Rechtliche Checkliste **zum Einsatz von Cloud Computing**		**Information** **ChCC 1.0.0** **Ergebnis der AG**
Kurzbeschreibung	Dieses Dokument soll Behörden vor der Entscheidung, ob ein Datenbestand in die Cloud übergeführt wird bzw. bei der Auswahl eines Cloud-Dienstleisters in Form einer rechtlichen Checkliste / eines Fragenkatalogs als Hilfestellung dienen. Es werden dabei ausschließlich die rechtlichen Eckpfeiler behandelt und keinerlei Aussagen über die technische, organisatorische oder wirtschaftliche Machbarkeit getroffen.	
Autor(en):	Karin Luttenberger (Wien) Gregor Schmied (BKA)	Projektteam / Arbeitsgruppe: AG Recht und Sicherheit
Beiträge von:	Anna-Karina Hafner (Tirol), Bernhard Karning (BKA), Christian Schuller (HVB), Harald Stradal (BMI), Hannes Wittmann (Wien) Inhaltlich basiert die Checkliste größtenteils auf Kapitel 4 des Cloud Computing Positionspapiers (CloudComp-Pos-1.0.1).	

Version: 1.0.0 Angenommen: 25.11.2015 mit VSt-1712/527

Rechtliche Checkliste zum Einsatz von Cloud Computing

Inhaltsverzeichnis

1. DATENSCHUTZ

- ✓ Werden personenbezogene Daten verwendet?

  Werden keine personenbezogenen Daten verwendet, dann ist keine weitere datenschutzrechtliche Prüfung erforderlich.

  Wenn es sich hingegen um personenbezogene Daten handelt, dann sind bei der Wahl des Cloud Service Providers (CSP), welcher als Dienstleister[1] im Sinne des § 4 Z 5 DSG 2000 zu beurteilen ist, nachstehende Fragen zum Datenschutz zu prüfen. Alle Fragen sind vor der Auswahl eines Cloud-Dienstes stets mit „**Ja**“ zu beantworten:

1.1. Verarbeitungs- bzw. Speicherort von Daten (Storage)

Bestimmte Datenschutzbestimmungen verbieten den Transfer von Daten in andere oder bestimmte Länder, oder es ist die explizite Zustimmung durch jene Person, auf die sich die Daten beziehen, erforderlich. Eine dynamische Umverteilung im Laufe der Zeit ist mit zu beachten.

Bestehende Regelungen, wonach Daten ausschließlich im Inland gespeichert werden dürfen (zB im Zusammenhang der umfassenden Landesverteidigung), schließen CSP außerhalb Österreichs aus!

- ✓ Werden die Daten ausschließlich im europäischen Wirtschaftsraum oder in Ländern, die in der Datenschutzangemessenheits-Verordnung angeführt sind, verarbeitet? [2]
  - o Wenn nein, liegt eine Genehmigung der Datenschutzbehörde oder liegen Standardvertragsklauseln[3] für die Übermittlung personenbezogener Daten in Drittländer (2001/497/EG) vor?

---

[1] Es wird angemerkt, dass der Auftraggeber bei der Auswahl seines Dienstleisters die freie Wahl hat, jedoch muss dieser die auch die Dienstleisterpflichten einhalten. Der Auftraggeber hat weiters seine Auftraggeberpflichten einzuhalten bzw. sicherzustellen, dass sein Dienstleister dies tut. Die Verantwortung für die Einhaltung dieser Auftraggeber- und Dienstleisterpflichten verbleibt jedoch letztlich beim Auftraggeber. Im Einzelfall kann die Abgrenzung der Rolle des Auftraggebers und des Dienstleisters schwierig sein. Im Zweifel ist jedoch anzunehmen, dass die Behörde als Auftraggeber angesehen wird.

[2] § 12 DSG 2000: Übermittlung und Überlassung an Empfänger im Europäischen Wirtschaftsraum ist keinen Beschränkungen unterworfen. Weiters bedarf der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutz keiner Genehmigung gemäß § 13 (vgl. auch Datenschutzangemessenheits-Verordnung).

§ 13 DSG 2000: Sofern die Datenübermittlung ins Ausland nicht genehmigungsfrei gemäß § 12 ist, so ist eine Genehmigung der Datenschutzbehörde vor der Übermittlung einzuholen.

[3] http://www.dsb.gv.at/site/6208/default.aspx

1.2. Datensichersicherheitsmaßnahmen

- ✓ Stellt der Dienstleister die Maßnahmen zur Datensicherheit gemäß § 14 DSG 2000 sicher?
- ✓ Trifft der Dienstleister insbesondere Maßnahmen zum Schutz vor zufälliger und unrechtmäßiger Zerstörung?
- ✓ Trifft der Dienstleister insbesondere Maßnahmen gegen den Verlust oder unbefugtem Zugriff auf die Daten?
- ✓ Trifft der Dienstleister insbesondere Maßnahmen zur Protokollierung der Zugriffe?

1.3. Betroffenenrechte (Auskunfts-, Richtigstellungs-, Löschungs- und Widerspruchrecht) gemäß §§ 26 bis 28 DSG 2000

Zugriff auf Daten (Access): Die Person, auf die sich Daten beziehen (d.h. der/die Betroffene im Sinne des DSG), kann sowohl Auskunft über, als auch Korrektur oder das Löschen dieser Daten verlangen.

- ✓ Ist daher sowohl die Einsichtnahme als auch die Richtigstellung bzw. das Löschen der Daten der Betroffenen in der Cloud gemäß den rechtlichen Vorgaben gewährleistet und durchführbar?
- ✓ Gibt es ein Regelwerk das das Verfahren zur Wahrung der Rechte der Betroffenen in einem Informationsverbundsystem klar regelt?

1.4. Verbleib und Vernichtung von Daten (Retention/Destruction)

Am Ende der Haltezeit von Daten müssen diese geeignet gelöscht werden.

- ✓ Gibt es ein Regelwerk zur Umsetzung der Skartierung von Daten (Retention-Policy)?
- ✓ Gibt es ein Regelwerk zur Skartierung von Protokolldaten einschließlich Verkehrs- und Metadaten?
- ✓ Werden die Daten tatsächlich gelöscht (und nicht nur die Zugriffsrechte entzogen)?
- ✓ Ist dabei sichergestellt, dass keine Kopien der Daten (z.B. Back-Up) erhalten bleiben?
- ✓ Gibt es ein Regelwerk, wonach die Zurückstellung (inkl. Löschung der Daten beim CSP) an den Auftraggeber nach Beendigung des Vertragsverhältnisses erfolgt?

1.5. Datenschutzverletzungen (Privacy Breaches):

- ✓ Ist bei Datenschutzverletzungen ein Meldeprozess bei Auftraggeber und Dienstleister etabliert?

2. VERTRAGSRECHT

Sollte immer auf den Einzelfall abgestimmt sein. Folgende Punkte könnten jedoch Inhalt einer vertraglichen Regelung sein:

- ✓ Zusicherung der Einhaltung der datenschutzrechtlichen Anforderungen;
- ✓ Informationsverfahren bei datenschutzrechtlichen Verletzungen;
- ✓ Gewährung eines Kontrollzugriffs durch den Auftraggeber;
- ✓ Dienstleistervereinbarungen (abhängig von der Anzahl der Dienstleister bzw. Sub-Dienstleister die in Anspruch genommen werden);
- ✓ Art der Leistung (Leihe, Miete, Werk- oder Dienstleistung);
- ✓ Haftung und Gewährleistungsansprüche;
- ✓ Service-Level-Agreement (SLA);
- ✓ Sonstige Vereinbarungen (zB ISO 27001, Informationssicherheitsmanagementsystem (ISMS);
- ✓ Einhaltung referenzierter Konvention (internationale Standards, BLSG-Konventionen);
- ✓ Migrierbarkeit der (Daten-)Standards im Fall des Betreiberwechsels, Unternehmensübergang oder im Insolvenzfall;

3. VERGABERECHT

- ✓ Cloud Service Provider sind meist international tätig und stellen ihre Leistungen unter Standard-AGB zur Verfügung. Es ist daher zu prüfen, ob sich diese CSP überhaupt an einem formellen Ausschreibungsverfahren beteiligen würden und sich Abweichungen von den AGB mit dem jeweiligen CSP vereinbaren lassen.

4. STRAFPROZESSRECHT

- ✓ Innerstaatliche Auskunftspflichten gegenüber österreichischen Strafverfolgungsbehörden sind zu beachten (zB Verkehrsdaten)

Dokumentenhistorie

Version 1.0.0	14.10.2015	- Erstellt
Autoren: siehe oben		