

Dr. Wolfgang Straub
Advokaturbüro Deutsch & Wyss
Postfach 5860
3001 Bern

wolfgang.straub@advobern.ch

Checkliste zum Vertragsaufbau für Sicherheits-Outsourcingverträge

Diese Checkliste erhebt keinerlei Anspruch auf Vollständigkeit und kann eine individuelle Analyse der zu regelnden Punkte nicht ersetzen. Besondere Aufmerksamkeit sind der Definition der zu erbringenden Leistungen (in der Regeln in einem Service Level Agreement als Anhang des Rahmenvertrages) und den Beendigungsmodalitäten zu widmen.

In der Schweiz gibt es bisher kaum Fachliteratur zu rechtlichen Aspekten von Managed Security Services bzw. des Outsourcing von Sicherheitsaufgaben. Einige Fragen stellen sich in ähnlicher Weise auch bei einem umfassenden IT-Outsourcing.

- Eine Übersicht über weiterführende Literatur zum Outsourcing ist verfügbar unter <http://www.advobern.ch/files/literaturhinweise01.pdf>
- Eine Checkliste zu Outsourcingverträgen im allgemeinen kann bei Swiss ICT bestellt werden: <http://www.swissict.ch/publi/bestellformular.php>
- Checklisten zum Controlling von Outsourcingverträgen verschiedener Art sind verfügbar unter http://www.isaca.ch/files/titel_d_bs.doc
- Zu den datenschutzrechtlichen Anforderungen an Outsourcing-Verträge gibt es eine Checkliste des Datenschutzbeauftragten des Kantons Zürich unter http://www.datenschutz.ch/checklisten_outsourcing.pdf

1. Einleitung

- 1.1. Genaue Bezeichnung der **Vertragsparteien** (in Konzernverhältnissen eventuell Bezeichnung der federführenden Konzerngesellschaft und Möglichkeit des Beitrittes weiterer Konzerngesellschaften → Verfahren definieren)
- 1.2. Definition des **Vertragszwecks**
- 1.3. **Struktur und Organisation** des Projekts
- 1.4. Eventuell **Begriffsdefinitionen** oder Referenzieren eines Glossars
- 1.5. Verhältnis zu allfälligen **verbundenen Verträgen**
- 1.6. Allenfalls Referenzieren von **eingereichten Unterlagen**, welche sich auf die Erfahrung des Dienstleisters beziehen (→ Haftungsmaßstab)

2. Übertragung der Betriebsverantwortung von sicherheitsrelevanten Teilen des Informationssystems des Kunden auf den Dienstleister

- 2.1. Eventuell Übertragung von **Systemen und Infrastruktur**
 - 2.1.1. Einräumung von **Eigentums- oder Nutzungsrechten**
 - 2.1.2. **Zeitpunkt** des Übergangs von Nutzen und Gefahr
 - 2.1.3. **Gewährleistung** des Kunden für übertragene Gegenstände
 - 2.1.4. **Rückkaufsoption** des Kunden für den Fall des Backsourcing (vgl. auch Ziff. 9.5.5)
- 2.2. Eventuell Übertragung von **Verträgen mit Dritten** auf den Dienstleister (z.B. Lizenz- und Wartungsverträge) → Zustimmung der Vertragspartner sicherstellen!
- 2.3. Eventuell Übernahme von **Personal** des Kunden durch den Dienstleister
- 2.4. Eventuell Nutzung von **Infrastruktur** und Zugang zu Betriebsräumlichkeiten des Kunden

2.5. Immaterialgüterrechte

- 2.5.1. Erteilung von Gebrauchslizenzen an Software des **Dienstleisters** (bei der Verwendung von Software von Drittherstellern muss vorgängig deren Zustimmung sichergestellt werden)
- 2.5.2. Zuweisung der Rechte an allfälligen im Rahmen des Vertrags geschaffenen **Immaterialgüterrechten** und Arbeitsergebnissen
- 2.6. Eventuell besondere Regeln für die **Transitionsphase** (schrittweise Übertragung der Betriebsverantwortung vom Kunden auf den Dienstleister), z.B. Testphase, Abnahmeverfahren

3. Definition der zu erbringenden Leistungen

- 3.1. **Prämissen** der Leistungserbringung, insbesondere technische und organisatorische Voraussetzungen
- 3.2. Zugrunde liegendes **Sicherheitskonzept**. Sofern dieses noch nicht vorliegt, ist allenfalls das Verfahren zu seiner Erarbeitung näher zu regeln. Das Sicherheitskonzept sollte insbesondere folgende Themen umfassen:
 - 3.2.1. Klassierung von Daten/Anwendungen nach **Schutzniveaus**
 - 3.2.2. **Zugriffsberechtigungen**, physischer und technischer Schutz vor unerwünschten logischen Zugriffen
 - 3.2.3. Verantwortung für **Datensicherung**
 - 3.2.4. Notfallplanung zu Aufrechterhaltung und Wiederanlauf des Betriebs bei Systemausfällen oder bei Datenverlust (**Disaster Recovery Management** beim Kunden und beim Dienstleister)
 - 3.2.5. **Dokumentation** der Sicherheitsmassnahmen und aller sicherheitsrelevanter Vorkommnisse
 - 3.2.6. Art und Weise der **Überprüfung** der Informationssicherheit (z.B. Auditing und Penetration Tests durch unabhängige Dritte)
 - 3.2.7. Verfahren zur **Aktualisierung** des Sicherheitskonzepts
- 3.3. **Datenschutzkonzept** sofern der Dienstleister im Rahmen des Vertragsverhältnisses Einblick in personenbezogene Daten erhalten kann

(z.B. auch Daten über Mitarbeiter des Kunden). Das Datenschutzkonzept sollte insbesondere folgende Themen umfassen:

- 3.3.1. **Datenherrschaft**, Weisungsrecht des Kunden, Zweckbindung
- 3.3.2. Technische und organisatorische Massnahmen zur **Vermeidung und Erkennung** allfälliger Datenschutzverletzungen (z.B. Beschränkungen und automatische Protokollierung der Zugriffe)
- 3.3.3. Eventuell besondere Massnahmen zum Schutz von Daten, welche **spezialgesetzlichen oder vertraglichen Geheimhaltungspflichten** unterstehen.
- 3.3.4. **Kontrollrechte** des Kunden
- 3.3.5. **Folgen** von Datenschutzverletzungen (z.B. Konventionalstrafen, ausserordentliches Kündigungsrecht)
- 3.3.6. **Geheimhaltungspflicht** des Dienstleisters und Pflicht zur Überbindung auf diejenigen Arbeitnehmer, welche Einblick in die Daten des Kunden erhalten
- 3.3.7. Zustimmung des Kunden vor dem **Beizug von Dritten** zu Aufgaben, bei welchen Möglichkeit zum Dateneinblick besteht
- 3.3.8. Zustimmung des Kunden vor einer allfälligen **Verlagerung der Leistungserbringung ins Ausland**
- 3.3.9. Schutzmassnahmen gegen **Vermischung**/Zugriff durch andere Kunden des Dienstleisters
- 3.4. **Spezifikation aller zu erbringenden Dienstleistungen in einem Service Level Agreement**, eventuell Definition unterschiedlicher Sicherheitsniveaus für verschiedene Teile des Informationssystems des Kunden, eventuell Verfügbarkeits- und Performancegarantien → Definition des relevanten Zeitraums und der Ausnahmen (Batchzeiten, Wartungsfenster etc.), Messkriterien
- 3.5. Einhaltung von **Standards**
- 3.6. **Support Levels** und Eskalation

- 3.7. Eventuell **Sicherheitsschulung** der Mitarbeiter des Kunden und **Einweisung in den Gebrauch** neuer Komponenten der Sicherheitsarchitektur
- 3.8. **Skalierbarkeit** des Umfangs der Dienstleistungen (z.B. Definition von ‚Warenkörben‘ mit unterschiedlichen Realisierungszeiten)
- 3.9. **Ort** der Leistungserbringung → Auswirkungen bei Veränderungen des Kundenstandorts definieren

4. Neben- und Mitwirkungspflichten

- 4.1. Kompetenzverteilung für **Systemadministrationsaufgaben**, z.B. Zuständigkeit für Konfigurationsänderungen, Konfliktlösung beim Patch Management, Berechtigung zur Abschaltung von Diensten im Notfall
- 4.2. **Koordination** mit externen Leistungserbringern (weitere IT-Dienstleister, Hard- und Softwarelieferanten)
- 4.3. **Mitwirkungs- und Informationspflichten**, z.B. Benachrichtigungsverfahren bei Sicherheitsrisiken, welche für den Kunden nicht ohne weiteres erkennbar sind, eventuell Mitwirkung bei Entwicklung / Einführung neuer sicherheitsrelevanter Anwendungen des Kunden
- 4.4. **Form** des Abrufs und der Abmahnung von Mitwirkungspflichten
- 4.5. **Geheimhaltung** (vgl. dazu auch Ziff. 3.3.6) → Verpflichtung des Dienstleisters, eine Liste der Personen zu führen, welche Einblick in vertrauliche Informationen erhalten und die Geheimhaltungspflichten auf diese zu überbinden
- 4.6. Eventuell Recht zur Mitsprache hinsichtlich der vom Dienstleister in für den Kunden sensitiven Bereichen eingesetzten **Mitarbeiter**
- 4.7. Verbot der Abwerbung von Mitarbeitern des Dienstleisters durch den Kunden (**Anstellungsverzicht**) → Definition der betroffenen Mitarbeiterkategorien und Ausnahmen bei Aufgabe des Geschäftsbetriebs, Konkurs etc.

5. Vertragsdurchführung

- 5.1. Eventuell **Abnahmeverfahren** am Ende der Transitionsphase
 - 5.1.1. **Vorbereitungshandlungen** des Kunden
 - 5.1.2. **Mitwirkungspflichten** des Dienstleisters
 - 5.1.3. **Testmethoden**, Testdaten und Bewertungskriterien
 - 5.1.4. Gründe für **Abnahmeverweigerung** und Eskalationsprozedere bei Meinungsverschiedenheiten über deren Berechtigung
 - 5.1.5. **Folgen** der Abnahmeverweigerung (z.B. Recht zur ausserordentlichen Vertragsauflösung nach zweimaligem Scheitern der Abnahme)
 - 5.1.6. Vergütung von **Aufwand** in Zusammenhang mit dem Abnahmeverfahren
- 5.2. **Reporting und Controlling** (vgl. auch Ziff. 7.1)
 - 5.2.1. Inhalt, Form und Periodizität der **Berichterstattung** über sicherheits- und kostenrelevante Umstände
 - 5.2.2. Eventuell **Online-Tools** → Inhalte, Zugriff und Archivierung definieren
 - 5.2.3. **Kontrollrechte** des Bestellers, insbesondere Recht zur Überprüfung durch Dritte (vgl. auch Ziff. 3.3.4 und 7.1.4)
- 5.3. **Claim Management Verfahren** zum periodischen Leistungs-Review, zur Aktualisierung von Mitwirkungspflichten des Kunden und zur Konkretisierung von Unklarheiten in der Leistungsbeschreibung
- 5.4. **Change Management Verfahren** zur Anpassung der Vertragsleistungen an neue Vorgaben und zur Festlegung der Auswirkungen auf Kosten, Fristen etc.
- 5.5. **Eskalationsverfahren** für den Fall von Meinungsverschiedenheiten zwischen den Vertragsparteien (Verhältnis zu Ziff. 10.2 regeln)

6. Vergütung

- 6.1. Vergütungsarten, z.B.:
 - 6.1.1. **Pauschalpreise** für ein bestimmtes Leistungspaket → genaue Definition der umfassten Leistungen
 - 6.1.2. **Aufwandsabhängige** Leistungen
 - 6.1.3. **Nutzungsabhängige Gebühren** → genaue Definition der Messgrößen.
- 6.2. **Auslagen**, Spesen und Gebühren
- 6.3. Eventuell **Bonus / Malus-System**
- 6.4. Eventuell Regeln zur **Preisanpassung**, z.B.:
 - 6.4.1. Zeitlich **degressive Preise** für automatisierbare Leistungen
 - 6.4.2. **Indexierung** von aufwandsabhängigen Leistungen
 - 6.4.3. **Mengenrabatte** für skalierbare Leistungen (z.B. für entsprechend der Anzahl Arbeitsplätze festgesetzte Pauschalpreise)
 - 6.4.4. Eventuell periodisches **Benchmarking**
 - 6.4.5. Konsequenzen der **Erhöhung des Aufwands** durch unvorhergesehene Ereignisse
- 6.5. **Abrechnungs- und Zahlungsmodalitäten**
- 6.6. Folgen bei **Verzug des Kunden** (insbesondere Regelung der Zulässigkeit der Leistungseinstellung)

7. Vertragskonformität (Service Level Management)

- 7.1. **Monitoring** (vgl. auch Ziff. 5.1)
 - 7.1.1. **Messmethoden**
 - 7.1.2. **Tiefe** der zu erfassenden Informationen
 - 7.1.3. **Gewichtung** verschiedener Kriterien

- 7.1.4. Möglichkeit zur **externen Überprüfung** (vgl. auch Ziff. 3.3.4 und 5.2.3)
- 7.2. Eventuell **Boni** bei Übererfüllung und **Mali / Konventionalstrafen** bei nicht vertragsmässigen Leistungen
- 7.3. **Gewährleistung** (d.h. welche Leistungen erbringt der Dienstleister unentgeltlich, um einen durch ihn zu vertretenden Sicherheitsdefekt und dessen Folgen zu beheben)
- 7.4. **Ausserordentliches Kündigungsrecht** bei schwerwiegenden Vertragsverletzungen (vgl. auch Ziff. 9.3)
- 7.5. Zulässigkeit von Verrechnung und **Zurückbehaltung von Zahlungen**

8. Haftung für Schäden

- 8.1. Eventuell Regeln zur Abgrenzung der **Risikosphären** von Kunde und Dienstleister
- 8.2. Eventuell Regeln zur **Beweislastverteilung**
- 8.3. Eventuell Pauschalierung bestimmter **Schadenskategorien**
- 8.4. Eventuell **Haftungsausschlüsse** bzw. Haftungsbeschränkungen des Dienstleisters und des Kunden
- 8.5. Verhältnis zu allfälligen **Konventionalstrafen**
- 8.6. Eventuell **Versicherung** gewisser Risiken durch den Dienstleister

9. Vertragsbeendigung

- 9.1. Eventuell **Befristung** mit Möglichkeit zur stillschweigenden Verlängerung
- 9.2. **Ordentliche Kündigung** (z.B. jährlich, eventuell erst nach einer bestimmten Mindestvertragsdauer)
 - 9.2.1. **Kündigungsfristen** (z.B. sechs Monate im Voraus)
 - 9.2.2. **Kündigungstermine** (z.B. auf Ende eines Kalenderjahres)
 - 9.2.3. **Form** (z.B. eingeschriebener Brief)

- 9.3. **Ausserordentliche Vertragsauflösung** in Fällen, in welchen eine weitere Zusammenarbeit nicht mehr zumutbar ist
- 9.4. Eventuell **Option** zur vorzeitigen Vertragsauflösung zu einem zum Voraus bestimmbar Preis
- 9.5. **Folgen** der Vertragsauflösung / **Backsourcing**
 - 9.5.1. **Vergütung**, z.B. Berechnung für angebrochene Perioden *pro rata temporis*, eventuell Verpflichtung zur Übernahme von noch nicht amortisierter kundenspezifischer Hard- und Software (vgl. auch Ziff. 9.5.5)
 - 9.5.2. Falls **Beendigung einzelner Vertragsteile** möglich ist: Auswirkung auf den Rest des Vertrages definieren
 - 9.5.3. **Geheimhaltungs-** und Vernichtungspflichten
 - 9.5.4. **Unterstützungspflichten des Dienstleisters** beim Backsourcing → Konkretisierung im Rahmen eines Claim Management Verfahrens (vgl. Ziff. 5.3)
 - 9.5.5. Eventuell **Ansprüche** auf Herausgabe von Dokumentationen, individuell entwickelten Tools etc.
 - 9.5.6. Eventuell **Kaufrechte** für Hardware, Software und Infrastruktur → Festlegung der Bewertungsgrundlagen
 - 9.5.7. Eventuell Recht zur **Übernahme von Arbeitnehmern** des Dienstleisters in bestimmten Fällen
 - 9.5.8. Verteilung der **Backsourcingkosten**

10. Schlussbestimmungen

- 10.1. **Anwendbares Recht**, falls es sich um ein grenzüberschreitendes Verhältnis handelt
- 10.2. **Gerichtsstand**, eventuell alternatives Streitbeilegungsverfahren
- 10.3. Abschliessendes Verzeichnis aller **Anhänge** des Vertrages und Verhältnis der einzelnen Vertragsdokumente zueinander

- 10.4. **Vollständigkeitsklausel** (es bestehen keine mündlichen Nebenabreden)
- 10.5. **Form** von Vertragsänderungen und Erklärungen an die Gegenpartei, welche die Rechtslage gestalten
- 10.6. Mitteilungsmodalitäten für Änderungen von **Korrespondenzadressen und Ansprechpartnern**
- 10.7. **Rechtsnachfolge**, eventuell grundsätzliche Zustimmung zur Übertragung des Vertrages unter Vorbehalt bestimmter Ablehnungsgründe → Ablehnungsverfahren definieren.
- 10.8. Berechtigung des Dienstleisters, das Projekt als **Referenz** zu verwenden, Modalitäten der Referenzerteilung
- 10.9. **Unterschriften** → darauf achten, dass alle Unterzeichnenden unterschriftsberechtigt sind (aktuellen Handelsregisterauszug als Anhang aufnehmen)