datenschutzbeauftragter
kanton zürich

Checklisten für Outsourcing-Verträge

Datenschutzbeauftragter des Kantons Zürich
Kaspar Escher-Haus
8090 Zürich

E-Mail: datenschutz@dsb.zh.ch
Homepage: http://www.datenschutz.ch

Zürich, 02. Dezember 2005

Version 1.1

datenschutzbeauftragter kanton zürich

Inhaltsverzeichnis

datenschutzbeauftragter
kanton zürich

Einleitung

Öffentliche Organe ziehen in vielen Geschäftsbereichen oder bei einzelnen Tätigkeiten Dritte als Dienstleistungserbringer bei oder lagern gar ganze Bereiche aus (Outsourcing). Die Bandbreite reicht von der einfachen Adressierung für ein Mailing bis zum umfassenden Outsourcing der Informatik.

Das Vertragswerk ist insbesondere bei ausgelagerten Bereichen die zentrale und häufig einzige Steuerungsfunktion, die dem öffentlichen Organ verbleibt. Dabei ist zu berücksichtigen, dass für ein Outsourcing oder die Auslagerung einzelner wichtiger Tätigkeiten und Bereiche in der Regel ein strategischer Entscheid zu fällen ist, da eine solche Auslagerung nur mit grossen Aufwendungen rückgängig gemacht werden kann. Deshalb sind die Verträge mit der entsprechenden Sorgfalt zu erarbeiten.

Die folgenden Checklisten sind Hilfestellungen für den Abschluss und die Kontrolle von Verträgen mit Dienstleistungserbringern. Sie erheben keinen Anspruch auf Vollständigkeit, sondern fokussieren die für die Geheimhaltung, den Datenschutz und die Informationssicherheit zentralen Aspekte.

Die „Checklisten für Outsourcing-Verträge“ richten sich an alle öffentlichen Organe des Kantons Zürich. Sie stellen Hilfsmittel dar, damit die verantwortlichen Organe die Anforderungen an die Geheimhaltung, den Datenschutz und die Informationssicherheit auch bei der Auslagerung einzelner Geschäftstätigkeiten oder –bereiche bzw. beim Beizug Dritter erfüllen können. Weiter richten sich die Checklisten auch an die Vertragspartner, die für öffentliche Organe des Kantons Zürich Dienstleistungen erbringen.

Die Verwendung durch andere Stellen und Institutionen ist möglich. Zu beachten ist dabei, dass die Checklisten auf die Rechtslage im Kanton Zürich ausgerichtet sind, insbesondere was die Quellen und Verweisungen anbelangt.

1. Checkliste Klärung des Umfelds[1]

Folgende Voraussetzungen und Aufgaben sind beim Outsourcing bzw. Beizug Dritter für Datenbearbeitungen in einem ersten Schritt zu klären:

Die **auszulagernden Geschäftsbereiche bzw. Tätigkeiten** sind zu **definieren**.

Der **Leistungserbringer** ist **sorgfältig auszuwählen**, zu **instruieren** und zu **kontrollieren**.

Die **Verantwortung bleibt** auch für die ausgelagerten Bereiche bzw. Tätigkeiten bei der Behörde, Amtsstelle, Gemeinde bzw. öffentlichrechtlichen Institution.

Das öffentliche Organ hat die **Sicherheitsanforderungen** zu **erarbeiten**. Dazu ist eine Risikobeurteilung vorzunehmen und es sind die Schutzziele festzulegen. Die Massnahmenpläne sind zusammen mit dem Leistungserbringer zu erarbeiten.[2]

Die **staatliche Aufgabenerfüllung** muss auch im Falle eines Vertragsbruches oder der Einstellung der Geschäftstätigkeit des Leistungserbringers **sichergestellt** sein.

Die **gesetzlichen Geheimhaltungspflichten** sind zu **wahren**.[3]

Die betroffenen Personen sind über das Outsourcing bzw. den Beizug Dritter zu **informieren**.

Der **Leistungserbringer** ist **periodisch** zu **kontrollieren**, und die **gesetzliche Revision und Aufsicht** ist **sicherzustellen**.

Mit dem Leistungserbringer sind **schriftliche Verträge** zu schliessen.[4]

---

[1] Basierend auf dem Rundschreiben „Outsourcing“ der Eidgenössischen Bankenkommission.

[2] Siehe zum Vorgehen Ziffer 2 (Checkliste Vorgehen bezüglich Informationssicherheit).

[3] Siehe dazu § 3 des Gesetzes über die Auslagerung von Informatikdienstleistungen bzw. Ziffer 2.13 der „AGB Sicherheit“.

[4] Siehe dazu Ziffer 3 (Checkliste Verträge).

2. Checkliste Vorgehen bezüglich Informationssicherheit[5]

Bei der Auslagerung verbleibt die Verantwortung grundsätzlich beim öffentlichen Organ. In Bezug auf die Erarbeitung und Umsetzung einzelner Schritte ist es jedoch auf die Unterstützung durch den Leistungserbringer angewiesen. Es empfiehlt sich folgendes Vorgehen:

Der Leistungsbezüger (=öffentliches Organ) macht eine Ist-Aufnahme und **Risikoanalyse**.

Daraufhin wählt der **Leistungsbezüger** eine der drei **Sicherheitsstufen** auf Grund der Ergebnisse der Risikoanalyse.

Der Leistungsbezüger legt die **Schutzziele** fest. Er entscheidet, ob er dazu die Zusammenarbeit mit dem Leistungserbringer benötigt.

Die **Massnahmenpläne** sind durch die Vertragspartner (Leistungsbezüger und Leistungserbringer) **gemeinsam festzulegen**.

Die **Massnahmenpläne** sind vom Leistungsbezüger durch die vorgesetzte Direktion **genehmigen zu lassen**.

In den Verträgen ist eine **Regelung** über die **periodische Überarbeitung** zu treffen (Verantwortungen, Periodizität, Schnittstellen).

[5] Das Vorgehen entspricht den Vorgaben der Informatiksicherheitsverordnung des Kantons Zürich.

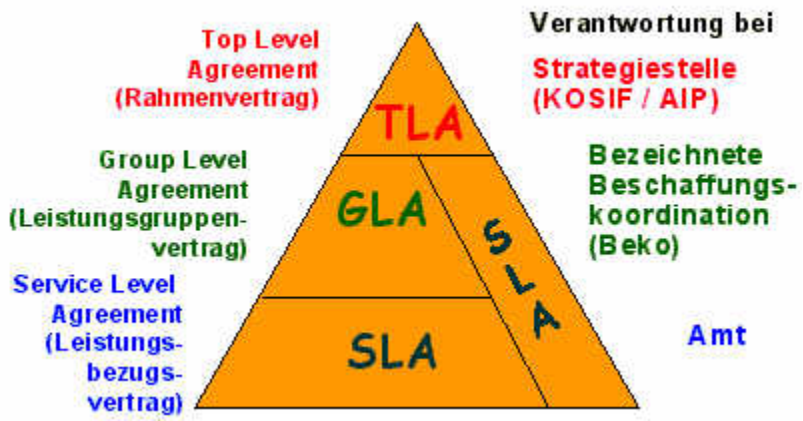
3. Checkliste Verträge[6]

3.1 Wahl des Vertragsmodells

Die Checkliste präjudiziert kein bestimmtes Vertragsmodell. Die einzelnen Punkte sind – je nach gewähltem Vertragsmodell – im „richtigen" Vertrag abzuhandeln.

Folgende Beispiele von Vertragsmodellen können empfohlen werden:

Beispiel Kanton Zürich (Auslagerung von Informatikdienstleistungen)



zusätzlich: „AGB Sicherheit" **Je nach Vertragsstufe**

(Abbildung aus Projekt „Avanti – Verträge"; http://web.aip.zh.ch [Intranet der Abteilung für Informatikplanung des Kantons Zürich], Status: in Arbeit; ergänzt um AGB Sicherheit)

[6] Basierend auf der „Outsourcing Contracts Control Review" der ISACA (Switzerland Chapter).

Beispiel ISACA Switzerland Chapter (Outsourcing Contracts Control Review)[7]

Teil 1: Rahmenvertrag über „Outsourced Domain"

ist ausgerichtet auf allgemeine Grundsätze, Vertragsbestimmungen und nimmt so zusätzlich Bezug auf rechtliche Aspekte

Teil 2: Leistungsbeschreibung über „Outsourced Domain"

nimmt vorwiegend Bezug auf „outsourced" Dienstleistungen/Prozesse

Teil 3: Sicherheit in der „Outsourced Domain"

nimmt vorwiegend Bezug auf die Informationssicherheit von „outsourced" Dienstleistungen/Prozesse

Teil 4: Revision der „Outsourced Domain"

ist ausgerichtet auf die Zusammenarbeit zwischen Leistungserbringer und Leistungsbezüger hinsichtlich Revision und nimmt so zusätzlich Bezug auf alle Teile eines Vertragswerkes

[7] Es handelt sich hierbei nicht um ein eigentliches Vertragsmodell, sondern um eine Checkliste zur „Opportunity and Risk Analysis für Outsourcing-Verträge" aus Sicht der Informatikrevision. Das Modell ist die Basis für die nachfolgende Checkliste (siehe Fussnote 6).

3.2 Vertragsinhalt

Die Verträge sollten grundsätzlich folgende Regelungen enthalten[8]:

Definitionen

Die wichtigen **Ausdrücke** sind ausformuliert und **definiert**.

[➔ AGB Sicherheit, Ziffer 1.2][9]

Vertragsmanagement

Der Leistungsbezüger bestimmt eine **verantwortliche Stelle** für die **Verwaltung und Pflege der eingegangenen Beziehung**.

Dieser Stelle **obliegt** insbesondere

- die **Führung von Vertragsverhandlungen** bei Veränderungen, Erneuerungen, Auflösungen des Dienstleistungsverhältnisses, Fusion, Übernahme, Konkurs oder Geschäftsaufgabe des Leistungserbringers,
- die **Festlegung von Prozessen und Regelungen für die Notfallvorsorge** einschliesslich Abstimmung derselben mit denjenigen des Leistungserbringers,
- die **Festlegung der Verantwortung der Vertragspartner für Sicherheitsbelange** (einschliesslich Umfang der Sicherheitsanforderungen sowie Überwachung und Kontrolle der Einhaltung).

Vertragsgegenstand

Die **Zielsetzung** und der **Umfang der vereinbarten Dienstleistung** sind **beschrieben**.

[➔ AGB Sicherheit, Ziffer 1.1 und 1.3]

Die **„Allgemeinen Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen**“ (September 2001) sind dem Leistungserbringer **überbunden**.

---

[8] Zur Erinnerung: Die Checklisten fokussieren Aspekte der Geheimhaltung, des Datenschutzes und der Informationssicherheit.

[9] Die Verweisungen auf die „AGB Sicherheit“ beziehen sich auf die „Allgemeinen Geschäftsbedingungen des Kantons Zürich über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen“ (September 2001).

Die **vereinbarten Dienstleistungen** sind **bezüglich Qualität und Quantität** klar **definiert und dokumentiert.**

Die **Auslagerung** oder Verschiebung der Dienstleistungen **in ein anderes Land** durch den Leistungserbringer ist **ausgeschlossen**.

[➔ AGB Sicherheit, Ziffer 2.8]

Die **Vertreter des Leistungsbezügers kennen die Anforderungen der Informationssicherheit** bei Veränderungen von Informatiksystemen und -anwendungen.

Sie werden bei solchen Veränderungen miteinbezogen.

[➔ AGB Sicherheit, Ziffer 2.1]

Die **organisatorischen Abläufe** der ausgelagerten Dienste oder Bereiche sind **definiert und dokumentiert**, insbesondere sind

die *Prozesse beschrieben*,

die *Schnittstellen* zwischen Leistungserbringer und Leistungsbezüger *definiert*,

Sicherheits-, Kontroll- und Überwachungsmassnahmen in den betroffenen Prozessen *implementiert* und

Notfallpläne (inkl. Informationsfluss und Entscheidungskompetenzen) *erstellt*.

<u>Vertragsdauer und -auflösung</u>

☐ **Beginn und Ende** sowie allfällige **Mindestdauer** des Vertrages ist **geregelt** und dokumentiert.

Bei langfristigen Vertragspartnerschaften ist eine **periodische Neuverhandlung vorgesehen** und deren Ablauf ist geregelt.

Der Vertrag ist unter Einhaltung einer der Dienstleistung **angemessenen Kündigungsfrist auflösbar**.

Zeitpunkt und Bedingungen hierfür sind **geregelt**.

☐ Eine **Vertragsauflösung** erfolgt **bei krassen Vertragsverletzungen**, insbesondere bei groben Verletzungen von Geheimhaltungs- und Sicherheitsanforderungen.

[➔ AGB Sicherheit, Ziffer 4]

Der **Leistungserbringer** wird verpflichtet, **alle** aus dem Dienstleistungsverhältnis erworbenen **Kenntnisse und Informationen** über den Leistungsbezüger auch nach der Vertragsauflö-

sung **vertraulich zu behandeln** sowie sämtliche **Daten und Unterlagen zurückzugeben** oder auf Verlangen des Leistungsbezügers zu vernichten.

[➔ AGB Sicherheit, Ziffer 2.9]

Fusion, Übernahme, Konkurs oder Geschäftsaufgabe des Leistungserbringers gefährden die gesetzlichen Aufgaben des Leistungsbezügers nicht.

Verantwortungen

Die **technischen und organisatorischen Schnittstellen** zwischen Leistungserbringer und Leistungsbezüger sind **klar definiert**.

Die **Verantwortungen für die Pflege der Schnittstellen** sind sowohl seitens des Leistungserbringers als auch seitens des Leistungsbezügers **geregelt**, insbesondere bezüglich Berichtswesen, Kontrolle und Überwachung, Sicherheitsmassnahmen und Notfallplanung.

Leistungsüberwachung und -kontrolle

Es existiert ein **laufender Überwachungs- und Kontrollprozess** zur Sicherstellung der Verfügbarkeit der vereinbarten Dienstleistungen.

Technologische Veränderungen mit Auswirkungen auf die Dienstleistungen **werden erkannt**, **insbesondere** auch hinsichtlich **Auswirkungen für die Informationssicherheit**.

Es **existiert ein Prozess zwischen Leistungserbringer und Leistungsbezüger** zur **Diskussion der Folgen** und **Festlegung allfälliger Massnahmen**.

[➔ AGB Sicherheit, Ziffern 2.1 und 3]

Berichtswesen

Der **Leistungserbringer informiert** den Leistungsbezüger schriftlich **über Veränderungen und Probleme in den Dienstleistungen**, insbesondere bei Veränderungen im Umfeld der Informationssicherheit.

[➔ AGB Sicherheit, Ziffer 2.1 und 2.6]

Der **Leistungsbezüger informiert** den Leistungserbringer periodisch **über Veränderungen von vertragsrelevanten Vorhaben und Daten**, insbesondere auch bei Veränderungen gesetzlicher Grundlagen oder Praxisänderungen.

[➔ AGB Sicherheit, Ziffern 1.3 und 2.2]

Archivierung

Die **Aufbewahrungsdauer** von Daten ist **durch den Leistungsbezüger spezifiziert** und berücksichtigt die gesetzlichen Anforderungen.

Der **Leistungserbringer stellt sicher**, dass **während dieser Dauer** die **Verfügbarkeit, Integrität und Authentizität der Daten** durch **gewährleistet** ist und die notwendigen Informatiksysteme und -anwendungen zur Verfügung stehen.

Es ist ein **Prozess definiert**, um die Daten **nach Ablauf der Aufbewahrungsdauer** nach den Anforderungen der Archivgesetzgebung **archivieren** zu können.

Haftung, Schadenersatz, Gerichtsstand und anwendbares Recht

Die **Verbindlichkeiten** von Leistungserbringer und Leistungsbezüger sind klar **definiert** und dokumentiert.

Es ist **geregelt**, **in welchen Fällen Schadenersatz oder Konventionalstrafe zu zahlen** ist und/oder der **Vertrag aufgelöst** werden kann.

[➔ AGB Sicherheit, Ziffer 4]

Es ist **geregelt**, **welches Gericht** (einschliesslich allfällige Schiedsgerichte und –verfahren) in Streitfällen anzurufen ist und **welches Recht** zur Anwendung kommt.

[➔ AGB Sicherheit, Ziffer 5]

Rechte und Pflichten

[➔ AGB Sicherheit (gesamt)]

Die **Rechte und Pflichten der Vertragspartner** sind **eindeutig geregelt**.

Die **massgebenden gesetzlichen Bestimmungen werden eingehalten**, insbesondere Datenschutzgesetz, Finanzkontrollgesetz, Archivgesetz, Gesetz über die Auslagerung von Informatikdienstleistungen sowie Informatiksicherheitsverordnung.

Es sind **Massnahmen getroffen**, um die **anwendbaren Geheimhaltungsvorschriften** (Amtsgeheimnis, Steuergeheimnis, Sozialversicherungsgeheimnisse, Berufsgeheimnisse usw.) **zu wahren**.

Der **Leistungserbringer wird verpflichtet**, alle aus dem Dienstleistungsverhältnis erworbenen **Kenntnisse und Informationen über den Leistungsbezüger vertraulich zu behandeln.**

Rahmenbedingungen des Datenschutzgesetzes

- Der **Leistungserbringer** ist **verantwortlich** für einen **angemessenen Schutz der ihm anvertrauten Daten**.[10]

- Die **Sicherheit der Daten und Informationen** des Leistungsbezügers sowie der damit verbundenen Informatiksysteme und -anwendungen ist **gewährleistet** und **vertraglich geregelt.**
  [➔ AGB Sicherheit (gesamt)]

- Der **Leistungserbringer richtet seine Prozesse so** aus, dass er die **Anforderungen des Datenschutzgesetzes des Kantons Zürich einhalten kann**, wenn er Dienstleistungen für öffentliche Organe des Kantons Zürich erbringt.

Der **Leistungsbezüger** zeichnet **verantwortlich für die Durchsetzung von § 13 des Datenschutzgesetzes (Datenbearbeitung durch Dritte) sowie des Gesetzes über die Auslagerung von Informatikdienstleistungen beim Leistungserbringer**.

Die **Anforderungen** an den Datenschutz beim Leistungsbezüger sind **bekannt**, liegen schriftlich vor und sind **genehmigt**.

Der **Zugriff** zu ausgelagerten Datenbeständen und insbesondere zu Datenbeständen mit besonders schützenswerten Personendaten und Daten, die im Interesse des Staates einer besonderen Geheimhaltung unterliegen, ist **konsistent zu regeln und zu dokumentieren**.

Es bestehen **Verfahren zur Gewährleistung der datenschutzrechtlichen Ansprüche** auf Auskunft, Berichtigung und Vernichtung.

[10] Insbesondere sind die Daten gegen unbefugte oder zufällige Zerstörung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl oder widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, unbefugte Kenntnisnahme oder andere unbefugte Bearbeitungen zu schützen.

Die **Verantwortlichkeiten und Schnittstellen** seitens des Leistungsbezügers und des Leistungserbringers sind **definiert** und **dokumentiert**.

Die **Eigentümer der Daten** sind **benannt** und deren Namen sind jederzeit aktuell (Verantwortung).

☐ **Inhalt und Ort der Datenbestände** des Leistungsbezügers sind aktuell **dokumentiert**.

☐ **Vertraulichkeitsklassierungen, Verfügbarkeits- und Integritätsanforderungen** der Datenbestände sind **spezifiziert**.

Die **Daten** werden nur **zur Erfüllung der vertraglich vereinbarten Dienstleistung genutzt** (Zweckbindung).

☐ **Bekanntgabe, Verkauf, Vermietung der Daten oder anderweitige Verwendung** derselben durch Drittparteien oder die kommerzielle Verwendung im Namen des Leistungserbringers sind **verboten**.

☐ Der **Leistungserbringer stellt die Einhaltung von vertraglich vereinbarten Anforderungen an die Datenverwaltung und Datennutzung sicher**.

Sicherheits-Policy

Anforderungen an die Sicherheit sind durch eine **aktuelle Sicherheits-Policy** für beide Vertragsparteien verbindlich geregelt.

Die **Sicherheits-Policy** richtet sich **nach anerkannten Standards**.[11]

☐ **Aktualisierungen** der Policy erfolgen **in Übereinstimmung von beiden Vertragspartnern** und werden rechtsgültig unterzeichnet.

☐ In der Policy ist **festgelegt**, welche **Sicherheitsanforderungen** durch die Vertragspartner verbindlich eingehalten werden müssen.

[11] Für Informatik sind dies z.B. CobiT (Control Objectives for Information and related Technology]) 'Code of Practice for Information Security Management' der 'British Standards Institution' (BS7799) oder IT-Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Bonn. Der Kanton Zürich hat den letztgenannten Standard gewählt.

- Die jeweiligen **Anforderungen/Direktiven/Weisungen für beide Vertragspartner** liegen **schriftlich** vor.

- Das **Verfahren** für die **Behandlung** sowohl von **Sicherheitsverletzungen** als auch das **Eskalationsverfahren** für solche Fälle sind **spezifiziert**.

- Der Leistungsbezüger und der Leistungserbringer führen eine **zentrale Aufzeichnung** mit allen die Informationssicherheit betreffenden Vorkommnissen, wie Zugriffsverletzungen, Manipulationen, Beweismittel für Betrugsfälle, Hacking etc.
- Diese **Aufzeichnung** ist **Basis für die Festlegung der Zusammenarbeit bei Verletzungen** der Informationssicherheit und der **Einführung** von entsprechenden **neuen Kontrollen und Verfahren**.

Personal

Die bei der Anstellung von neuem Personal durchgeführten **Personalrekrutierungen** beim Leistungserbringer sind **konsistent zu den Anforderungen an die Informationssicherheit** beim Leistungsbezüger.

Der **Leistungserbringer verpflichtet** sein **Personal** schriftlich zur **Einhaltung** der gesetzlichen und vertraglichen **Geheimhaltungs- und Sicherheitsbestimmungen.**

[➔ AGB Sicherheit, Ziffer 2.4]

- Bei **Datenbearbeitungen, die besonders schützenswerte Daten oder Daten betreffen, die im Interesse des Staates einer besonderen Geheimhaltungspflicht unterliegen**, schliesst der Leistungserbringer durch organisatorische und technische Massnahmen aus, dass sein Personal Einsicht in die Daten nehmen kann.
- Ist dies nicht möglich, stellt er die **Einbindung** des Personals in die **funktionelle Hierarchie** des Leistungsbezügers sicher.[12]

[➔ AGB Sicherheit, Ziffer 2.13]

[12] Folgende Massnahmen sind zu treffen: (1) Das Personal untersteht dem direkten fachlichen Weisungsrecht des Leistungsbezügers. (2) Sämtliche Systemeingriffe sind revisionssicher protokolliert. (3) Dem Leistungsbezüger werden Namen und Einsatzbereiche der betreffenden Mitarbeitenden mitgeteilt (inkl. Mutationen). (4) Der Leistungsbezüger hat ein Vetorecht bezüglich Personaleinsatz.

Notfall-Vorsorge

- Der **Leistungserbringer** unterhält einen **aktuellen Notfallvorsorgeplan**.
- Die darin eingebundenen **Verfahren** werden **periodisch** auf Aktualität und Angemessenheit **überprüft** und getestet.

- Beim **Leistungserbringer** sind **Prozeduren und Regelungen** implementiert, die in einem Notfall dem Leistungsbezüger die **Verfügbarkeit** der vertraglich vereinbarten Service-Leistung **garantieren**.[13]

- Im Rahmen der Notfallvorsorge **ausgelagerte Daten, Programme und Dokumentationen unterstehen** den zwischen den beiden Vertragspartnern vereinbarten **Geheimhaltungspflichten**.

- Das **Recht zur Einsichtnahme** in die aktuelle **Notfallvorsorgedokumentation** sowie in **Resultate periodischer Tests** der Wiederanlaufverfahren ist, soweit sie Elemente der vertraglich vereinbarten Service-Leistung betreffen, geregelt.

- Mit der Unterzeichnung des Rahmenvertrages wird der **Leistungserbringer verpflichtet**, in einem **Notfall gemäss den im Notfallvorsorgeplan dokumentierten Verfahren**, soweit sie Elemente der vertraglich vereinbarten Service-Leistung betreffen, zu **handeln**.

- Beim **Leistungsbezüger** sind **Prozeduren und Regelungen** implementiert, die in einem Notfall beim Leistungserbringer, die **Fortführung der üblichen Geschäftstätigkeit garantieren.**
- Diese Prozeduren und Regelungen sind **mit der Notfallvorsorge beim Leistungserbringer periodisch abgestimmt**; sie werden aktuell gehalten und periodisch getestet.

- Der **Leistungsbezüger** trifft **vorsorgliche Massnahmen** um einer **möglichen Vertragsauflösung vor Vertragsende zu begegnen**.[14]

[13] Prozeduren und Regelungen sind z.B. Alarmkonzepte, Hardware-Backup, Verfahren für die Sicherheits-Auslagerung von Daten, Applikations-Software, System-Software, Dokumentationen und anderer in einem Notfall benötigten Hilfsmittel (Backup's), Wiederanlaufverfahren bzw. Wiederanlaufplan zur Wiederherstellung des letzten produktiven Status vor Eintritt eines Vorkommnisses, Zugriffsregelung zu ausgelagerten Daten, Eskalationsverfahren zur verantwortlichen Stelle beim Leistungsnehmer inkl. Statusmeldungen an den Leistungsnehmer.

[14] Z.B. Erstellung eine Wiederanlaufplans, Archivieren aktueller Kopien von Applikations- und System-Software, Lizenzen und Dokumentationen oder Eigentumsrechte an solchen.

Logische Zugriffe

- Zur Sicherung der Ressourcen vor Schaden, Verlust oder Veränderungen durch unautorisierte Zugriffe sind **Zugriffskontrollen** installiert.
- Diese unterliegend einer **laufenden Überwachung**.

- Verantwortlich für die **Kontrolle der Zugriffssicherheit** zeichnet das Management des **Leistungsbezügers**.

- Adäquate **Richtlinien und Verfahren für die Administration von Zugriffsrechten sind definiert**, liegen schriftlich vor und sind durch den Leistungsbezüger **genehmigt**.[15]

- Alle **durch ihre Tätigkeit mit Zugriffen** auf Daten des Leistungsbezügers **betroffenen Personen** haben die genannten **Richtlinien unterzeichnet** und übernehmen damit direkt die **Verantwortung für jeden Zugriff mit ihrer Benutzer-Identifikation**.

- Die **Zugriffssicherheit** umfasst im Minimum die folgenden Anforderungen: **Anmeldung** (Sign-on) mit eindeutiger Benutzer-Identifikation, **Verifizierung** der Identität eines Benutzers (Authentisierung), **Aufzeichnung** (Logging) und **Auswertung** bzw. periodische Überprüfung sicherheitsrelevanter Informationen.

- Durch **automatisierte Zugriffseinschränkungen** soll das Risiko von potentiellen Verlusten durch bewussten oder unbewussten Missbrauch, Diebstahl, Betrug, Veruntreuung, Manipulation oder Zerstörung von Daten bzw. sensitiven Zugriffsinformationen reduziert werden.[16]

Physische Sicherheit

- Alle vom Leistungsbezüger **an die physische Sicherheit gestellten Anforderungen** werden vom Leistungserbringer an den davon betroffenen örtlichen Stellen **eingehalten**.

- Die **Anforderungen an die physische Sicherheit beim Leistungserbringer** erreichen im Minimum **denselben Gütegrad wie derjenige beim Leistungsbezüger**.

[15] Beispiele dazu sind: Policy und Verfahren der Zugriffsrechte, Administration der Zugriffsrechte, Standardisierung der Zugriffsrechte, Schutz der Zugriffskontrolldaten, wie: Benutzer-Identifikationen, Passwörter, Zugriffsregeln, spezifische Zugriffsprivilegien etc.

[16] Beispiele dazu sind: Automatischer Terminal Log-off, Access Control Software, Call-Back Verfahren.

- Die **Anforderungen an die physische Sicherheit** beim Leistungsbezüger sind **bekannt**, liegen schriftlich vor und sind vom Management **genehmigt**.

- Zum **Schutz der Ressourcen gegen unautorisierte Zutritte**, **unautorisierte physische Zugriffe** und vor **Schaden oder Verlust** sind **angemessene Sicherheitsmassnahmen** getroffen.

- **Verantwortlich** für die **periodische Kontrolle der Umsetzung der Sicherheitsmassnahmen** in wichtigen und schutzwürdigen Risikobereichen für Ressourcen zeichnet der **Leistungserbringer**.[17]

Revision und Aufsicht

- Der **Leistungsbezüger** sowie seine **Aufsichtsorgane** haben das **Recht zur Revision** beim Leistungserbringer.
  [➔ AGB Sicherheit, Ziffer 2.12]

- Die **internen und externen Revisionsstellen des Leistungserbringers** und die **Revisions- und Aufsichtsstellen des Leistungsbezügers** sind **bezeichnet**.

- Die mit der Revision **betrauten Personen** sind **fachlich ausgewiesen** bzw. haben fundierte Kenntnisse in Revisionsverfahren sowie eine ausgewiesene Fachkompetenz in der Bearbeitung von Revisionsaufgaben.

- Die **Durchführung einer periodischen Revision** beim Leistungserbringer ist durch beide Vertragspartner mit der Unterzeichnung des Rahmenvertrages **genehmigt**; die Periodizität ist festgelegt.

- Der **Leistungserbringer unterstützt Revisoren** bei der Erledigung des Revisionsauftrages.

[17] Wichtige und schutzwürdige Risikobereiche für Ressourcen umfassen insbesondere: Zugang zu Ressourcen, Physische Zugriffe auf jegliche Ressourcen, Daten, Datenfiles etc., Gebäude und Gebäudeumgebung, Brandschutz, Schutz vor Wasser, Klima- und Kühlungsanlagen, Stromversorgung.

4. Grundlagen und Quellen

Rechtsgrundlagen (Kanton Zürich)

Gesetz über die Auslagerung von Informatikdienstleitungen vom 23. August 1999 (LS 172.71)
Datenschutzgesetz vom 6. Juni 1993 (LS 236.1), insbesondere § 13
Datenschutzverordnung vom 7. Dezember 1994 (LS 236.11)
Informatiksicherheitsverordnung vom 17. Dezember 1997 (LS 170.8)
Finanzkontrollgesetz vom 30. Oktober 2000 (LS 614)
http://www.zhlex.zh.ch → „LS Aktuelle Fassungen“

Mitgeltende Unterlagen (Kanton Zürich)

Allgemeine Geschäftsbedingungen des Kantons Zürich über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen (AGB Sicherheit, September 2001) mit Kommentar
http://www.datenschutz.ch/themen/2001_agb_sicherheit.pdf
http://www.datenschutz.ch/themen/2001_agb_sicherheit_anhang.pdf

Datenschutzbeauftragter des Kantons Zürich, Muster-Vereinbarung zu § 13 Datenschutzgesetz
http://www.datenschutz.ch/themen/themen_datenschutz_1159.pdf

Weitere Quellen

Rundschreiben der Eidgenössischen Bankenkommission: Auslagerung von Geschäftsbereichen (Outsourcing) vom 26. August 1999 (EBK-RS 99/2 Outsourcing)
http://www.ebk.admin.ch/d/publik/rundsch/99-2.pdf

ISACA Switzerland Chapter IG Outsourcing, Outsourcing Contracts Control Review, 1999
http://www.isaca.ch/html/arbeitsgruppen.html

digma – Zeitschrift für Datenrecht und Informationssicherheit, Heft 4/2001 (Fokus: Outsourcing)
http://www.e-digma.ch

Abkürzungen und Begriffe

ISACA	Information Systems Audit and Control Association http://www.isaca.org bzw. http://www.isaca.ch
Leistungsbezüger	→ *Öffentliches Organ*, welches Dienstleistungen durch einen Dritten erbringen lässt bzw. Tätigkeiten oder Bereiche „outsourct“
Leistungserbringer	Öffentliche oder private Stelle, welche von einem → *öffentlichen Organ* für die Erbringung von Dienstleistungen beigezogen wird bzw. an welche Tätigkeiten oder Bereiche „outgesourct“ werden
LS	Loseblattsammlung der Gesetze des Kantons Zürich; http://www.zhlex.zh.ch
Öffentliches Organ	Behörde oder Amtsstelle des Kantons oder der Gemeinden, andere öffentliche Einrichtungen sowie Personen und Institutionen, soweit sie mit öffentlichen Aufgaben betraut sind (Definition gemäss § 2 Buchstabe c Datenschutzgesetz).