Finanzdirektion  
Amt für Informatik und Organisation

Anhang «Kontrolle und ISDS»

vom [DATUM]

zum (Rahmenvertrag oder Bestellung betreffend …]

1. Generelle Bestimmungen
   1. Kontrolle
      1. Kontrollrechte

Um zu gewährleisten, dass sie ihre Aufsichtsfunktion gegenüber dem KAIO gesetzmässig wahrnehmen können, räumt die Leistungserbringerin folgenden Stellen des Kantons Bern ein umfassendes Kontrollrecht ein:

1. der Datenschutzaufsichtsstelle des Kantons Bern (gem. Ziff. 2.9 AGB ISDS i.V.m. Art. 34 des kantonalen Datenschutzgesetzes; BSG 152.04); sowie
2. der Finanzkontrolle des Kantons Bern (gem. Art. 3 des kantonalen Finanzkontrollgesetzes; BSG 622.1).
   * 1. Audits

Das KAIO kann im Zusammenhang mit den erbrachten Leistungen Audits im Bereich der Informationssicherheit, der Prozessreifegrade, des Datenschutzes und der Leistungsabrechnung durchführen lassen.

Dem KAIO obliegt die Leitung des Audits. Es bestimmt nach Anhörung der Leistungserbringerin

1. die Auditobjekte (bspw. Prozesse, Core Services, Software, dazugehörige Datenbanken, Verfahren und Unterlagen, inkl. Dokumentation und Quellcode, Abrechnungsunterlagen),
2. die mit dem Audit beauftragte Organisation, wobei es sich nicht um einen direkten Konkurrenten der Leistungserbringerin handeln darf, und
3. das Verfahren und die Einzelheiten des Audits.

Die Leistungserbringerin wirkt beim Audit gemäss den Weisungen der mit dem Audit beauftragten Organisation mit. Sie gewährt deren Mitarbeitenden oder Beauftragten den nötigen Zugang, gewährt ihnen die nötige Einsicht und beantwortet die von ihnen gestellten Fragen.

Das KAIO verpflichtet die mit dem Audit beauftragte Organisation und ihre Mitarbeitenden und / oder Beauftragten zur Verschwiegenheit.

Die durch die beauftragte Organisation in Rechnung gestellten Kosten trägt das KAIO. Die Parteien tragen ihre eigenen Kosten für die Mitwirkung am Audit selbst.

Die Rechnungen betreffend Audit werden ausschliesslich an das KAIO gestellt. Das KAIO wird die Kosten wie oben beschrieben an die Parteien weiterverrechnen.

* 1. ISDS
     1. Grundsätze

Die Leistungserbringerin stellt mit technischen und organisatorischen Massnahmen sicher, dass ihre Subunternehmen sämtliche ISDS-Bestimmungen des Vertragswerks, beachten und umsetzen, welche auch für sie selbst gelten (insbesondere die Bestimmungen des vorliegenden Anhangs).

Die folgenden Regelwerke sind durch die Leistungserbringerin zu beachten und umzusetzen:

1. KDSG
2. DSV
3. ISDS DV
4. NSP BE
5. ICT-Enduserweisung
6. Weisung über den Umgang mit Authentisierungsmerkmalen
7. Weisung über den Anschluss von Informatikgeräten
8. Weisung über die Zutrittsberechtigungen
9. Weisung über die Zugriffs- und Nutzungsberechtigungen
10. Weisung über den Einsatz mobiler Informatikmittel
11. Weisung über die Nutzung des Internets

Bezüglich des Orts der Datenbearbeitung gilt Ziffer 20 AGB SIK. Betreffend Informationssicherheit und Datenschutz gilt Ziffer 13 AGB SIK. Darüber hinaus sind nachfolgende Ziffern zu berücksichtigen.

* + 1. Vertraulichkeit

Die Leistungserbringerin verpflichtet sich und ihre Subunternehmen schriftlich, die vom KAIO im Rahmen des Vertragswerks zur Verfügung gestellten Unterlagen, Daten und Informationen vertraulich zu behandeln.

Die von der Leistungserbringerin sowie ihren Subunternehmen eingesetzten natürlichen Personen gelten aus strafrechtlicher Sicht als funktionelle Beamte und unterstehen deshalb im Rahmen der Erfüllung des Vertragswerks dem Amtsgeheimnis (Art. 320 i.V.m. Art. 110 Abs. 3 StGB). Die Leistungserbringerin ist verpflichtet, sicherzustellen, dass diese Personen schriftlich auf diesen Umstand hingewiesen werden und eine entsprechende Vertraulichkeitserklärung unterzeichnen, bevor sie im Rahmen dieses Vertragswerks eingesetzt werden.

Die Vertraulichkeitspflicht bleibt auch nach Beendigung des Vertragswerks bestehen.

Das KAIO kann in künftigen Beschaffungsverfahren Informationen aus diesem Vertragsverhältnis gegenüber potenziellen neuen Leistungsanbietern offenlegen, soweit dies notwendig ist, damit ein vollständiges und sachgerechtes Angebot abgegeben werden kann.

* + 1. Schulung

Benötigen einzelne, von der Leistungserbringerin oder ihren Subunternehmen eingesetzte natürliche Personen zum Zweck der Leistungserbringung ein Benutzerkonto im Active Directory des Kantons Bern, so sind diese Personen dazu verpflichtet, den Onlinekurs «BE-Secure» erfolgreich zu absolvieren. Die dadurch verursachten Aufwände der Leistungserbringerin sind nicht separat verrechenbar.

* + 1. Information Security Management

Die Leistungserbringerin ist dazu verpflichtet, in ihrem Zuständigkeitsbereich nach dem aktuellen Stand der Technik und den Regeln der Kunst die Sicherheit und den Schutz der Informationen und Daten des KAIO zu gewährleisten. Sie berücksichtigt dabei insbesondere auch die ISDS-Bestimmungen des Bundes sowie die Vorgaben gemäss der jeweils aktuellsten Version der Normenserie ISO/IEC 2700x. Sie legt ohne Zutun des KAIO entsprechende technische und organisatorische Massnahmen fest und setzt diese nach Kenntnisgabe an das KAIO um. Die dadurch verursachten Aufwände der Leistungserbringerin sind nicht separat verrechenbar.

[Wenn noch keine oder nicht alle ISDS-Unterlagen bestehen:] Die vom KAIO zu erstellenden ISDS-Unterlagen sind für die Leistungserbringerin verbindlich. Die Leistungserbringerin wirkt bei der Erstellung dieser ISDS-Unterlagen auf Aufforderung des KAIO hin mit. Die durch diese Mitwirkungsobliegenheit verursachten Aufwände der Leistungserbringerin sind nicht separat verrechenbar.

Die Leistungserbringerin ist verpflichtet, auf Anweisung des KAIO technische oder organisatorische Massnahmen im ISDS-Bereich umzusetzen. Gehen die angewiesenen Massnahmen über den aktuellen Stand der Technik und die Regeln der Kunst hinaus, so kann die Leistungserbringerin dem KAIO die durch die Umsetzung verursachten Aufwände separat verrechnen.

[Wenn bereits ein ISDS-Konzept besteht:] Die Leistungserbringerin ist verpflichtet, die im ISDS-Konzept des KAIO vom [DATUM] definierten technischen und organisatorischen Massnahmen umzusetzen. Die dadurch verursachten Aufwände der Leistungserbringerin sind nicht separat verrechenbar.

* + 1. Risk Management

Die Leistungserbringerin betreibt ein Risikomanagement bezüglich der IT-Sicherheit als Teil des auf dem ISO-Standard 27001 basierenden ISMS. Dieses Risikomanagement sorgt für eine frühzeitige Erkennung und Bewertung von Gefahren und definiert präventive und reaktive Massnahmen zur Risikoreduktion. Das Risikomanagement der Leistungserbringerin ist zudem verantwortlich für die Überprüfung von Massnahmen.

Die identifizierten und bewerteten Risiken werden dem KAIO jährlich schriftlich kommuniziert unter Nennung der entsprechend beabsichtigten Massnahmen, soweit diese die Daten, Systeme und Prozesse des KAIO sowie jene der DIR / STA / JUS betreffen.

* + 1. Internes Kontrollsystem

Die Leistungserbringerin verfügt über ein IKS, welches den rechtlichen Vorgaben genügt, die auch für die Kantonsverwaltung gelten (Kontrollmodell COSO oder COBIT; analog Art. 12 FLV). Das IKS der Leistungserbringerin wird regelmässig von ihrer Revisionsstelle oder einer anderen, unabhängigen externen Stelle überprüft. Die Reports der Prüfungen werden dem Service Owner [X] unaufgefordert innert 30 Tagen seit sie die Leistungserbringerin erhalten hat zur Verfügung gestellt.

1. Spezialbestimmungen für Treuhandnetzwerke
   1. Präambel

Aufgrund der spezifischen Fallkonstellationen, welche sich bei der Beauftragung von Unternehmen stellen, welche einem internationalen Netzwerk von voneinander unabhängigen Treuhandunternehmen angehören, rechtfertigen sich die nachstehenden Spezifizierungen.

* 1. Datenbekanntgabe
     1. Grundsatz

Die Datenbekanntgabe untersteht - als Unterfall der Datenbearbeitung - dem Verhältnismässigkeits- und Vorsichtsprinzip. Die Leistungserbringerin darf demnach generell keine Daten bekanntgeben,

1. wenn die Bekanntgabe für die korrekte Erbringung der vereinbarten Leistungen ungeeignet ist;
2. wenn die Bekanntgabe für die korrekte Erbringung der vereinbarten Leistungen nicht notwendig ist (insb. Need-to-Know-Prinzip);
3. wenn die Bekanntgabe angesichts der Interessen, welche durch die bekanntzugebenden Daten betroffen sind, für den Kanton Bern unzumutbar ist; oder
4. wenn nicht zweifelsfrei klar ist, ob eine Datenbekanntgabe unter den eben angeführten Punkten a bis c zulässig ist.
   * 1. Datenbekanntgabe ins Ausland

Eine Datenbekanntgabe ins Ausland sowie eine Datenbearbeitung im Ausland müssen einerseits dem Verhältnismässigkeits- und Vorsichtsprinzip genügen und sind andererseits ausschliesslich für einen oder mehrere der nachfolgenden Zwecke erlaubt:

1. Sicherstellung der Einhaltung von berufsrechtlichen Vorschriften,
2. Prüfung der Einhaltung von internen Prozessen,
3. Prüfung von Interessenkonflikten und Sicherstellung der Unabhängigkeit,
4. Führung der Finanzbuchhaltung,
5. Erbringen von administrativen und IT-Unterstützungsleistungen, und
6. Kundenpflege.

Für die Zwecke gemäss der obenstehenden Buchstaben c bis f dürfen ausschliesslich der Kundenname, die Kundenadresse, die im Vertrag festgehaltenen Namen und Rollen, die Beschreibung der Dienstleistung und die Honorarhöhe bekanntgegeben und bearbeitet werden.

Es ist der Leistungserbringerin grundsätzlich verboten, besonders schützenswerte Personendaten und Daten, die dem Amtsgeheimnis unterstehen ins Ausland bekanntzugegeben.

* + 1. Datenbekanntgabe im Inland

Innerhalb der schweizerischen Landesgrenzen ist eine Datenbekanntgabe zu jedem Zweck erlaubt, sofern sie zur Vertragsdurchführung notwendig ist. Darüber hinaus gelten die Regeln über die Datenbekanntgabe ins Ausland sinngemäss.

* 1. Aufsicht und Kontrolle

Der Kanton Bern übt seine Auditrechte im Bereich der Aufsicht und Kontrolle nach Treu und Glauben aus. Dies bedeutet insbesondere, dass

1. der Kanton Bern Audits ausschliesslich unter Vorankündigung durchführen darf;
2. der Kanton Bern zusammen mit der Vorankündigung ein Auditprogramm bekannt gibt, welches mindestens umfasst:

* die Angaben der oder des Auditbeauftragten;
* den Scope des Audits;
* den Ablauf des Audits;
* die Vertraulichkeit des Audits; und
* das allfällige Eskalationsprozedere.

1. der Leistungserbringerin für jegliche Art von Audit ein Ablehnungsrecht gemäss oder analog Ziffer 2.8 AGB ISDS eingeräumt wird;
2. das Auditprogramm vor Durchführung des Audits gemeinsam geklärt wird, sodass die Leistungserbringerin ihr Ablehnungsrecht ordentlich wahrnehmen kann;
3. die oder der Auditbeauftragte keine Systemzugriffe oder Zutritte zu Räumlichkeiten der Leistungserbringerin erhält; ohne dass die Leistungserbringerin ihn oder sie überwacht, bzw. begleitet;
4. der Kanton Bern das Berufsgeheimnis der Leistungserbringerin respektiert und insbesondere keine Einsicht in Akten anderer Kunden der Leistungserbringerin erhält; und
5. die durch die oder den Auditbeauftragten einzusehenden Unterlagen zu jeder Zeit im Gewahrsam der Leistungserbringerin verbleiben, namentlich diese nicht aus den Räumlichkeiten der Leistungserbringerin entfernt werden.

\* \* \*