Anhang Checkliste zum Bericht rechtlicher Rahmen für die Benutzung von Public-Cloud in der Bundesverwaltung

Diese Checkliste soll Sie dabei unterstützen, vor «dem Gang in die Cloud» die richtigen Fragen zu stellen. Mit anderen Worten: Sollen Daten Ihrer Verwaltungseinheit in die Cloud ausgelagert werden, und wenn ja, welche technischen Massnahmen zu deren Schutz sollten vorhanden sein?

Adressatinnen und Adressaten dieses Hilfsmittels sind daher primär Mitarbeitende von Verwaltungseinheiten, die sich im Rahmen von Projekten zum ersten Mal die Frage einer Auslagerung der Daten in die Cloud stellen. Die Checkliste kann jedoch auch für bereits erfahrene Mitarbeitende eine nützliche Hilfe sein, sich die wichtigen Fragen zum Thema Auslagerung noch einmal zu vergegenwärtigen.

Die Checkliste soll weiter zum Ziel haben, dass die Auslagerung oder die Nichtauslagerung von Daten in die Cloud nachweisbar und wiederauffindbar dokumentiert ist.

Wichtig:

- Die Checkliste kann bei Bedarf und je nach Konstellation mit weiteren Fragen ergänzt werden.
- Die Einstufung der Antworten erfordert vertiefte Kenntnis der jeweiligen Thematik und sollte demnach in Absprache mit den dafür zuständigen Stellen erfolgen.
- Die Checkliste ersetzt KEINE Dokumentationen, die im Rahmen bspw. der Schuban oder des ISDS-Konzepts erstellt werden müssen.
- Sie behandelt auch keine Fragen zu Vertragsinhalten und gibt keine Antworten auf grundsätzliche rechtliche Problemstellungen im Zusammenhang mit der Auslagerung von Daten in die Cloud.

Anweisungen zur Benutzung der Checkliste

In einem *ersten Schritt* sollen die unten gestellten Fragen beantwortet und anhand des sich unter jeder Fragekategorie befindenden Balkens eingestuft werden. Die Idee ist, dass sich zu jeder Frage überlegt wird, in welchem Bereich die Antwort einzustufen ist: Je heikler / kritischer / wichtiger etc. die auszulagernden Daten bzw. die Antworten auf die Fragen einzustufen sind, umso eher ist der Themenkomplex im orange/roten Bereich zu verankern.

Die Antworten sind aus der (subjektiven) Perspektive des Amtes einzustufen. Je nach Art der Frage sollen diese mit unterschiedlichen Fachpersonen oder für bestimmte Themen spezialisierte Fachabteilungen (z.B. Abteilung Kommunikation bei Fragen zum medialen Interesse) abgeklärt werden.

Im Anschluss soll ein Gesamtüberblick über die Fragen bzw. die Einstufungen entstehen, anhand dessen die Möglichkeiten und Herausforderungen einer Auslagerung der Daten in eine Cloud grob eingestuft werden können.

Im *zweiten Schritt* «Mitigierung der Risiken» soll geprüft werden, wie die eruierten Risiken technisch/organisatorisch minimiert werden können. Erst nach Abschluss von Schritt zwei ist in einer Endevaluation zu entscheiden, ob die Daten ausgelagert werden oder nicht.

Im dritten Schritt soll die abschliessende Evaluation stattfinden und der Entscheid dokumentiert werden, ob die Daten in eine Cloud ausgelagert werden sollen oder nicht.

I. Schritt: Fragen zur Auslagerung in die Cloud

1.1 Datenschutz (siehe Kapitel 1 des Berichts)

a) Mögliche Fragestellungen

1. Sollen Personendaten in die Cloud ausgelagert werden? Wenn ja, welche, und wozu werden diese im Rahmen der Aufgabenerfüllung benötigt?
2. Sollen besonders schützenswerte Personendaten in die Cloud ausgelagert werden? Wenn ja[1], welche, und wozu werden diese im Rahmen der Aufgabenerfüllung benötigt?
3. Ist eine Datenschutzfolgeabschätzung notwendig? Diese muss dann durchgeführt werden, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.
4. Sofern notwendig oder erwünscht: Können die Personendaten anonymisiert (in diesem Fall spricht man nicht mehr von Personendaten mehr) oder pseudonymisiert (in diesem Fall sind rechtlich gesehen noch Personendaten vorhanden) werden? Wer hat den Schlüssel für die Pseudonymisierung?
5. Sofern notwendig oder erwünscht: Können die Daten verschlüsselt werden? Wenn ja, wer hat den Schlüssel (bring your own key; hold your own key)?

b) Einstufung der Antworten

1.2 Geheimhaltungspflichten (siehe Kapitel 2 des Berichts)

a) Mögliche Fragestellungen

6. Gibt es eine spezialgesetzliche Grundlage, welche die eine Auslagerung in eine Cloud verbietet?
7. Unterstehen Daten spezialgesetzlichen Geheimhaltungsvorschriften?
8. Sofern notwendig oder erwünscht: Können die Daten gemäss ihrem Schutzbedarf angemessen geschützt werden?

b) Einstufung der Antworten

1.3 Informationssicherheit (siehe Kapitel 3 und 4 des Berichts)

a) Mögliche Fragestellungen

9. Ist die Klassifizierungsstufe der Informationen nach ISchV (künftig ISG) noch aktuell bzw. korrekt, das heisst wurden die Kriterien der Klassifizierung nochmals überprüft? Insbesondere:

[1] Achtung, in diesem Falle muss gem. Cloud Strategie eine Info an NCSC, EDÖB, GSK erfolgen.

9.1. Gibt es noch weitere Geheimhaltungsinteressen, die in diesem Zusammenhang beachtet werden müssen?
9.2. Kann das behördliche Handeln gefährdet oder verunmöglicht werden, wenn die Daten bekannt werden?
10. Können klassifizierte Informationen bei der Cloud-Nutzung gemäss ihrem Schutzbedarf angemessen geschützt (bspw. verschlüsselt) werden?
Können trotz einer Auslagerung die Anforderungen an den IKT-Grundschutz der Bundesverwaltung eingehalten/erfüllt werden?

b) Einstufung der Antworten

1.4 Integrität (siehe Kapitel 2 des Berichts)

a) Mögliche Fragestellungen

11. Kann sichergestellt werden, dass auch bei einer Auslagerung der Daten Bearbeitungsvorgänge nachvollziehbar dokumentiert werden, so dass Daten nicht unbemerkt oder unberechtigt verändert werden?
12. Welche Auswirkungen hätte eine unbemerkte Veränderung der Daten?
13. Ist sichergestellt, dass bei der Übertragung von Daten keine Fehler passieren und die Daten nicht verändert werden können?
14. Kann die Revisionssicherheit der Daten bei einer Auslagerung sichergestellt werden?

b) Einstufung der Antworten

1.5 Verfügbarkeit / Resilienz / Einsatzkritikalität

a) Mögliche Fragestellungen

15. Von wem werden die Daten genutzt? Müssen Bürgerinnen und Bürger darauf zugreifen können oder «nur» Mitarbeitende?
16. Welche Anforderungen an die Verfügbarkeit sind gegeben? 24/7 (für CH-Botschaften, Zoll usw.)? Bürozeiten (MEZ)?
17. Wie lange darf ein Unterbruch der Zugriffsmöglichkeit maximal andauern?
18. Gibt es gesetzliche/vertragliche (bspw. EU) Vorgaben, welche die Verfügbarkeit regeln?
19. Was wäre die Konsequenz, wenn nicht verfügbar?
20. Gibt es Ausweichmöglichkeiten BCM (Business Continuity Managemen)?

b) Einstufung der Antworten

1.6 Staatliche Souveränität / ausländische Rechtsnormen (siehe Kapitel 2.6 des Berichts)

a) Mögliche Fragestellungen

21. Gibt es Gründe, dass die Daten ausschliesslich in der Schweiz bearbeitet werden dürfen?
    21.1. Rechtliche Grundlagen?
    21.2. Politische Gründe?
22. Gibt es ausländische Rechtsnormen, welche gewisse, für den Schutz der Daten notwendige Massnahmen in bestimmten Staats/Regionen einschränken oder verbieten?
23. Was sind die Folgen / Konsequenzen für die Bundesverwaltung, wenn die Daten aufgrund internationaler rechtlicher Grundlagen herausgegeben werden? (Bspw. Beschlagnahmung)
24. Was sind die Folgen / Konsequenzen, wenn aufgrund staatlicher Sanktionen bspw. der Zugang zu den Daten (temporär) verwehrt wird?
25. Was sind die Folgen / Konsequenzen, wenn aufgrund von staatlichen Sanktionen die Verschlüsselung von Daten verboten wird?

b) Einstufung der Antworten

1.7 Politische Vertretbarkeit einer Auslagerung / Medieninteresse

a) Mögliche Fragestellungen

26. Wie gross ist das mediale Interesse an den auszulagernden Daten?
27. Wie gross ist das mediale Interesse, wenn die Daten widerrechtlich bekannt werden?
28. Besteht ein Risiko eines bei der Auslagerung der Daten in eine Cloud? Wenn ja, wie gross wäre dieser? Folgen/Konsequenzen?

b) Einstufung der Antworten

1.8 Cloud Exit-Strategie

a) Mögliche Fragestellungen

29. Wie sieht eine mögliche Cloud-Exit Strategie aus?
30. Welche (technischen) Lösungen gibt es?
31. Mit welchem Aufwand und mit welchen Kosten muss bei einem Cloud-Exit gerechnet werden?

b) Einstufung der Antworten

1.9 Vendor Lock-In

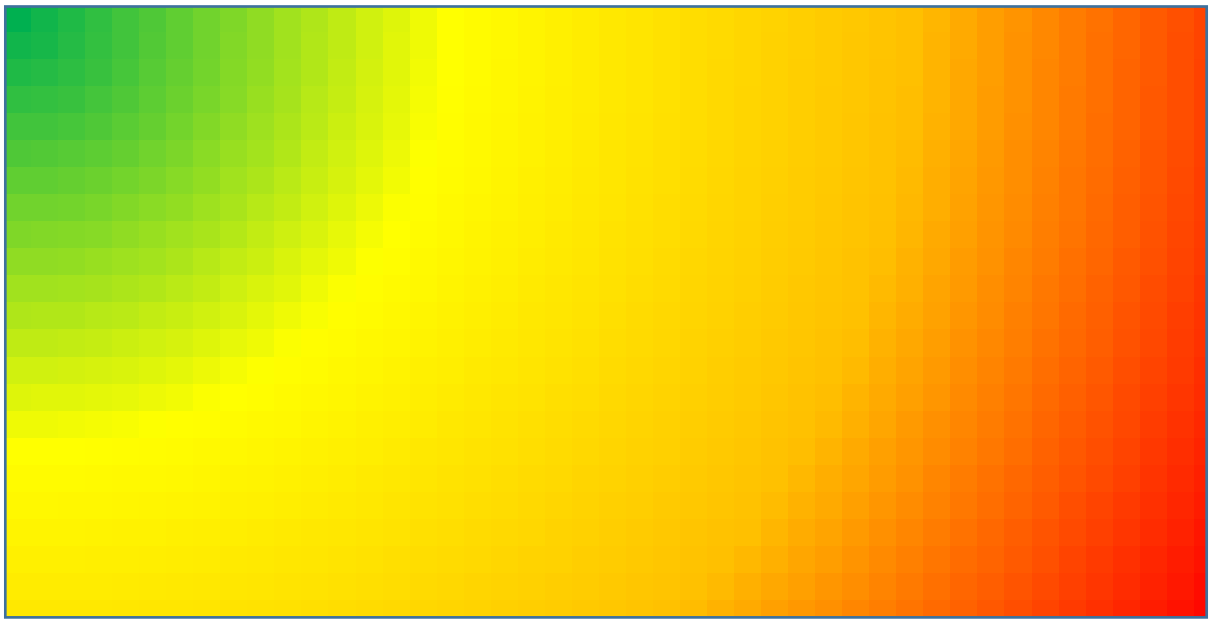
a) Mögliche Fragestellungen

32. Gibt es ein Migrationskonzept für einen Wechsel zu einem anderen Cloud-Provider?
33. Mit welchem Aufwand und mit welchen Kosten muss bei einer Migration gerechnet werden?
34. Lässt es die Art der Datensammlung zu, die einzelnen Datensätze getrennt in verschieden Clouds auszulagern? Was ist der Aufwand und die geschätzten Kosten?
35. Gibt es die Möglichkeit, die Lösung portabel zu offenen Standards machen?

b) Einstufung der Antworten

2. Gesamtübersicht der Beurteilung der Antworten

Hier können die in den Ziff. 1-33 gegebenen und in den jeweiligen Balken verorteten Antworten zu einer Gesamtübersicht zusammengetragen werden.



II. Schritt: Mitigierung der Risiken (siehe Kapitel 1.4 des Berichts)

Es sind mögliche Massnahmen zur Mitigierung der in Schritt I erkannten Risiken zu evaluieren («was muss ein Cloud-Anbieter bieten, damit trotz oranger/roter Einstufung den Gang in die Cloud gewagt werden kann», «welche Massnahmen können intern getroffen werden»). Ebenfalls ist festzulegen, welche Risiken getragen werden können / sollen.

[*Folgende Dokumente werden hier verlinkt*]:

- Anhang C Risiken und Massnahmen
- GAP-Analysen der Cloud-Anbieter
- Vorlage Risikoanalyse WTO 20007

III. Schritt: Abschliessende Evaluation und Entscheidung

Nachdem alle Fragen gestellt wurden und eine Mitigierung der Risiken gemacht wurden, muss ein abschliessender Entscheid für oder gegen eine Auslagerung der Daten in die Cloud gefällt werden. Diesem sollen die oben gemachten Erkenntnisse zugrunde gelegt und im Rahmen der Begründung die verschiedenen Abwägungen etc. belegt/dokumentiert werden.