

Wolfgang Straub

Checkliste zu Cloud Verträgen in der Anwaltskanzlei

Die vorliegende Checkliste ergänzt den Beitrag, «Vom Keller zur Cloud – digitales Arbeiten in der Anwaltskanzlei» im Jusletter vom 1. Mai 2017

Beitragsarten: Tagungsberichte

Rechtsgebiete: Notariats- und Anwaltsrecht, Informatikrecht

Zitiervorschlag: Wolfgang Straub, Checkliste zu Cloud Verträgen in der Anwaltskanzlei, in: Jusletter 1. Mai 2017

[Rz 1] Der Einsatz von Cloud Services in der Anwaltskanzlei wirft eine Vielzahl von Rechtsfragen auf. Einige – aber nicht alle – dieser Fragen lassen sich vertraglich regeln. Die vorliegende Checkliste¹ versteht sich als Ergänzung zu einer systematischen Vorgehensmethodik, welche folgende Elemente umfasst:²

- Analyse der Interessenlage
- Bestimmung des auszulagernden Bereiches
- Analyse der rechtlichen Anforderungen und der notwendigen Ressourcen
- Analyse der wirtschaftlichen, technischen und rechtlichen Chancen und Risiken
- Festlegung der Kriterien für die Auswahl und die Zusammenarbeit mit dem Provider
- Regelung der Zuständigkeiten und Verantwortlichkeiten zwischen den Parteien
- Instruktion und Überwachung des Providers
- Eventuell Information/Zustimmung der Klienten einholen

[Rz 2] Die vorliegende Checkliste ist auf komplexe Services zugeschnitten. Sie erhebt aber keinen Anspruch auf Vollständigkeit. Wenn die Vertragsbedingungen vom Provider vorgegeben werden, kann die Checkliste helfen, Risiken zu erkennen und darüber zu entscheiden, ob die Konditionen für die beabsichtigte Verwendung akzeptabel sind oder nicht.

¹ Siehe auch die Checkliste ‚Cloud Computing‘ des Zürcher Anwaltsverbandes, sowie die Checkliste des CCBE, Guidelines on the use of cloud computing services by lawyers, www.ccbe.eu

² Siehe auch STRAUB WOLFGANG, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: AJP 7/2014, S. 905 ff. Weitere – nicht anwaltsspezifische – Checklisten zum Cloud Computing finden sich auch in den EURO CLOUD LEITFÄDEN zum Cloud Computing, online verfügbar unter www.eurocloudswiss.ch/index.php/publikationen/leitfaden. Siehe insbesondere den detaillierten Fragekatalog zur Informationssicherheit im Leitfaden Risk & Compliance, Kap. 6, S. 28 ff. Eine Checkliste für Audits findet sich bei HALPERT BEN (Hrsg.), Auditing Cloud Computing: A Security and Privacy Guide, Hoboken NJ 2011, S. 175 ff.

1. Rahmenbedingungen

1.1. Vertragsparteien

- 1.1.1. *Informationen zum Provider* und seinen Subunternehmern, insbesondere wo die Services erbracht werden und welche nationalen Rechtsvorschriften anwendbar sein können
- 1.1.2. Informationen zu bestehenden *Zertifizierungen des Providers* und seiner Subunternehmer; Verpflichtung zur Aufrechterhaltung während der Vertragsdauer
- 1.1.3. *Informationen zur Anwaltskanzlei*, insbesondere an welchen Standorten, von welchen Nutzern (z.B. Mitarbeitende, Klienten) und wofür die Services bezogen werden und welche Rechtsvorschriften anwendbar sein könnten

1.2. Vertragsdokumente und Änderungen

- 1.2.1. Verzeichnis der *Vertragsbestandteile* und Hierarchie der einzelnen Vertragsdokumente (keine Verweise auf URLs, welche vom Provider einseitig aktualisiert werden können!)
- 1.2.2. *Form* von Vertragsänderungen (keine einseitigen Änderungsrechte!) und von Erklärungen an die Gegenpartei, welche die Rechtslage gestalten; elektronische Zustellung von Dokumenten (z.B. Rechnungen, Reports, Mitteilungen)

1.3. Begriffsdefinitionen und Verweise auf Standards

1.4. Nebenpflichten und Obliegenheiten

- 1.4.1. *Mitwirkungs- und Informationspflichten* (z.B. Benachrichtigung bei Leistungseinschränkungen, welche für die Anwaltskanzlei nicht ohne weiteres erkennbar sind); Form des Abrufs und der Abmahnung von Mitwirkungspflichten
- 1.4.2. Unterstützung von Dritteleistungserbringern der Anwaltskanzlei durch den Provider
- 1.4.3. *Dokumentation* von System und Prozessen

2. Inhalt der Leistung

2.1. Grundlagen

- 2.1.1. *Beschreibung aller Kanzleistandorte* etc., von denen aus *Zugriffe* auf Daten der Anwaltskanzlei möglich sind

- 2.1.2. *Beschreibung aller Rechenzentren etc.*, in welchen vertragliche Leistungen erbracht werden können (Lokalisierung, Zertifizierung etc.)
- 2.1.3. Beschreibung der dedizierten Infrastruktur (Private Cloud)
- 2.1.4. Spezifizierung der zur Verfügung gestellten *Softwareversionen* (Funktionen, Optionen, Customizing-Möglichkeiten etc.)
- 2.1.5. Deklaration von *Drittleistungen*, welche der Provider anbietet (z.B. Zurverfügungstellen von Software Dritter oder Leistungen externer Infrastructure Service Provider); Offenlegung der Lizenzbedingungen für entsprechende Software und der Service Level Agreements für Wartungs- und Supportleistungen Dritter → Einbezug in Geheimhaltungspflichten
- 2.1.6. Regelung der *Nutzungsrechte* an vom Provider verwendeter Software bzw. von ihm erbrachten Services. Sofern Drittsoftware im Rahmen von Cloud Services genutzt werden soll, sind dafür entsprechende Lizenzen erforderlich. Können auch allfällige bereits vorhandene Lizenzen der Anwaltskanzlei im Rahmen der Cloud Services verwendet werden? Dies setzt eventuell Erweiterungen/Umwandlungen der Lizenzen voraus.
- 2.1.7. Regelung der Immaterialgüterrechte an individuellen *Zusatzentwicklungen* für die Anwaltskanzlei
- 2.1.8. Technische Voraussetzungen auf Seiten der Anwaltskanzlei, Möglichkeiten des Datenimports und -exports, Beschreibung der *Schnittstellen* zu Systemen und Anwendungen der Anwaltskanzlei
- 2.1.9. *Portierbarkeit* von Applikationen und Daten auf andere Plattformen, Compliance mit Standards
- 2.1.10. Schulungskonzepte, Anwender- und *Betriebshandbücher*
- 2.2. Verantwortungsbereiche
 - 2.2.1. Definition der *Verantwortungsbereiche der Anwaltskanzlei* (inhaltliche Verantwortung, Datenherrschaft)
 - 2.2.2. Definition der *Verantwortungsbereiche des Providers* (Leistungserbringung, Umsetzung von Weisungen der Anwaltskanzlei als Erfüllungshilfe, technische Schutzmassnahmen etc.)
 - 2.2.3. Subsidiäre Abgrenzungsregeln
- 2.3. Weisungsrecht
 - 2.3.1. Ist das *Weisungsrecht* der Anwaltskanzlei klar definiert?

- 2.3.2. Wie ist vorzugehen, wenn *Weisungen der Anwaltskanzlei* nach Auffassung des Providers *gegen* das Datenschutzrecht oder sonstige gesetzliche *Vorschriften verstossen*?
- 2.3.3. Innerhalb welcher Fristen und in welcher Form müssen *Verstöße des Providers* oder seiner Mitarbeitenden und Subunternehmer gegen gesetzliche Vorschriften, vertragliche Bestimmungen oder Weisungen der Anwaltskanzlei diesem mitgeteilt werden? (siehe auch Ziff. 4.1.2)
- 2.4. Migration
 - 2.4.1. Beschreibung Initialprojekts sowie einer allfälligen *Migration* (z.B. Ablauf, Projektorganisation, Konflikteskalationsprozedere)
 - 2.4.2. Beschreibung der *Abnahmeprozesse* und der Bedeutung der Abnahmen (Inkraftsetzen von Service Level Agreements, Zahlungsvoraussetzungen, Vertragsausstiegsmöglichkeiten beim Scheitern von Abnahmen etc.)
- 2.5. Servicebeschreibung
 - 2.5.1. *Beschreibung der Leistungen und Definition der Service Levels*, z.B. Definition von Mindestverfügbarkeiten, Übertragungsbandbreiten, Systemantwortzeiten, Support Levels, Recovery Time Objectives (wie lange darf ein Geschäftsprozess oder ein System ausfallen?), Recovery Point Objectives (wie viel Datenverlust kann in Kauf genommen werden?) und Zufriedenheit der Nutzer durch Key Performance Indicators
 - 2.5.2. Definition von *Wartungsfenstern* (maximale Unterbruchsdauer, Form, Inhalt und Fristen der Vorankündigung)
 - 2.5.3. *Support, Störungs- und Fehlermanagement* (Beschreibung des Behebungs- und Supportprozesses, insbesondere Verfügbarkeit der Hotline, Ticketing, Supportsprachen, Interventions- und Behebungszeiten, Konflikteskalationsprozesse)
 - 2.5.4. *Service Level Monitoring*: Wie wird die Erfüllung der Service Levels gemessen? Über welche Parameter wird informiert? Welches sind die Mess- und Abrechnungsperioden (Synchronisierung mit Vergütungsperioden!)? Besteht eine Möglichkeit zur externen Überprüfung?
 - 2.5.5. *Service Level Management* (z.B. automatische Preisminderungen, Malus, Konventionalstrafen)
 - 2.5.6. *Release Management* für Software (Beschreibung von Releasezyklus, Testing, Ablehnungsmöglichkeiten neuer Releases, Pflege von individuellen Modifikationen und Konfigurationen etc.)

2.6. Change Management

- 2.6.1. *Voraussetzungen für Leistungsänderungen auf Wunsch der Anwaltskanzlei* (z.B. Mindestbezugsmengen / Mindestbezugsdauern, Skalierungsmöglichkeiten, Exit-Optionen)
- 2.6.2. *Voraussetzungen für Leistungsänderungen auf Wunsch des Providers* (z.B. garantierte Mindestdauer bestimmter Services, Vorankündigungsfristen für die Einstellung oder Änderung bestimmter Services oder Schnittstellen, Definition von Subunternehmern, bei deren Wechsel die ausdrückliche Zustimmung der Anwaltskanzlei eingeholt werden muss)
- 2.6.3. Beschreibung des *Prozesses zur Anpassung der Services* an veränderte Anforderungen, insbesondere Skalierbarkeit (z.B. Storage, Bandbreiten, Softwarelizenzzpakete) und Modalitäten der Skalierung (z.B. wie rasch und zu welchen Kosten die Mengen erhöht oder reduziert werden können)

3. Vergütungen

3.1. Vergütungen

- 3.1.1. *Pauschalpreise* (z.B. für ein bestimmtes Leistungspaket)
- 3.1.2. *Nutzungsabhängige Gebühren* (z.B. nach Datenvolumen / zeitlicher Beanspruchung von Rechenleistung und Applikationen). Gibt es zusätzlich auch Flatrates (z.B. bei Erreichen bestimmter Schwellenwerte)? Gibt es eine Best Price Option?
- 3.1.3. *Aufwandsabhängige Leistungen* (Ansätze, Anforderungsprofile etc.)

3.2. Zusätzliche Kosten

- 3.2.1. Überwälzung von Auslagen, Spesen und Gebühren
- 3.2.2. Tragung von Umsatzsteuern (anwendbare Steuern, Steuersätze etc.)

3.3. Anpassungsmöglichkeiten von Vergütungen

- 3.3.1. Erhöhung und Reduktion entsprechend dem effektiven *Nutzungsumfang*
- 3.3.2. *Mengenrabatte* (z.B. für skalierbare Leistungen)
- 3.3.3. *Zeitlich degressive Vergütungen* (z.B. Infrastrukturleistungen)
- 3.3.4. *Indexierung* (z.B. aufwandsabhängige Leistungen)
- 3.3.5. Kosten für die *Pflege von individuellen Softwareanpassungen*

- 3.3.6. Eventuell *Benchmarking* marktgängiger Leistungen (Voraussetzungen, Wirkung, Kostentragung etc.)
- 3.4. Messung des Leistungsbezugs
- 3.5. Fälligkeitstermine, Abrechnungs- und Zahlungsmodalitäten
 - 3.5.1. *Beginn und Ende* der einzelnen Vergütungspflichten entsprechend der tatsächlichen Nutzung
 - 3.5.2. *Abrechnungs- und Zahlungsmodalitäten* (Abrechnungsperioden mit Service Level Management koordinieren!)
- 3.6. Verzug und Lösung von Differenzen über Zahlungsverpflichtungen
 - 3.6.1. Folgen bei *Verzug der Anwaltskanzlei* (z.B. Verzugszinsen, Leistungseinstellung, Vertragsauflösung)
 - 3.6.2. *Hinterlegungsmöglichkeit* auf ein Sperrkonto mit befreiender Wirkung bei Auseinandersetzungen über Zahlungsverpflichtungen, vertragliches Konflikt-skalationsverfahren bezüglich der Herausgabe
 - 3.6.3. *Verrechenbarkeit* gegenseitiger Ansprüche
 - 3.6.4. Ausschluss der *Zurückbehaltung oder Löschung von Daten der Anwaltskanzlei*

4. Sicherheit, Geheimnis- und Datenschutz

- 4.1. Geheimnis- und Datenschutz
 - 4.1.1. Definition von *Art, Zweck und Umfang der Erfassung, Bearbeitung und Nutzung von Klienten- und sonstigen Personendaten*, insbesondere Kreis der Betroffenen und der Zugriffsberechtigten, Dauer der Nutzung, Archivierung und Löschung der Daten.
 - 4.1.2. *Compliance mit Geheimhaltungs- und Datenschutzvorschriften* seitens der Anwaltskanzlei und des Providers sowie seiner Subunternehmer (z.B. Registrierung von Datensammlungen, Bearbeitungsreglemente, Datenschutzbeauftragte). Innerhalb von internationalen Anwaltskanzleien müssen unter Umständen kumulativ die Normen mehrerer Länder eingehalten werden!
 - 4.1.3. *Unterstellung des Providers* und seiner Subunternehmer als Hilfsperson unter die für die Anwaltskanzlei geltenden Geheimhaltungs- und Datenschutzvorschriften
 - 4.1.4. Definition einer *Ansprechstelle* für alle Belange des Datenschutzes auf Seiten der Anwaltskanzlei sowie auf Seiten des Providers und seiner

- Subunternehmer (z.B. Datenschutzverantwortlicher gemäss Art. 11a Abs. 5 lit. e DSGVO)
- 4.1.5. Unterstützungspflichten des Providers bezüglich von *Betroffenenrechten* (Auskunft, Berichtigung, Löschung und Sperrung der Daten)
- 4.1.6. *Geheimhaltungspflicht und Verwertungsverbot* des Providers sowie Pflicht zur Aufklärung, Überbindung und Überwachung der Einhaltung der Vorgaben auf Arbeitnehmer, Subunternehmer, Konzerngesellschaften etc., welche Einblick in die Daten der Anwaltskanzlei erhalten könnten
- 4.1.7. *Zertifizierungen des Providers* und seiner Subunternehmer, Verpflichtung zu deren Aufrechterhaltung
- 4.1.8. *Allfällige Zertifizierungen der Anwaltskanzlei*, Mitwirkungspflichten des Providers und Vergütung von Aufwand in Zusammenhang mit Zertifizierungsprozessen
- 4.1.9. Technische und organisatorische Massnahmen zur *Vermeidung und Erkennung* allfälliger Geheimnis- und Datenschutzverletzungen (z.B. Trennung der Daten verschiedener Kunden, Beschränkungen und automatische Protokollierung der Zugriffe)
- 4.1.10. *Verbot der Verlagerung der Leistungserbringung ins Ausland oder auf Subunternehmer* ohne vorgängige schriftliche Zustimmung der Anwaltskanzlei
- 4.1.11. Besondere Massnahmen zum Schutz von Daten, welche *den Anwaltsgeheimnis sowie allfälligen weiteren spezialgesetzlichen oder besonderen vertraglichen Geheimhaltungspflichten* unterstehen
- 4.1.12. *Sofortige Informationspflichten des Providers gegenüber* der Anwaltskanzlei für den Fall bestimmter Incidents, insbesondere Verstössen gegen Geheimhaltungs-, Datenschutz- oder Informationssicherheitspflichten (siehe auch Ziff. 2.3.3)
- 4.1.13. Regelungen über rechtlich zulässige Information der Anwaltskanzlei wenn Strafverfolgungsbehörden und andere *staatliche Stellen Informationen* verlangt oder erhalten haben; Verpflichtung des Providers zur Ausschöpfung von Rechtsbehelfen und Einreden (auch gestützt auf das Anwaltsgeheimnis) gegenüber staatlichen Herausgabebegehren; Erklärung des Providers, auf freiwillige Datenherausgabe oder freiwillige Erteilung von Zugriffsrechten auf Daten gegenüber staatlichen Organen zu verzichten
- 4.1.14. *Folgen* von Geheimnis- und Datenschutzverletzungen (z.B. Informationspflichten, Konventionalstrafen, ausserordentliche Kündigungsrechte)

- 4.2. Informationssicherheit
 - 4.2.1. Anwendbare *Sicherheitsstandards*, Zertifizierungen
 - 4.2.2. *Sicherheitskonzept*; Beschreibung des Prozesses und der Verantwortlichkeiten bei der Erstellung und Aktualisierung des Informationssicherheits- und Datenschutzkonzepts
 - 4.2.3. Beschreibung der *Prozesse, Rollen und Verantwortlichkeiten* (Bestandteil des Sicherheitskonzepts)
 - 4.2.4. *Beschreibung der Sicherheitsarchitektur* (Trennung von Entwicklungs-, Test- und Produktionssystemen, Systemredundanzen, Firewalls, Intrusion Detection Systeme etc.)
 - 4.2.5. Beschreibung von *Verschlüsselungsmethoden* und Schlüsselmanagement für Speichermedien und für den Datenverkehr zwischen Anwaltskanzlei und Provider
 - 4.2.6. Detaillierte Beschreibung der *Authentifizierungsprozesse* zur Nutzung des Services und der Benutzerverwaltung; Auditierbarkeit von Login-Vorgängen etc.
 - 4.2.7. *Logging*: Definition, welche Zugriffe auf Daten und Systeme in Logfiles aufgezeichnet werden, wie und durch wen diese ausgewertet werden können
 - 4.2.8. *Risiko- und Katastrophenvorsorge* (z.B. redundante Anbindung an Internet, Stromversorgung etc.); Beschreibung der Prozesse und der Service Levels für Back-Up und Recovery
 - 4.2.9. Rechte und Pflichten des Providers bei massiven Sicherheitsproblemen oder im *Katastrophenfall*: Wann darf und muss der Provider selber kurzfristig welche Massnahmen treffen (mit oder ohne Einbezug der Anwaltskanzlei)?
 - 4.2.10. Beschreibung der *Security-Checks*, die beim Provider durchgeführt werden (Audits, Penetration Tests etc.) und Wahrung der Geheimhaltungspflichten bei deren Durchführung
- 4.3. Datensicherung, Archivierung und Datenlöschung
 - 4.3.1. Umfang, Art und Frequenz der *Datensicherung*
 - 4.3.2. Compliance mit Vorschriften zur Beweissicherung und Archivierung bestimmter Daten (z.B. Anwaltsrecht, Steuerrecht, Buchführungsrecht, Sozialversicherungsrecht); Definition der betroffenen Prozesse und Daten, Art, Umfang und Dauer der *Archivierung*, Rückübermittlungsprozess an die Anwaltskanzlei, Prüfungs- und Kontrollrechte

- 4.3.3. *Aufbewahrung von Sicherungsmedien* (räumliche Trennung, Kennzeichnung, Verschlüsselung der Sicherungen, Zugriffsmöglichkeiten der Anwaltskanzlei etc.)
- 4.3.4. *Verwertungsverbot* und Verzicht auf allfällige Retentionsrechte an Daten der Anwaltskanzlei (insbesondere für den Fall eines Zahlungsverzuges der Anwaltskanzlei oder der Insolvenz des Providers)
- 4.3.5. *Verfahren der Datenlöschung*
- 4.4. **Audit und Kontrollrechte**
 - 4.4.1. *Audit- und Kontrollrechte* beim Provider und seinen Subunternehmern
 - 4.4.2. *Mitwirkungspflichten des Providers* bei Audits und Kontrollen
 - 4.4.3. Beizug von *Drittexperten* zur Durchführung der Audits und Kontrollen im Auftrag der Anwaltskanzlei (insbesondere Verfahren zu deren Bestimmung)
 - 4.4.4. *Eigene Auditierungspflichten des Providers* (z.B. im Rahmen von Zertifizierungen oder behördlichen Kontrollen); Welche Informationen daraus werden der Anwaltskanzlei zur Verfügung gestellt?
 - 4.4.5. Einbindung in ein allfälliges *Interne Kontrollsystem* der Anwaltskanzlei
 - 4.4.6. Kontrollrechte von *Aufsichtsbehörden der Anwaltskanzlei* (z.B. Anwaltsaufsichtsbehörde, ESTV, EDÖB) beim Provider und seinen Subunternehmern
 - 4.4.7. Tragung von *Kosten und Aufwand* in Zusammenhang mit Audits und Kontrollen

5. Gewährleistung und Haftung

- 5.1. Abgrenzung der Risikosphären zwischen Anwaltskanzlei und Provider sowie Dritten (z.B. Zugangs Providern)
- 5.2. Haftung
 - 5.2.1. Beweis und Berechnung von Schäden
 - 5.2.2. Bedeutung des Verschuldens im Hinblick auf Haftungsansprüche
 - 5.2.3. Haftungsausschlüsse
 - 5.2.4. Verhältnis zu allfälligen Konventionalstrafen
 - 5.2.5. Verjährungsfristen

- 5.3. Rechtsgewährleistung
- 5.4. Versicherung von Risiken durch den Provider

6. Vertragsdauer und Vertragsbeendigung

- 6.1. Vertragsdauer
 - 6.1.1. *Inkrafttreten* des Vertrages
 - 6.1.2. *Vertragsdauer*
- 6.2. Ordentliche Kündigungsmöglichkeiten
 - 6.2.1. Kündigungsfristen
 - 6.2.2. Kündigungstermine
 - 6.2.3. Form
- 6.3. Ausserordentliche Vertragsauflösungsmöglichkeiten
 - 6.3.1. Ausserordentliche Vertragsauflösungsgründe
 - 6.3.2. Kündigungsfristen
 - 6.3.3. Form
- 6.4. Folgen der Vertragsauflösung
 - 6.4.1. *Vergütung* (Berechnung für angebrochene Perioden *pro rata temporis*)
 - 6.4.2. Schutz der Daten der Anwaltskanzlei und der Verfügbarkeit der Anwendungen bei *Insolvenz des Providers* (z.B. Kennzeichnung von Datenträgern im Hinblick auf eine Aussonderung, Verwertungsverbot für Daten, Herausgabe von Datensicherungen und Dokumentationen, Escrow des Sourcecodes von Software)
 - 6.4.3. Beschreibung der *Prozesse bei Vertragsbeendigung* (z.B. Zugangsbeendigung, Auslieferung und Löschung von Daten, Übergabe elektronischer Schlüssel, Abrechnungsmodalitäten)
- 6.5. Backsourcing
 - 6.5.1. *Unterstützungspflichten* des Providers (z.B. Datenmigration)
 - 6.5.2. *Planung des Vorgehens* (Backsourcingkonzept, Datenmigration, Verantwortlichkeiten etc.)
 - 6.5.3. *Lieferung* von Daten, Dokumentationen, Schnittstelleinformationen, Parametrisierungsinformationen, virtuelle Maschinen etc.

- 6.5.4. *Konditionen einer Weiterführung der Services* während einer Übergangsphase
- 6.5.5. *Vergütung* von Unterstützungsleistungen

7. Weitere Bestimmungen

- 7.1. Recht und Gerichtsstand
 - 7.1.1. Anwendbares Recht
 - 7.1.2. Gerichtsstand, eventuell vertragliches Konflikteskalationsverfahren / alternatives Streitbeilegungsverfahren
- 7.2. Schlussbestimmungen
 - 7.2.1. *Rechtsnachfolge*, eventuell grundsätzliche Zustimmung zur Übertragung des Vertrages unter Vorbehalt bestimmter Ablehnungsgründe → Ablehnungsverfahren definieren
 - 7.2.2. *Offenlegung*: Recht der Anwaltskanzlei, die Bedingungen des Vertrages gegenüber ihren Aufsichtsbehörden und dem EDÖB offen zu legen
 - 7.2.3. *Schriftform/Formvorbehalte*
 - 7.2.4. *Unterschriften* → darauf achten, dass die Unterzeichnenden unterschriftsberechtigt sind (z.B. aktuellen Handelsregisterauszug als Anhang aufnehmen)

WOLFGANG STRAUB, Dr. iur., LL.M., Fürsprecher, ist Rechtsanwalt in Bern und Lehrbeauftragter am CAS ICT Beschaffungen der Universität Bern

Die vorliegende Checkliste ist aus der Diskussion mit zahlreichen Kolleginnen und Kollegen heraus entstanden. Für wertvolle Anregungen und Hinweise danke ich namentlich CHRISTIAN LAUX und PETER NEUENSCHWANDER.