kategorie von Information, insbesondere um das reibungslose Funktionieren der Verwaltung zu gewährleisten.

Die jeweiligen Schutzobjekte können wie folgt grob umrissen werden:

DSG	ISG	Amtsgeheimnis (320 StGB)
Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.	Klassifizierte Informationen, deren Kenntnisnahme durch Unberechtigte den Landesinteressen: • GEHEIM: einen schweren Schaden zufügen kann. • VERTRAULICH: Schaden zufügen kann. • INTERN (und als "RESTRICTED" oder gleichwertig klassifizierte Informationen aus dem Ausland): einen Nachteil zufügen kann.	Informationen, die in der Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist oder die jemand aufgrund einer amtlichen oder dienstlichen Stellung oder als Hilfsperson eines Beamten oder einer Behörde wahrgenommen hat. Hier sind insb. die Beschränkungen der Tragweite des Amtsgeheimnisses zu beachten, die sich aus dem Öffentlichkeitsprinzip ergeben, vgl. die Ausführungen im Bericht.

Verweis: Art. 5 Bst. a und 2 Abs. 2-4 DSG, Teil 2 (Ziff. 1); Art. 5-7 ISchV, Teil 2 (Ziff. 4); Art. 320 StGB, 3-4 und 7-8 BGÖ, Teil 2 (Ziff. 2).

2.6 Auftragsdatenbearbeitung

Frage: Was ist eine Hilfsperson? Unter welchen Voraussetzungen kann ein Auftragsbearbeiter seinerseits eine Hilfsperson beiziehen?

Antwort: Der Begriff der Hilfsperson ist im Kontext des Amtsgeheimnisses relevant. Analog zu den Berufsgeheimnissen nach Art. 321 StGB, ist eine Hilfsperson «wer bei der Berufstätigkeit eines der genannten (Haupt-)Geheimnisträgers in der Weise mitwirkt, dass er grundsätzlich von den dabei wahrgenommenen Tatsachen ebenfalls Kenntnis erhält». Hilfspersonen wie Cloud-Anbieter und Auftragsbearbeiter werden somit mit dem neuen Art. 320 Ziff. 1 StGB in den Kreis der Amtsgeheimnisträger eingeschlossen.

Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. Die Datensicherheit muss insb. gewährleistet werden. Soweit Auftragnehmende weitere Unterauftragnehmer beiziehen, ist durch entsprechende Vertragsgestaltung und allenfalls auch technische Massnahmen durch die Auftraggebenden sicherzustellen, dass diese an die gleichen Regelungen gebunden sind, wie der Cloud-Anbieter selbst. Der Auftragsbearbeiter muss insbesondere die Genehmigung des Verantwortlichen vorgängig einholen. Die gleichen Elemente wie für eine einfache Auftragsbearbeitung können geltend gemacht werden.

Verweis: Art. 9 DSG, Art. 11 VDTI, Teil 2 (Ziff. 1.5 und 2), Art. 320 StGB, PK StGB-TRECHSEL/VEST (Art. 321 N 13).

2.7 Verantwortlichkeit für den IT-Grundschutz

Frage: Wer stellt die Einhaltung des IT-Grundschutzes im Betrieb sicher?

Antwort: Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verantwortlichen Verwaltungseinheiten zu dokumentieren und zu überprüfen. Dabei muss die Dokumentation mindestens von

a) der oder dem Schutzobjektverantwortlichen,

b) der oder dem Informatiksicherheitsbeauftragten der verantwortlichen Verwaltungseinheit,

c) der Auftraggeberin oder dem Auftraggeber (bei einem Projekt) und

d) der oder dem Geschäftsprozessverantwortlichen

überprüft und unterzeichnet sein. Die Unterzeichnenden bestätigen auch, dass gemäss ihrer Einschätzung alle am Betrieb des Schutzobjektes beteiligten Leistungserbringer die sie betreffenden Anforderungen erfüllen**.**

Verweis: Vorgabe Si001 (IT-Grundschutz in der Bundesverwaltung).

2.8 Konfiguration

Frage: Gibt es allgemeine Sicherheitsempfehlungen für Einstellungen, Berechtigungen, etc.?

Antwort: Das Schutzobjekt muss vor der ersten Inbetriebnahme so konfiguriert und eingestellt sein, dass es vor unberechtigtem Zugriff geschützt ist, es soweit technisch möglich gehärtet ist und in einer zur Aufgabenerfüllung erforderlichen und vom Benutzer nicht veränderbaren Minimalkonfiguration betrieben wird (d.h. nicht genutzte Schnittstellen, Module und Funktionen müssen deaktiviert sein), und wichtige sicherheitsrelevante Aktivitäten und Ereignisse (mit Zeitangaben) aufgezeichnet und zeitnah ausgewertet werden. Sicherheitskonfigurationen und -einstellungen dürfen ausserdem nur autorisiert, aktiviert, geändert, deaktiviert und deinstalliert werden. Der Kreis der zur Bearbeitung Berechtigten wird insbesondere durch Identitätsmanagement-Tools eingeschränkt und kontrolliert.

Verweis: Vorgabe Si001 (IT-Grundschutz in der Bundesverwaltung).

2.9 Vorgehen bei Sicherheitsvorfällen

Frage: Gibt es ein geregeltes Vorgehen bei einem möglich Sicherheitsvorfalls (z.B. Datenverlust, Ransomware-Angriff)?

Antwort: Wenn ein Sicherheitsvorfall (z.B. Data-Leak, Ransomware Angriff etc.) stattfindet, wurde aus datenschutzrechtlicher Sicht die Datensicherheit verletzt. Wenn Personendaten betroffen sind, sieht Art. 24 DSG zudem eine Meldepflicht vor, welche ausdrücklich auch Auftragsbearbeiter (Cloud-Service-Anbieter inbegriffen) trifft.

Gemäss dieser Bestimmung muss der Verantwortliche dem EDÖB (bzw. der Auftragsbearbeiter dem Verantwortlichen) so rasch als möglich eine Verletzung der Datensicherheit melden, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Ein Datenverlust kann oft eine solche Intensität der Verletzung erreichen. In dieser Meldung muss er insb. die ergriffenen oder vorgesehenen Massnahmen nennen. Er muss auch die betroffene Person informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

Zudem sollte, auch wenn keine Personendaten betroffen, eine Meldung ans NCSC erfolgen.

Verweis: Art. 24 DSG, Teil 2 (Ziff. 1.3); Cyberattacke – was tun? Informationen und Checklisten (admin.ch).

2.10 Zugriff des Auftragsbearbeiter auf die Daten

Frage: Kann der Auftragsbearbeiter auf die (Klartext-)Daten zugreifen? Wenn ja, in welchen Fällen?

Antwort: Daten, die nicht allgemein zugänglich sind, dürfen externen Leistungserbringern nur zugänglich gemacht werden, wenn zusätzlich zu Art. 9 DSG, die Voraussetzungen von Art. 11 VDTI erfüllt sind:

- Das Zugänglichmachen der Daten ist zur Erbringung der Leistung *erforderlich*. D.h., die Daten müssen für den Leistungserbringer zwingend einsehbar sein, damit er seinen Auftrag erfüllen kann bzw. es würde einen nicht verhältnismässigen Aufwand bedeuten, wenn er dies ohne Zugang zu den Daten (bzw. nur in entpersonalisierter oder verschlüsselter Form) tun müsste.
- Die für die Daten verantwortliche Behörde hat schriftlich zugestimmt.
- Es wurden angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen, um eine weitere Verbreitung der Daten zu verhindern.

Somit wird der Auftragsbearbeiter, wenn überhaupt, auf Daten im Klartext nur in ganz bestimmten und im Voraus vereinbarten Einzelfällen zugreifen und diese selbst bearbeiten dürfen (z.B. zu Supportzwecken). Ausnahme davon bildet der Zugriff insbesondere auf Randdaten; solche werden vom Cloud-Anbieter in der Regel zumindest für die Abrechnung seiner Dienstleistung regelmässig erhoben und bearbeitet.

Verweis: Art. 9 DSG, 11 VDTI, Teil 2 (Ziff. 1.2.2, 1.5, 2.2.2.2), Anhänge C-E.

3 Datenbekanntgabe ins Ausland

3.1 Möglichkeit zur Datenbekanntgabe ins Ausland

Frage: Wann ist eine grenzüberschreitende Datenbekanntgabe möglich?

Antwort: Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 DSG). Diese Staaten werden in einer Liste im Anhang der Datenschutzverordnung (DSV) aufgeführt. Aktuell erfüllen beispielsweise die Mitgliedstaaten der EU, UK, Argentinien und Neuseeland diese Anforderungen, im Gegensatz zu beispielsweise den USA und China.

Weiter dürfen Daten in gewissen Ausnahmefällen in Staaten übermittelt werden, die nicht über ein angemessenes Datenschutzniveau verfügen, insbesondere wenn die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat (Art. 17 Abs. 1 Bst. a DSG).

Ist ausnahmsweise eine Datenbearbeitung in einem Staat erforderlich, der nicht über eine angemessene Datenschutzgesetzgebung verfügt, so ist eine entsprechende vertragliche Absicherung vorzusehen, etwa unter Verwendung der vom EDÖB genehmigten bzw. bereitgestellten Standardvertragsklauseln oder spezifischer Garantien, die die zuständige Verwaltungseinheit erarbeitet und dem EDÖB vorgängig mitgeteilt hat. Zudem sind auch angemessene technische und organisatorische Massnahmen zu treffen.

Verweis: Art. 16 ff. DSG, Anhang 1 DSV, Teil 2 (Ziff. 1.6).

3.2 Fragen zum US-Cloud Act und FISA

Frage: Was ist FISA und CLOUD-Act?

Antwort: FISA (Foreign Intelligence Surveillance Act) und CLOUD-Act (Clarifying Lawful Overseas Use of Data Act) sind amerikanische Gesetze, die in gewissen Fällen Datenzugriffe für amerikanische Behörden ermöglichen, auch dann, wenn diese Daten ausserhalb der USA bearbeitet bzw. gehostet werden, namentlich von Firmen mit Sitz in den USA oder mit anderen rechtlichen Beziehungen zur USA («incorporated in the United States»).

- FISA: Der FISA zielt auf präventive Zwecke und Auslandüberwachung ab. Er erlaubt gewissen amerikanische Behörden die Beschaffung von ausländischen Informationen über bestimmte Zielpersonen zu verlangen. Für Datenzugriffe gemäss FISA bestehen nur beschränkte verfahrensrechtlichen Sicherungen. Zudem ist die Transparenz nicht gewährleistet, soweit die Cloud-Service-Anbieter keine Auskunft darüber geben dürfen, dass eine Behörde Datenzugang verlangt («gag order»), auch wenn sie rechtliche Möglichkeiten haben, gegen Überwachungsanordnungen vorzugehen.
- US-Cloud Act: Im Rahmen eines Justizverfahrens schafft dieses Gesetz die Möglichkeit für Strafverfolgungsbehörden, auf Daten beim Cloud-Anbieter zuzugreifen, ohne dass ein Rechtshilfeverfahren durchgeführt werden muss. Solche Massnahmen sind an bestimmte Voraussetzungen gebunden. Der US-Cloud Act kommt insb. nur in Frage, wenn schwere Straftaten betroffen sind und der betroffene Cloud-Service-Anbieter eine faktische oder rechtliche Kontrolle über die Daten hat. Verfahrensrechtlich können die Cloud-Service-Anbieter die Massnahmen vom US-Cloud Act vor einem US-Gericht anfechten, aber kein Rechtsschutz in der Schweiz möglich ist.

Verweis: Teil 2 (Ziff. 1.7.2).

Frage: Unterstehen auch Tochtergesellschaften von amerikanischen Firmen dem US-Cloud Act und FISA?

Antwort: Grundsätzlich fallen auch die europäischen Tochterfirmen von amerikanischen Firmen unter diese Bestimmungen. Allerdings kann eine direkt an sie adressierte Herausgabeanordnung der US-Strafverfolgungsbehörden ausserhalb des US-Territoriums nicht mit strafprozessualem Zwang durchgesetzt werden. Daher werden die US-Strafverfolgungsbehörden ihre Herausgabeanordnungen aller Voraussicht nach an die in den USA angesiedelten Mutterkonzerne richten. Eine (nach US-amerikanischem) Recht rechtskonforme Herausgabe ist dabei nur unter bestimmten Voraussetzungen möglich, insb. dann, wenn die Muttergesellschaft bereits Zugriff auf die Daten hat.

Verweis: Teil 2 (Ziff. 1.7.2).

Frage: Wie kann man mit vertraglichen Massnahmen das Risiko, welches durch den US-Cloud Act oder FISA verursacht wird, minimieren?

Antwort: Für den US-Cloud Act kann grundsätzlich von Folgendem ausgegangen werden: Daten von Schweizer Behörden geniessen angesichts der im Cloud Act enthaltenen Verfahrensmechanismen einen gewissen Schutz vor Datenzugriffen durch US-Behörden. Auch das Risiko von – aus Schweizer Sicht nicht rechtskonformen – Zugriffen gestützt auf FISA kann auf ein aus rechtlicher Sicht akzeptables Niveau reduziert werden, wenn die im US-Recht bereits vorgesehen Mechanismen mit vertraglichen Vereinbarungen (z. B. der Verpflichtung, eine Herausgabe anzufechten) ergänzt werden. Soweit gesetzlich zulässig sind insbesondere Vereinbarungen darüber zu treffen, wie der Cloud-Anbieter auf Anfragen von Behörden oder Verfahren im Zusammenhang mit der Übergabe oder Übertragung geschützter Informationen vorgeht (Informationspflicht, Berichterstattung, Zugang zu Auditergebnis).

In jedem Fall sind vertragliche Massnahmen daher mit anderen Schutzmechanismen zu kombinieren. Die Prüfung der Situation ist immer gemäss den konkreten Umständen vorzunehmen.

Verweis: Teil 2 (Ziff. 1.7.2), Anhang C.

3.3 Verhältnis von schweizerischem und ausländischen Recht

Frage: Kann die Anwendung von ausländischem Recht auf Daten einer Schweizer Behörde, die sich im Ausland befinden, vertraglich verhindert werden?

Antwort: Auch wenn die Anwendbarkeit von Schweizer Recht zwischen die Parteien vereinbart werden kann, bezieht sie sich lediglich auf die Vertragsbestandteile. Das Territorialitätsprinzip gilt immer. Beispielsweise kann sich ein amerikanisches Unternehmen nicht vollständig seiner gesetzlichen Verpflichtung entziehen, Daten im Rahmen eines Rechtsverfahrens in den USA offenzulegen, indem es einfach einen Vertrag unterschreibt, worin es sich verpflichtet, dies nicht zu tun. Deshalb sind vertragliche Massnahmen immer mit anderen Schutzmechanismen zu kombinieren.

Aber das Territorialitätsprinzip bedeutet auch, dass eine direkt an eine europäische Tochterfirma von einer amerikanischen Firma adressierte Herausgabeanordnung der US-Strafverfolgungsbehörden ausserhalb des US-Territoriums nicht mit strafprozessualem Zwang durchgesetzt werden kann.

Verweis: Teil 2 (Ziff. 1.6-1.7).

4 Technische Fragen mit rechtlichem Bezug

4.1 Verschlüsselung von Daten

Frage: Wann ist eine Verschlüsselung der Daten sinnvoll? Gibt es Empfehlungen?

Antwort: Das Datenschutzgesetz verpflichtet die Bearbeiter, Daten auch durch technische Massnahmen zu schützen. Eine Verschlüsselung ist sinnvoll, wenn die Risikoanalyse im Einzelfall aufgezeigt hat, dass eine solche Schutzmassnahme für die jeweiligen Daten am angemessensten ist und dass sie dazu beiträgt, einen adäquaten und rechtskonformen Schutz zu erreichen. Das ist insbesondere der Fall, wenn es um Personendaten (ohne Anonymisierungsmöglichkeit) oder klassifizierte Informationen geht und ein Risiko eines Behördenzugriffs auf die Daten im Ausland besteht.

Entscheidend ist bei Verschlüsselungsmassnahmen das Schlüsselmanagement. Dabei ist zu klären, wer den Schlüssel tatsächlich verwaltet, ob der Schlüssel aufgeteilt wird und wie ein Verlust des Schlüssels verhindert wird oder wie Schlüssel wiederhergestellt werden können (Key Recovery).

- Grundsätzlich sind in dieser Hinsicht Lösungen anzustreben, bei denen die Auftragsdatenbearbeitenden keinen oder nur sehr eingeschränkten Zugriff auf die Schlüssel haben (z.B. «Bring Your own Key» oder «Keep your own Key»). Andere Ansätze, die dazu dienen, Daten vor unberechtigter Kenntnisnahme zu schützen, wie bsp. durch Beschränkung der Zugriffsrechte und durch ergänzende Sicherheits- bzw. Authentifizierungssysteme, müssen auch berücksichtigt werden.
- Ebenfalls ist zu beachten, dass die Verschlüsselungstechnologie einem raschen Wandel unterliegt und gegebenenfalls dem aktuellen Stand der Technik angepasst werden muss.
- Es ist jeweils insbesondere zu prüfen, ob die verwendeten Verschlüsselungsstandards sowie die Massnahmen zum Schutz der Schlüssel genügend sind. Der Zustand der Daten ist auch zu berücksichtigen (*data in transit; data in use* oder *data at rest*).
- Neue Verschlüsselungstechniken (z.B. homomorphe Verschlüsselung) versprechen ebenfalls neue Möglichkeiten; sie sind allerdings noch nicht überall marktreif.

Verweis: Teil 2 (Ziff. 1.2.2), Anhang B bis D; Vorgabe Si001 (IT-Grundschutz in der Bundesverwaltung); Art. 7 und 9 DSG.

4.2 Vorgaben über die Verfügbarkeit von Daten

Frage: Gibt es gesetzliche/vertragliche (bspw. EU) Vorgaben, welche die Verfügbarkeit von Daten regeln?

Antwort: Nach Art. 2 Bst. b DSV sorgt der Verantwortliche dafür, dass die Daten jederzeit eingesehen werden können. Diese Anforderung ist umso höher, wenn die Informationen für die Erfüllung wesentlicher oder sogar gesetzlicher Aufgaben ständig verfügbar sein müssen. Art. 3 Abs. 2 DSV sieht diesbezüglich vor, dass die Massnahmen die Kontrolle der Datenträger, des Speichers, des Transports sowie der Wiederherstellung gewährleisten sollen. Die Massnahmen müssen geeignet sein, um die Verfügbarkeit zu gewährleisten. In diesem Sinn muss die Sicherheit des Systems auf dem neuesten Stand gehalten werden.

Die Verfügbarkeit von geschäftsrelevanten Informationen muss jederzeit dem Schutzbedarf entsprechend sichergestellt sein. Die für Informationen verantwortliche Verwaltungseinheit muss über eine Backup-Strategie verfügen und diese auch umsetzen. Diese Strategie muss ein Mehrgenerationen-Prinzip und eine offline Speicherung wichtiger Datenbestände vorsehen, so dass Daten auch im Falle von datenverschlüsselnder Malware («Ransomware») wiederhergestellt werden können.

Die Verwaltungseinheit kann ausserdem die Einhaltung von Standards/Best Practices durch den Cloud-Service-Anbieter in Bezug auf die Verfügbarkeit vertraglich verlangen oder Konventionalstrafen vereinbaren, die fällig werden, wenn bestimmte Verfügbarkeitsziele nicht eingehalten werden.

Verweis: Art. 8 nLPD, Art. 2 Bst. b und 3 Abs. 2 DSV, Art. 32 Abs. 1 Bst. b und c DSGVO, Anhang C, Vorgabe Si001 (IT-Grundschutz in der Bundesverwaltung), Vorgabe P041 (Schutzbedarfsanalyse), Vorgabe SD100 (Servicekatalog SD).

5 WTO-20007

5.1 Verträge der WTO 20007

Frage: Welche vertraglichen Abmachungen sind in der WTO-20007 vereinbart und wo kann ich die Rahmenverträge einsehen, damit ich sehe, was überhaupt abgedeckt ist mit dieser WTO?

Antwort: Mit den fünf Cloud-Anbietern Ali Baba, Amazon, IBM, Microsoft und Oracle als Zuschlagsempfängerinnen wurden gestützt auf die Ausschreibungsbedingungen zur WTO-20007 Rahmenverträge für die Nutzung von Public-Cloud-Diensten ausgehandelt. Dabei wurde unter anderen mit allen fünf Anbietern verbindlich vereinbart, dass Schweizer Recht anwendbar und der Gerichtsstand Schweiz vorzusehen ist. Da die Verträge teils unterschiedliche Vereinbarungen beinhalten, sollte bei einem bestehenden konkreten Bedarf neben vorab zu prüfender Frage, ob der jeweilige Bedarf vom Leistungsgegenstand und der sonstigen inhaltlichen und formellen Vorgaben der Ausschreibung umfasst ist, jeweils auch die Verträge eingesehen werden. Die Rahmenverträge liegen bei den Generalsekretariaten der Departemente. Wollen diese eingesehen werden, müssen die Verwaltungseinheiten die Rahmenverträge bei ihren Departementen anfordern.

5.2 Fragen zu Power BI / Power Apps

Frage: Fallen Power BI (Server) und Power Apps unter die WTO 20007?

Antwort: Der Leistungsgegenstand zur WTO-20007 wird in Ziff. 3.1 f. des Pflichtenheftes sowie in den dazugehörigen Anhängen zur Ausschreibung konkret beschrieben. Die Abgrenzung dazu in Ziff. 3.2.1 ist nicht als abschliessende Aufzählung zu verstehen. Soweit demnach ein bestimmter Bedarf nicht konkret im Leistungsgegenstand umschrieben ist, ist durch Auslegung der Ausschreibungsunterlagern zu ermitteln, ob ein nicht explizit genannter Inhalt - aus der Betrachtung der Fachwelt - als vom Beschaffungsgegenstand noch erfasst gelten kann (auf den subjektiven Willen der Vergabestelle kommt es nicht an).

Aus diesem Prüfprozess ergibt sich im Einzelfall, ob eine ausreichende vergaberechtliche Grundlage für die Erstellung eines Pflichtenheftes im Rahmen eines Abrufverfahrens unter der WTO-20007 besteht oder andernfalls eine andere Beschaffungsgrundlage zu schaffen sein wird.

Soweit ein konkreter Bedarf unter den Scope der WTO-20007 fällt, hat sich die Vergabestelle in der Ausschreibung zur Durchführung von Abrufverfahren wie im Pflichtenheft beschrieben formell bekannt (d.h. Herstellung eines Wettbewerbs unter den Zuschlagsempfängern), wie der Ablauf im Pflichtenheft dazu beschrieben ist.

5.3 Ablauf der WTO 20007

Frage: Muss man immer das Abrufverfahren durchlaufen oder kann man direkt zu einem Anbieter?

Antwort: Ja, man muss immer ein Abrufverfahren durchlaufen. Das Cloud Abrufverfahren ist in den Rahmenverträgen mit den Cloud-Anbietern geregelt. Die Verwaltungseinheit, die einen Bedarf abdecken möchte, klärt zuerst, ob Cloud-Dienste genutzt werden dürfen. Im positiven Fall erstellt der Bedarfsträger ein anbieterneutrales Pflichtenheft sowie einen Kriterienkatalog.

Der Bedarfsträger bewertet die Kriterien anhand der öffentlich verfügbaren Informationen der Cloud-Anbieter. Der in der Evaluation am besten bewertete Anbieter muss gewählt werden.

Das Abrufverfahren ist in den Cloud-Prinzipien näher umschrieben. Weitere Fragen und Informationen gibt das BIT als CSB der Bundesverwaltung unter der E-Mail Adresse: csb@bit.admin.ch.

Verweis: AR010 – Cloud-Prinzipien der Bundesverwaltung

5.4 Leistungserbringer vs. Leistungsbezüger

Frage: Brauche ich noch einen (internen) LE für die Integration und den Betrieb?

Antwort: Gemäss Cloud-Strategie der Bundesverwaltung[2] beziehen die Verwaltungseinheiten Public Cloud-Dienste grundsätzlich über einen Cloud-Service-Broker (CSB). Der CSB der Bundesverwaltung ist das BIT. Die Public-Cloud-Dienste sind somit grundsätzlich über das BIT zu beziehen. Der Bereich DTI der Bundeskanzlei kann gemäss Cloud-Strategie Ausnahmen vorsehen. Solche Ausnahmen sind heute MeteoSchweiz und Swisstopo.

Verweis: Cloud Strategie der Bundesverwaltung, S. 11, Grundsatz 0-2.

5.5 Verhältnis zwischen der WTO 20007 und anderen Beschaffungen

Frage: Ich habe eine Software-Beschaffung gemacht. Der Lieferant setzt eine Komponente ein, welche durch einen der WTO 20007-Cloud-Anbieter geleistet wird (z.B. KI/Scanning); was gilt es zu beachten?

Antwort: Dieses Szenario ist aus Sicht WTO 20007 nicht relevant, denn der Lieferant setzt den Cloud-Anbieter als Unterauftragnehmer ein. Der Zuschlagsempfänger der beschaffungsrechtlich relevanten Vergabe war der betreffende Lieferant (mit dem in der Folge auch der Vertrag abgeschlossen wurde). Das Vertragsverhältnis besteht nur zwischen dem Lieferanten und dem Cloud-Anbieter. Auch hier sind indessen die nötigen vertraglichen, organisatorischen und technischen Massnahmen vorzusehen um den Schutz von Informationen und insb. Personendaten sowie die Business Continuity zu gewährleisten.

Frage: Wie ist vorzugehen, wenn ich einen Bezug gemacht habe für einen Teil meiner Anwendung und die WTO 20007 ausläuft, jedoch die meiner Anwendung nicht? Wer muss das im Auge behalten?

Antwort: Grundsätzlich tragen die Verwaltungseinheiten die Verantwortung für ihre Anwendungen. Soweit der Beschaffungsgegenstand aus der WTO 20007 volumenmässig oder zeitlich ausgeschöpft sein wird, wird eine neue vergaberechtliche Grundlage zu prüfen sein.

Frage: Was ist zu beachten, wenn ich schon eine Cloud-Anwendung beschafft habe? (sei es bei einem dieser Anbieter oder einem anderen mit gleichwertigen Angeboten)?

Antwort: Wurden Cloud-Dienste in einem eigenständigen Beschaffungsverfahren bereits früher oder parallel zu WTO 20007 beschafft, so behalten die entsprechenden Verträge weiterhin Gültigkeit. Auch hier sind indessen die nötigen vertraglichen, organisatorischen und technischen Massnahmen vorzusehen um den Schutz von Informationen und insb. Personendaten sowie die Business Continuity zu gewährleisten.

Frage: Was muss zuerst beschafft werden:

- Die Plattform oder
- der Entwickler/Die Fachanwendung?

[2] Cloud-Strategie der Bundesverwaltung (admin.ch)

Mache ich zuerst ein WTO 20007 Abrufverfahren und dann eine andere Beschaffung, um mir die Ressourcen oder Anwendungen zu kaufen, welche ich auf diese Plattform entwickeln/betreiben werde

oder

mache ich zuerst eine Beschaffung für die Ressourcen / Anwendungen und dann beschaffe ich die korrespondierende Plattform via WTO 20007?

Antwort: Es gibt keine Vorgaben, was zuerst beschafft werden muss. Es empfiehlt sich zuerst die Beschaffung der Plattform bzw. der Public-Cloud-Dienste. Je nach Auswahl des Cloud-Anbieters können dann die entsprechenden Entwickler der Fachanwendung beschafft werden. Bei der Beschaffung der Plattform muss gewährleistet werden können, dass ein anbieterneutrales Pflichtenheft ausgefüllt wird. Ist das von Beginn weg nicht möglich, kann nicht über die WTO 20007 beschafft werden.

Frage: Was ist das vorgesehene Vorgehen, falls die WTO 20007 einen Cloud-Anbieter vorgibt, für den keine verfügbare Ressourcen/Skills über die Dienstleistungs-WTO beschafft werden können – entweder weil es diese auf den Markt nicht gibt oder weil diese schon zeitlich nicht verfügbar sind?

Antwort: Die Verfügbarkeit von Ressourcen/Skills kann als Kriterium in die Evaluation des passenden Cloud-Anbieters aufgenommen werden. Die passenden Ressourcen/Skills können über unterschiedliche Beschaffungen laufen (die Cloud-Dienstleistungs-WTO 2007ist nur ein mögliches Gefäss). Falls für den gewählten Cloud-Anbieter dann keine Ressourcen gefunden werden können, kann eine neue Evaluation durchgeführt werden.